UNIVERZITA KOMENSKÉHO
V BRATISLAVE

FAKULTA MATEMATIKY, FYZIKY
A INFORMATIKY

RNDr. Martina Bátorová

Autoreferát dizertačnej práce

SINGULARITY HYPERELIPTICKÝCH A SUPERELIPTICKÝCH KRIVIEK

na získanie akademického titulu philosophiae doctor
v odbore doktorandského štúdia

9.1.7 Geometria a topológia

Bratislava 2013

Dizertačná práca bola vypracovaná v dennej forme doktorandského štúdia na Katedre algebry, geometrie a didaktiky matematiky Fakulty matematiky, fyziky a informatiky Univerzity Komenského v Bratislave.

Predkladateľ: RNDr. Martina Bátorová
Katedra algebry, geometrie a didaktiky matematiky
FMFI UK, Mlynská Dolina, 842 48 Bratislava

Školiteľ: doc. RNDr. Pavel Chalmovianský, PhD.
Katedra algebry, geometrie a didaktiky matematiky
FMFI UK, Mlynská Dolina, 842 48 Bratislava

Oponenti: .....
.....

.....
.....

.....
.....

Obhajoba dizertačnej práce sa koná ..... o ..... h
pred komisiou pre obhajobu dizertačnej práce v odbore doktorandského štúdia vymenovanou predsedom odborovej komisie .....

Geometria and topológia – 9.1.7 Geometria a topológia

na Fakulte matematiky, fyziky a informatiky Univerzity Komenského
Mlynská Dolina, 842 48 Bratislava

Predseda odborovej komisie:

prof. RNDr. Július Korbaš, CSc.
Katedra algebry, geometrie a didaktiky matematiky
FMFI UK, Mlynská Dolina, 842 48 Bratislava

Contents

On Singularities of Hyperelliptic and Superelliptic Curves

1 Introduction

Though some ideas and achievements in the area of plane algebraic curves and their singularities date back to ancient Greece, the beginnings of their systematic study are attributed to Newton. However, it was not until the centuries after his lifetime, especially the 19th one, that the rigorous methods for the investigation of singularities of algebraic curves were developed.

Today, the area of singularities of algebraic curves is a meeting point of many mathematical disciplines, both theoretical and applied. The interactions and ideas of algebraic geometry, topology, robotics, approximation theory or scientific visualizations – to mention just few – make the subject of the singularities of algebraic curves a very fruitful and exciting field of study.

Singular points introduce complications not only in theory, e.g. when computing an image of a curve in a suitable map, but also in practice, e.g. in numerical and scientific computations, "division by zero", linear dependence of vectors, discontinuous behavior in certain characteristic values etc. Moreover, the singularities of algebraic curves are not of the same nature. Their internal structure varies from very simple, e.g. so called *ordinary* having only different non-multiple tangents to the curve at the corresponding point, to very complex ones.

The complexity and structure of singularities can be captured using special numerical values resp. algebraic structures, called *invariants*. Among these are e.g. the genus g, the *Milnor's number* μ, the *torus knot type* or a system of *multiplicity sequences* [5].

The changes in the values of invariants are often used to describe the simplification of singularities during their *resolution* [25]. The resolution of singularities is a procedure with a goal to eliminate or simplify these points. Considering the *blowup* technique, we replace them locally by a birationally equivalent curve that is either regular or whose singularities are less complicated in a certain way. After a finite number of iterations, a curve that no longer contains singularities is obtained.

Besides the resolution of singularities, the technique of *deformations* is another fundamental method used for studying the singularities of algebraic curves [14]. Loosely speaking, the deformation is a modification of the curve in the neighborhood of its sin-

gularity in such a way, that the new curve still carries enough information about the original one. In case of plane singularities, any deformation can be defined via an s-parameter *unfolding*. These are a special parameterizations of the defining equation of the curve that enable us to modify the curve in a desired way.

In particular, a special 1-parameter system of deformations can be used to resolve the singularities of a class of so called *ADE singularities* [2], each of these deformations causing Milnor's number μ to drop by one up to regularity, i.e. until $\mu = 0$. On the other hand, the singularities of *hyperelliptic* and *superelliptic curves* are stable even under multiparameter unfoldings. Their internal structure and resolution of their singularities is independent of the configuration of roots of the defining polynomial created via given unfolding.

2 Goals and tasks

The thesis deals with singularities of plane curves defined over the field of complex numbers. It focuses on the changes in the structure of an isolated singularity of given plane curve, caused by a suitably picked deformation.

The first goal proposed in the *Project of Dissertation* (2011) was to explore the case of a single parameter deformation of given singularity. The first task was to study invariants of plane curve singularities and techniques used for their resolution. The second task was to look at possible representation of invariants of deformed curves, to examine the changes in the desingularization process of deformed singularities and to describe the changes in the structure.

The second goal was to investigate the case of multiparametric deformations, proceeding as above. The main task was to explore the interrelations and configurations of the parameters and their influence on the structure of given singularity and on the desingularization process.

In order to bring the abstract algebraic language closer to the interested reader, we aimed to visualize as many notions and procedures as possible. We used schematic pictures capturing only the basic idea (using Inkscape [15]) as well as precisely generated figures (via Maxima [1]). We extensively worked with available computer algebra systems Singular [6], Maxima and Sage [24], whose preprogrammed functionality was used to write routines for hypotheses testing.

3 Plane curves

Throughout the thesis, we work over the field of complex numbers $\mathbb{C}$, since it is algebraically closed and allows the notion of convergence. We work in the affine plane $\mathbb{A}^2(\mathbb{C})$ resp. in the projective plane $\mathbb{P}^2(\mathbb{C})$, where $\mathcal{A}_i$ with $i = 0, 1, 2$ denote the respective affine charts of $\mathbb{P}^2(\mathbb{C})$.

3.1 Algebraic and analytic plane curves

We focus on affine plane curves $\mathcal{C} \subset \mathbb{A}^2(\mathbb{C})$. They are defined as a zero set of an equation $f(x, y) = 0$, where $f\colon \mathbb{A}^2(\mathbb{C}) \to \mathbb{C}$ is an appropriate function (e.g. a non-constant polynomial $f \in \mathbb{C}[x, y]$ or a power series $f \in \mathbb{C}\{x, y\}$) in two indeterminates:

$$\mathcal{C} := \mathcal{V}(f) := \{(x, y) \in \mathbb{A}^2(\mathbb{C}) \mid f(x, y) = 0\}.$$

In the former case, the affine plane curve is called *algebraic*, in the latter it is called *analytic*. The power series enable us to handle curves in a small Euclidean neighborhood of given point, i.e. we have local access and control over the curve.

The *projectivization* $\mathcal{C}^* \subset \mathbb{P}^2(\mathbb{C})$ of $\mathcal{C}$ with $\deg(f) = \deg(\mathcal{C}) = d$ is the curve defined by a *homogenized* polynomial $F \in \mathbb{C}[x_0, x_1, x_2]$ of f, i.e. $F(x_0, x_1, x_2) := x_0^d f\left(\frac{x_1}{x_0}, \frac{x_2}{x_0}\right)$ and $\mathcal{C}^* := \mathcal{V}(F)$.

3.2 Singular points

The point $P \in \mathcal{V}(f)$ is singular iff $f(P) = \frac{\partial f}{\partial x}(P) = \frac{\partial f}{\partial y}(P) = 0$. Its multiplicity is given by the order m of the first non-vanishing partial derivative of f at P; here, P is called an *m-fold point* of $\mathcal{V}(f)$, a *singular point* or a *singularity* of $\mathcal{V}(f)$.

Assume the Taylor expansion of f at its m-fold point P. Its first non-vanishing component is

$$T_m(x, y) = \sum_{i=0}^{m} \binom{m}{i} \frac{\partial^m f}{\partial x^i \partial^{m-i} y}(P)(x - p_1)^i (y - p_2)^{m-i}.$$

By a linear change of coordinates that moves P to the origin O, the polynomial T_m is transformed to a homogeneous bivariate polynomial of degree m. In fact, if $P = O$, we have $T_m = f_m$, where $f(x, y) = \sum_{i \geq m} f_i(x, y)$ and each $f_i(x, y)$ is a form of degree i with $m = \operatorname{ord}(f)$. Since the number of factors of a polynomial is invariant under

linear changes of coordinates, the irreducible factors of T_m are all linear, each defining a *tangent to* $\mathcal{C}$ *at* P, together forming the *tangent cone to* $\mathcal{C}$ *at* P. The *multiplicity of a tangent* is the multiplicity of the corresponding factor of T_m.

If all the tangents to $\mathcal{C}$ at P are of multiplicity 1 (*simple*) and mutually distinct, we call P an *ordinary* singularity of $\mathcal{C}$, otherwise *non-ordinary*.

If a curve $\mathcal{V}(f)$ contains a singular point, $\mathcal{V}(f)$ is called *singular*, otherwise it is called *regular*.

3.3 Resolution of singularities

Resolution of singularity can be informally defined as a suitable simplification process, that transforms a singular object to an object that either no longer has singularities, or its singularities are less complicated in certain way.

One of the usual resolution techniques is known as *blowup*. It enables us to find a birationally equivalent curve, which is either regular, or is less singular in a certain way. In the latter case, we can repeat the process and obtain a regular curve after a finite number of steps, see [5, 25]. However, the final curve usually lies on an algebraic surface other than the plane $\mathbb{A}^2(\mathbb{C})$.

The simplest case happens when $\mathcal{X} \equiv \mathbb{C}^2$ and P is an ordinary singularity of $\mathcal{C}$ placed at the origin O. The essence of the blowup process then consists of replacing the plane $\mathbb{A}^2(\mathbb{C})$ by the set of all lines passing through P. Hence, P is replaced with the projective line $\mathbb{P}^1(\mathbb{C})$.

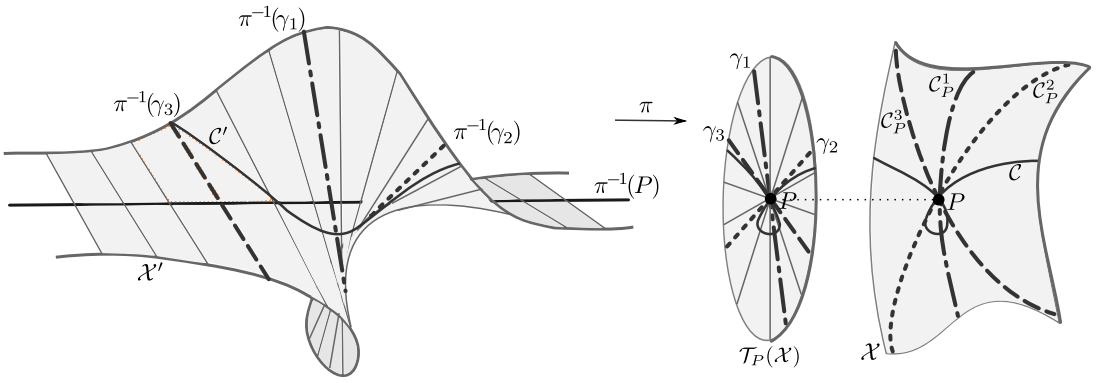

Figure 1: The blowup of a surface $\mathcal{X}$ at the point P is a regular surface $\mathcal{X}'$. Each of the lines γ_i is a tangent to a curve $\mathcal{C}_P^i \subset \mathcal{X}$ at the point P, together forming the tangent plane $\mathcal{T}_P(\mathcal{X})$ to $\mathcal{X}$ at P (schematic depiction).

In general, $\mathcal{X}$ is a surface in $\mathbb{P}^n(\mathbb{C})$. In this situation, we use the tangent plane to $\mathcal{X}$ at P (denoted by $\mathcal{T}_P(\mathcal{X})$). We construct $\mathcal{T}_P(\mathcal{X})$ by taking the set of all tangents $\{\gamma_i\}$ to all curves $\{\mathcal{C}_P^i\}$ at the origin P, such that each $\mathcal{C}_P^i \subset \mathcal{X}$ and $P \in \mathcal{C}_P^i$ is a regular point of $\mathcal{C}_P^i$ (for more see [7] and figure 1).

3.4 Topological invariants of singular points

The topology of singularities and eventual changes in the structure can be captured using *invariants*. These special values completely characterize the structure and describe the changes of singularity during desingularization.

Let the singularity of $\mathcal{V}(f)$ be placed at the origin. Then $f = \sum_{ij} c_{ij} x^i y^j$ can be conveniently displayed in the form of a *Newton diagram* [14, §I.2.1]. Each term $x^i y^j$ with non-zero coefficient c_{ij} is represented by a point (i, j) in a usual Cartesian plane. Then, a convex hull of such a set in the first quadrant is constructed, it is called the *Newton polygon* $\Delta(f)$. The boundary of $\Delta(f)$ consists of a polygonal path and two half lines. The polygonal part is called the *Newton diagram of* f (at the origin), denoted $\Gamma(f)$. Any polygonal segment $\sigma \subset \Gamma(f)$ is called a *facet.* For each facet $\sigma \subset \Gamma(f)$, we introduce the *truncation* $f^\sigma := \sum_{(i,j)\in\sigma} c_{ij} x^{ij}$ of f to σ, i.e. the sum of the terms in f corresponding to the points on σ.

The Newton diagram provides us with useful information that can be used to construct the local parameterization of given curve. Using the *Newton-Puiseux algorithm* [14, §I.3.1], a good parameterization $t \mapsto (t^m, g(t))$ is constructed, giving $f(x, g(x^{\frac{1}{m}})) = 0$. The fractional power series $g(t) = g(x^{\frac{1}{m}}) = \sum_{i\geq m} a_i x^{\frac{1}{m}}$ is called the *Puiseux expansion.*

Having the Puiseux expansion of f, we construct a special sequence $(m; \beta_1, \ldots, \beta_r)$ of positive integers via setting

$$\begin{aligned} \beta_1 &= \min\{k \mid a_k \neq 0, m \nmid k\}, & e_1 &= \gcd(m, \beta_1), \\ \beta_i &= \min\{k \mid a_k \neq 0, e_{i-1} \nmid k\}, & e_i &= \gcd(e_{i-1}, \beta_i), \end{aligned}$$

with $i = 2, \ldots, r$ s.t. $e_r = 1$. The algorithm always terminates, as the parameterization $g(t)$ was assumed to be good.

The sequence $(m; \beta_1, \ldots, \beta_r)$ is called the *Puiseux characteristic* of f, the numbers β_i are the *characteristic exponents* and the sequence $(e_0; e_1, \ldots, e_r)$ with $e_0 := m$ is the *associated Puiseux sequence.* It can be proven that the characteristic is independent of the choice of coordinates [25].

A complex curve $\mathcal{C} \subset \mathbb{A}^2(\mathbb{C})$ can be considered as a real surface in $\mathbb{A}^4(\mathbb{R}) \cong \mathbb{A}^2(\mathbb{C})$. Its intersection $\mathcal{K}$ with a small sphere $\mathbb{S}^3_\varepsilon$ around the singularity is called a *knot* associated to a singularity of $\mathcal{C}$: $\mathcal{K} = \mathcal{C} \cap \mathbb{S}^3_\varepsilon$. The knot is independent of the sphere radius ε for sufficiently small $\varepsilon > 0$ [5].

For a plane curve singularity, there is a nice description of the knot structure called the *cable knot* or the *iterated torus knot* [14, 25]. For each singularity, we assign a set of *Puiseux pairs* $(m_i, n_i), i = 1, \ldots, r$ defined by the Puiseux characteristic as

$$m_i = \frac{e_{i-1}}{e_i}, \qquad\qquad n_i = \frac{\beta_i}{e_i}$$

with $i = 2, \ldots, r$. The geometric interpretation of the previous formulae is as follows. We start with a simple (untied) knot $\mathcal{K}_0 \cong \mathbb{S}^1_\varepsilon$ and consider the surface of its small tubular neighborhood, i.e. a torus $\mathcal{T}_0$. Now, we construct a new knot $\mathcal{K}_1$ lying on $\mathcal{T}_0$ so that the coordinate x represents wrapping $\frac{m}{e_1}$ times around the parallels and the coordinate y wrapping $\frac{\beta_1}{e_1}$ times around the meridians of $\mathcal{T}_0$. If the singularity is more complicated, i.e. the Puiseux characteristic has $r > 1$ terms, we construct another tubular neighborhood $\mathcal{T}_1$ of $\mathcal{K}_1$ and a new knot $\mathcal{K}_2$ lying on $\mathcal{T}_1$. This knot is again determined by two integers specifying how many times it must turn around $\mathcal{T}_1$ in either direction. It turns out that these two numbers are given exactly by the next Puiseux pair $(m_2, n_2) = \left(\frac{e_1}{e_2}, \frac{\beta_2}{e_2}\right) = \left(\frac{\gcd(m,\beta_1)}{\gcd(m,\beta_1,\beta_2)}, \frac{\beta_2}{\gcd(m,\beta_1,\beta_2)}\right)$. The final knot is constructed via an r-step iteration of the previous procedure, when if $\mathcal{T}_i$ is a torus for the first i terms, adding of the $(i+1)$st term produces a knot of type $\left(\frac{e_i}{e_{i+1}}, \frac{\beta_{i+1}}{e_{i+1}}\right)$. The construction also explains the name cable knot and iterated torus knot.

The Milnor's number μ is one of the most important invariants. It may be defined in various ways, depending whether we wish to emphasize its topological, algebraic or geometric significance. In all cases, it is the key measure of the complexity of a singularity – it can be proven, that we can break up any (isolated) singularity into μ distinct ones, each with $\mu = 1$. These singularities are very simple, each is a union of two smooth branches meeting transversely [25]. In case of an irreducible curve $\mathcal{C}$, the Milnor's number $\mu(\mathcal{C})$ is even, if it is regular, $\mu(\mathcal{C}) = 0$.

3.5 ADE singularities

In the thesis, we focus on a very special kind of hypersurface singularities, the so called *ADE* or *simple* singularities [14]. They are isolated and additionally, their internal (topological) structure is very simple, e.g. they are describable by a single Puiseux pair, which indicates the least complicated type of isolated singularities. The *ADE*

string itself is a standard Vladimir Arnold's notation for simple singularities [2]. It is based on the deep connection of these singularities with simple Lie groups, where each of the A-D-E denotes the corresponding Lie algebra.

In the plane case, the ADE singularities are defined as zero sets of $f \in \mathbb{C}[x, y]$ or $f \in \mathbb{C}[[x, y]]$, where f has on of the following forms:

$$\begin{array}{llll} A_k\colon & x^{k+1} + y^2 & k \geq 1 & E_6\colon \quad x^4 + y^3 \\ D_k\colon & x(x^{k-2} + y^2) & k \geq 4 & E_7\colon \quad y(x^3 + y^2) \\ & & & E_8\colon \quad x^5 + y^3, \end{array}$$

The classification is valid upto a coordinate change, for more see [14, 25].

For k odd, the plane curves with the A_k singularity are reducible – they comprise of two lines or two generalized parabolas. The plane D_k singularities are all reducible – they consist of the y axis and the A_{k-3} singularity. The E_6 and E_8 singularities are irreducible, the E_7 one is not. The parabola $A_0\colon x + y^2$ is usually excluded, since it is regular.

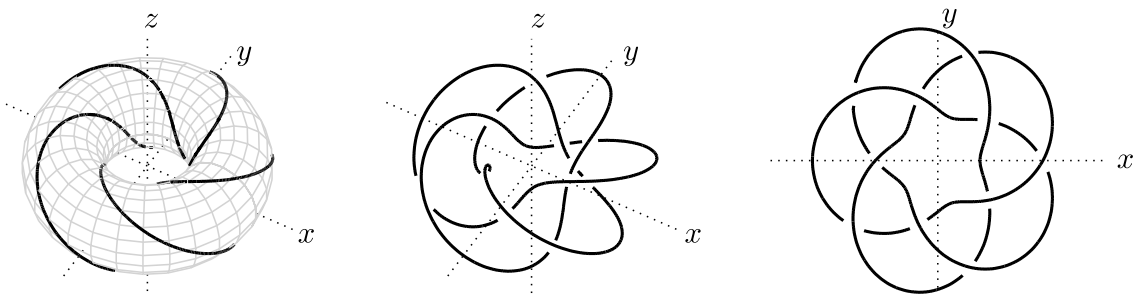

Figure 2: The knot associated to the E_8 singularity: the torus knot depicted on the $\mathcal{T}_0$ torus (left), the knot itself (middle) and the projection to the (x, y)-plane (right).

The ADE singularities are of a very special kind, either of so called *toric* or *quasitoric* type [16]. Let $p \geq q > 1$ be integers. A plane curve singularity $\mathcal{V}(f)$ is said to be of *toric type* (q, p), if it has the same topological type as $x^p + y^q$, i.e. it is representable in such a way in a suitably chosen coordinate system. The singularity $\mathcal{C}$ is of a *quasitoric type,* if it has the topological type as one of the following:

$$\begin{array}{rl} x(x^p + y^q) & \text{with } \ p > q, \\ y(x^p + y^q) & \text{with } \ p > q \ \text{ and } \ q \nmid p, \\ xy(x^p + y^q) & \text{with } \ p > q \ \text{ and } \ q \nmid p. \end{array}$$

We see that the A_k and D_4 singularities are of the toric type, the $D_k, k > 4$ of the quasitoric type, the E_k singularities of the toric (E_6, E_8) and the quasitoric type (E_7). The numbers (q, p) represent precisely the torus knot type of given singularity.

3.6 Deformations of singularities

We distinguish deformations of the defining series $f(x,y) \in \mathbb{C}\{x,y\}$ of the curve, and of the curve $\mathcal{V}(f)$ itself. The difference appears when isomorphism classes of deformations are considered. In our thesis, we work with the former.

The deformation of the defining series $f \in \mathbb{C}\{x,y\}$ of a curve passing through the origin is usually called an *unfolding*. It is any power series $\bar{f}(x,y,t_1,\ldots,t_s) \in \mathbb{C}\{x,y,t_1,\ldots,t_s\}$ s.t. $\bar{f}(x,y,0,\ldots,0) = f(x,y)$. Subsequently, any unfolding can be written as

$$\bar{f}(x,y,t_1,\ldots,t_s) = f(x,y) + u(x,y,t_1,\ldots,t_s).$$

In case of plane singularities, any deformation is given by an unfolding [14, §II.1.2].

3.7 Summary

Basic notions and definitions on plane curves and their singularities are recalled. The topology and structure of the singularities in terms of their topological (iterated torus knots, Puiseux characteristic) and numerical invariants (genus, Milnor's number, system of multiplicity sequences) are described, their mutual interrelations and conversion formulae are given. The blowup technique used for resolution of singularities is surveyed in detail. The desingularization process of the ADE singularities is investigated. The topological structure of toric and quasitoric singularities is shown and a general formula for computation of their Milnor's number is given. The deformations via unfoldings are surveyed and their most important properties are summarized.

4 Hyperelliptic curves

A particular class of algebraic curves, the *hyperelliptic curves* (HeC), play an important role in public key cryptography (see [12, 17, 19]) as a generalization of *elliptic curves* [8]. Although their usage in cryptography is not straightforward, the available HeC-based cryptosystems are very robust in terms of standard security attacks.

The theory of hyperelliptic curves may be approached from either algebraic or geometric point of view. The former handles these curves via the theory of quadratic field extensions and ideal theory, see e.g. [3, 9, 22] or via their automorphism groups [23]. We chose the latter since it provides us with high level of intuitive clarity. We

use a standard geometric definition [20], an alternative approach that uses the theory of Riemann surfaces can be found in [21].

4.1 Definition and basic properties

As a topological space, the curve $\mathcal{C}$ is a 2-dimensional topological (real) manifold in $\mathbb{A}^4(\mathbb{R}) \equiv \mathbb{A}^2(\mathbb{C})$, a surface. If $\mathcal{C}$ is regular, this surface is a *Riemann surface* $\mathcal{R}$ [10], i.e. a connected orientable manifold equipped with a complex structure [11]. The genus of $\mathcal{C}$ is the topological genus of the surface – an integer representing the maximum number of cuttings along closed simple curves without rendering $\mathcal{R}$ disconnected. Informally, it is the number of "holes" in $\mathcal{R}$ or the number of "handles" attached to a sphere $\mathbb{S}^2$. If the curve $\mathcal{C}$ is singular, the genus of $\mathcal{C}$ is the genus of its non-singular model constructed via resolution process.

In general, the g a non-negative integer. It is one of the basic birational invariants of algebraic varieties, i.e. it does not change under birational transformations of given object. In particular, the genus of any smooth (complex plane) curve of degree d is

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

A *hyperelliptic curve* $\mathcal{V}(f)$ *of genus* g *over* $\mathbb{C}$ is a regular affine complex plane algebraic curve defined by a bivariate absolutely irreducible polynomial $f \in \mathbb{C}[x, y]$ such that

$$f(x, y) = y^2 + y\,h(x) - r(x), \qquad (1)$$

where $h, r \in \mathbb{C}[x]$ and r is monic, i.e. the coefficient of the leading term is 1. Also, some additional genus-dependent conditions are put on the degrees of h, r in terms of genus g.

If the curve $\mathcal{C} := \mathcal{V}(f)$ defined by the equation (1) has an *odd* degree $\deg(f) := \deg(r) = 2g + 1$ and $\deg(h) \leq g$, it is called *imaginary*. If the curve $\mathcal{C}$ has an *even* degree $\deg(f) := \deg(r) = 2g + 2$ and $\deg(h) \leq g + 1$, it is called *real*.

The conversions between the two models exist [18] and we can also eliminate the y-linear term of $f(x, y)$ via the *Tchirnhaus transformation* [14, §I.2.4]. Thus the hyperelliptic curve $\mathcal{C}$ can be represented by an irreducible polynomial

$$y^2 - \frac{1}{4}h^2(x) - r(x) =: y^2 - \tilde{r}(x) =: \tilde{f}(x, y)$$

of degree $\deg(f) = \deg(r) = 2g + 1$ with r monic. In such a case, the regularity condition significantly simplifies – $\mathcal{C}$ is regular iff the polynomial r has no multiple roots.

After projectivization, the set of points of $\mathcal{C}$ at infinity consists of a single point P. It is the only projective point satisfying the homogenized equation of $\mathcal{C}$. In addition, it is singular.

4.2 Deformations of hyperelliptic curves via unfoldings

In particular, we study an s-parametric unfolding $\bar{f}$ of the defining polynomial f with $1 \leq s \leq d$ parameters given by

$$\bar{f}(x, y, t_1, \ldots, t_s) = y^k - (x - (x_1 + t_1)) \cdot \ldots \cdot (x - (x_r + t_s))u(x)$$

s.t. $\bar{f}(x, y, 0, \ldots, 0) = f(x, y)$ and $u \in \mathbb{C}[x, y]$ with $t_i, i = 1, \ldots, s$ having real resp. complex values. The unfolding and values of parameters need to be plausible, i.e. picked in such a way that the curve remains hyperelliptic (e.g. that $\mathcal{V}(\bar{f})$ is still regular).

4.3 Resolution of singularities of hyperelliptic curves

As a final step, we are interested in the structural changes of singularity of given hyperelliptic curve $\mathcal{C}$, caused by the complex parametrization of its roots. At first, we need to move the singularity of $\mathcal{C}$ from infinity to the origin. To do so, we projectivize the original curve, choose a different affine chart and dehomogenize with respect to it. The singularity is now placed in the origin, and we may resolve it by a series of blowups. Interestingly, the resolution process of a hyperelliptic curve of genus g always follows the same pattern; it is given in the thesis in the form of a pseudoalgorithm.

4.4 Stability of singularities of hyperelliptic curves

By an abuse of notation, let the curve with singularity moved to the origin of a suitable affine chart be defined by a polynomial denoted by f. It turns out that the particular deformations and configuration of roots of $\bar{f}$ have no effect on the structure of the singularity. This is due to the fact that the non-deformed polynomial f is *semiquasihomogeneous* (SQH) at the origin, i.e. that there is a facet σ of the corresponding Newton diagram $\Gamma(f)$ s.t. the truncation f^σ (called the *principal part* of f) has no critical points outside the origin.

Alternatively, f is SQH iff we can write $f = f^\sigma + v(x)$ with $\mu(f^\sigma) = \mu(f) < \infty$. Since the Milnor's number μ characterizes the singularity of f, the fact that $\mu(f^\sigma) = \mu(f)$

means that the entire topology of the (single) isolated singularity placed at the origin is encoded in the principal part f^σ. The principal part is always of the form $f^\sigma = y^{2g-1} - x^{2g+1}$, i.e. the parameterization of the roots caused by the unfoldings affects only the remaining terms of f, leaving f^σ intact. Therefore, the topology and resolution process of any hyperelliptic curve singularity are independent e.g. of the configuration of roots of $\bar{f}$ in the Gauss plane $\mathcal{G}$ representing the complex x-axis. Hence the singularities of hyperellitic curves are stable under plausible (in the above sense) unfoldings of the polynomial f.

The tangent cone to the singularity at the origin is given by the term of f of the lowest degree, i.e. by y^{2g-1}. Therefore, the singularity at the origin is non-ordinary, with a $(2g-1)$-tuple x-axis $\mathcal{V}(y)$ as the tangent at the origin. Since $\gcd(2g-1, 2g+1) = 1$, the singularity of $\mathcal{C}$ is of toric type $(2g-1, 2g+1)$. The torus knot type is $(2g-1, 2g+1)$; this is also the Puiseux characteristic of the singularity. The Milnor's number is $\mu(f) := \mu(f^\sigma) = 4g(g-1)$.

In the thesis, the claims of this section are proven in a series of lemmas.

4.5 Summary

The hyperelliptic curves over the field of complex numbers $\mathbb{C}$ are defined and their various representations and models are discussed. Necessary related notions are given to describe their singularities placed at infinity. The deformations using specific s-parameter unfoldings of the defining equation $f(x, y)$ are surveyed. The influence of particular configurations of roots of $f(x, y)$ on the structure of the singularity is investigated. The independence of this structure of the plausible unfoldings of $f(x, y)$ is proven, the topology of singularities and their desingularization process are described in detail.

5 Superelliptic curves

The *superelliptic curves* (SeC) are a generalization of both the classes of elliptic and hyperelliptic curves. Similarly to the latter, some cryptographic applications mostly over fields of finite characteristic are possible [13]. These curves are often studied via their automorphism groups [4]. We handle them in the sense of previous sections, i.e. we are interested in the structure of their singularities and in the changes caused by specific unfoldings of their defining polynomials.

5.1 Definition and basic properties

Superelliptic curves defined over the field of complex numbers $\mathbb{C}$ are given by polynomials $f \in \mathbb{C}[x, y], r \in \mathbb{C}[x]$ s.t.

$$f(x, y) := y^k - r(x) \quad \text{and} \quad r(x) = x^d + \ldots + c_1 x + c_0 = \prod_{i=1}^{d} (x - x_i)$$

satisfying the following constraints:

$$\gcd(k, d) = 1, \quad \gcd\left(r(x), \frac{\mathrm{d}\, r(x)}{\mathrm{d}\, x}\right) = 1, \quad r(x) \in \mathbb{C}[x] \text{ is monic}$$

In the first condition, any values of $k, d \in \mathbb{N}$ are allowed. We only adopt the lower bound condition $k, d \geq 3$ from [13], since $k = 2, d = 3$ results in elliptic and $k = 2, d \geq 5$ in hyperelliptic curves. The condition implies that the curve $\mathcal{V}(f)$ is irreducible and also ensures that the projectivization of $\mathcal{V}(f)$ has a single point at infinity. The second condition requires that $r(x)$ has no multiple roots. As a result, the (affine plane) curve $\mathcal{V}(f)$ is regular. Many authors do not explicitly require the monicity of $r(x)$. But since $\gcd(k, d) = 1$, a change of coordinates can be made to obtain a monic equation [13].

The genus $g \in \mathbb{N}_0$ of a superelliptic curve is $g = \frac{1}{2}(k-1)(d-1)$, for proof see [13].

Any superelliptic curves has a single point P at infinity. If $k < d$, the point P is singular iff $k + 1 < d$. If $k > d$, the point P is singular iff $d + 1 < k$.

5.2 Deformations of superelliptic curves via unfoldings

Assume a superelliptic curve $\mathcal{C} := \mathcal{V}(f)$ s.t. it is singular at infinity, i.e. $|d - k| > 1$. As before, we are interested in the influence of a similar parameterization of roots on the process of resolution of given singularity.

After parameterization of roots via an s-parameter unfolding of the defining polynomial f, the singularity at infinity can be resolved. After projectivization of the original curve and choice of a suitable affine chart, the curve is desingularized in a finite number of steps.

Again, we state and prove similar lemmas about stability of singularities of superelliptic curves. We also show that the singularity is of toric type $(d-k, k)$, both the torus knot type and the Puiseux characteristic are $(d - k, k)$ and the Milnor's number is $\mu(f) = (d - k - 1)(d - 1)$. The singularity of f is non-ordinary, its tangent cone at the origin of the corresponding affine chart is given by a $(d-k)$-tuple x-axis $\mathcal{V}(y)$.

5.3 Summary

An outline similar to that of the chapter on hyperelliptic curves is followed. The superelliptic curves over $\mathbb{C}$ are defined and their properties and behavior under plausible unfoldings are investigated. Analogous statements on the stability of their singularities are stated and proven. A general blowup desingularization procedure of the singularity at infinity is presented.

6 Conclusion

We presented an overview of the plane algebraic curves defined over the field of complex numbers $\mathbb{C}$ and their singularities. The emphasis was put on their structure and on the description techniques used for capturing the complexity of given singularity, in terms of numerical and topological invariants. Also, the resolution and deformation techniques were introduced as a tool for a systematic study of singularities and their behavior under specific transformations.

In particular, we focused on three classes of plane algebraic curves.

The ADE singularities were investigated and their topology was given. Values of Milnor's number μ and torus knot types were computed for a more general class of curves with toric and quasitoric singularities.

We described the structure of singularities at infinity of both the hyperelliptic and superelliptic curves defined over $\mathbb{C}$. We subjected their defining equations to a series of deformations using unfoldings, where the respective coefficients of the terms were parameterized. We investigated the behavior of the singularities of the modified curves under desingularization via blowups and observed the influence of said parameterizations on the structure and complexity of these singularities. For both the classes of curves, we concluded with the proof that the structure and resolution process is independent of the configuration of the roots in the Gauss plane $\mathcal{G} \cong \mathbb{R}^2$ representing the x-axis and of their mutual linear resp. higher order dependence. Also, a detailed description of the resolution of singularities of hyperelliptic curve of any genus g resp. of a superelliptic curve $\mathcal{V}(y^k - r(x)), \deg(r) = d$ for any plausible values of k, d was given.

For the sake of clarity and to aid the understanding of the subject, the more involving notions and procedures were illustrated via multiple examples and figures.

References

[1] Maxima 12.01.0. A Computer Algebra System, 2013. http://maxima.sourceforge.net/.

[2] V. I. Arnold, S. M. Gusein-Zade, and A. N Varchenko. *Singularities of Differentiable Maps: Classification of Critical Points, Caustics and Wave Fronts (reprint of the 1985 edition)*. Modern Birkhäuser Classics. Birkhäuser Boston, Inc., 2012.

[3] M. Bauer, M. J. Jacobson, Y. Lee, and R Scheidler. Construction of Hyperelliptic Function Fields of High Three Rank. *Mathematics of Computation*, 77:503–530, 2007. http://www.ams.org/journals/mcom/2008-77-261/S0025-5718-07-02001-7/.

[4] L. Beshaj, V. Hoxha, and T. Shaska. On Superelliptic Curves of Level n and their Quotients, I. *Albanian Journal of Mathematics*, 5(3):115–137, 2011. http://arxiv.org/abs/1209.0492/.

[5] E. Brieskorn and H. Knörrer. *Plane Algebraic Curves*. Springer-Verlag New York Inc., New York, 1986.

[6] W. Decker, G. M. Greuel, G. Pfister, and H. Schönemann. Singular 3.1.6. A Computer Algebra System for Polynomial Computations, 2013. http://www.singular.uni-kl.de.

[7] M. P. Do Carmo. *Differential Geometry of Curves and Surfaces*. Prentice Hall Inc. Englewood Cliffs, New Jersey, 1976.

[8] A. Enge. *Elliptic Curves and their Applications to Cryptography: An Introduction*. Springer Science + Bussiness Media, New York, 1999.

[9] A. Enge and A. Stein. Smooth Ideals in Hyperelliptic Function Fields. *Mathematics of Computation*, 71(239):1219–1230, 2001. http://www.ams.org/journals/mcom/2002-71-239/S0025-5718-01-01352-7/.

[10] H. M. Farkas and I. Kra. *Riemann Surfaces*. Springer Science + Bussiness Media, New York, 1992.

[11] O. Forster. *Lectures on Riemann Surfaces (Graduate Texts in Mathematics)*. Springer-Verlag, 1981.

[12] S. D. Galbraith. *Mathematics of Public Key Cryptography*. Cambridge University Press, Cambridge, 2004. http://www.math.auckland.ac.nz/∼sgal018/crypto-book/crypto-book.html.

[13] S. D. Galbraith, S. Paulus, and N. P. Smart. Arithmetic on Superelliptic Curves. *Mathematics of Computation*, 71:393–405, 2000. http://www.ams.org/journals/mcom/2002-71-237/S0025-5718-00-01297-7/.

[14] G. M. Greuel, Ch. Lossen, and E. Shustin. *Introduction to Singularities and Deformations*. Springer-Verlag New York Inc., New York, 2007.

[15] B. Harrington and The Inkscape Development Team. INKSCAPE 0.48. A Vector Graphics Editor, 2013. http://www.inkscape.net/.

[16] B. Hasset. Local Stable Reduction of Plane Curve Singularities. *Journal für die Reine und Angewandte Mathematik (Crelles Journal)*, 520:169–194, 2000.

[17] M. J. Jacobson, A. Menezes, and A. Stein. Hyperelliptic Curves and Cryptography. *Fields Institute Communications Series*, 41:255–282, 2004.

[18] M. J. Jacobson, R. Scheidler, and A. Stein. Cryptographic Aspects of Real Hyperelliptic Curves. In *Cryptology ePrint Archive, Report 2010/125*, 2010. http://eprint.iacr.org/2010/125.pdf.

[19] T. Lange. Efficient Arithmetic on Genus 2 Hyperelliptic Curves over Finite Fields via Explicit Formulae. In *Cryptology ePrint Archive, Report 2002/121*, 2002.

[20] A. J. Menezes, Y. H. Wu, and R. J. Zuccherato. An Elementary Introduction to Hyperelliptic Curves. In *Technical Report CORR 96-19*, 1996. http://www.math.uwaterloo.ca/∼ajmeneze/publications/hyperelliptic.pdf.

[21] G. Mess. A Note on Hyperelliptic Curves. In *Proceedings of the American Mathematical Society*, volume 115, pages 849–852, 1992. http://www.jstor.org/stable/2159236.

[22] S. Paulus and H. G. Rück. Real and Imaginary Quadratic Representations of Hyperelliptic Function Fields. *Mathematics of Computation*, 68(227):1233–1241, 1999. http://dx.doi.org/10.1090/S0025-5718-99-01066-2/.

[23] T. Shaska. Determining the Automorphism Group of a Hyperelliptic Curve. pages 248–254, 2003. http://arxiv.org/pdf/math/0312284v1.pdf.

[24] W. A. Stein and The Sage Development Team. SAGE 5.0. The Sage Mathematics Software, 2013. http://www.sagemath.org/.

[25] C. T. C. Wall. *Singular Points of Plane Curves*. Cambridge University Press, Cambridge, 2004.

Publications

Conference and journal publications

Bátorová, M. – Valíková, M. – Chalmovianský, P.: *Desingularization of ADE singularities via deformation.* In: Spring Conference on Computer Graphics SCCG'2013: Conference Proceedings. Bratislava: Comenius University, 2013. pp. 44-51. ISBN 978-80-223-3377-1.

Bátorová, M.: *Parameterized blowup of singularities of hyperelliptic curves* (in Slovak; Parametrizované rozdutie singularity hypereliptickej krivky). In: Geometry and its applications 2013: Seminar Proceedings. Bratislava: Slovak University of Technology, 2013. ISBN 978-80-227-3894-1.
http://www.math.sk/gaja/abstract/2013/Abstrakt_Batorova_GAJA2013.pdf

Bátorová, M. – Chalmovianský, P. – Pokorná, B. – Valíková, M.: *Singular point of curves, structure, visualization and application in geometric modeling.* In: Information Technology Applications: Journal. Bratislava: Paneuropean University, 2013 (to appear).

Bátorová, M. – Chalmovianský, P.: *Deformations of hyperelliptic curves of genus 2.* In: Proceedings of Symposium on Computer Geometry SCG'2012, Vol. 21: Conference Proceedings. Bratislava: Slovak University of Technology, 2012. pp. 11-16. ISBN 978-80-227-3798-2.

Bátorová, M.: *Blowup of an isolated singular point on an algebraic curve.* In: Proceedings of the 50th Anniversary of Foundation of the Department of Geometry on Faculty of Natural Sciences of Comenius University: Seminar Proceedings. Bratislava: Comenius University, 2010. (to appear)

Bátorová, M. – Chalmovianský, P.: *Blowing up a singular point of algebraic curve on algebraic surface.* In: Symposium on Computer Geometry SCG'2010, Vol. 19: Conference Proceedings. Bratislava: Slovak University of Technology, 2010. pp. 5-10. ISBN 978-80-227-3364-9.

Bátorová, M.: *First steps to resolution of singularities of plane curves via blowups* (in Slovak; Úvodné kroky rozkladu singularity rovinnej krivky metódou lokálneho rozdutia). In: Geometry and its applications 2010: Seminar Proceedings. Bratislava: Slovak University of Technology, 2010. ISBN 978-80-227-3258-1.
http://www.math.sk/gaja/abstract/2010/Abstrakt_Batorova2010.pdf

Bátorová, M.: *Desingularization of curves in affine plane* (in Slovak; Desingularizácia kriviek v affinnej rovine). Student Scientific Conference 2009. Bratislava: Comenius University, 2009.

Talks

Bátorová, M.: *Singularities of algebraic curves lying on algebraic surfaces.* Computer Graphics Seminar. Martin Luther University in Halle – Wittenberg. Germany. 2011.

Other publications

Varhaníková, Ivana - Bátorová, Martina - et. al.: *Virtual reality without borders: ... mini-conference for pupils and students.* In: ICL: Interactive Collaborative Learning. Piscataway: IEEE, 2012. ISBN 978-1-4673-2426-7.

Research projects

Geometrical and topological properties of varieties. VEGA 1/0330/13. 2013.
Principal investigator: prof. RNDr. Július Korbaš, CSc.

Parameterization of blowup of a singular point of a genus 2 hyperelliptic curve. UK/204/12. 2012. Comenius University grant (€920).
Principal investigator: RNDr. Martina Bátorová.

Geometry of isolated singularities of algebraic curves. 2011. SPP Foundation grant Hlavička (€1600).
Principal investigator: RNDr. Martina Bátorová.

Geometrical and algebraic properties of isolated singularities of algebraic curves. UK/ 529/10. 2010. Comenius University grant (€1160).
Principal investigator: RNDr. Martina Bátorová.

Tools of geometric modeling. VEGA 1/0730/09. 2009.
Principal investigator: doc. RNDr. Miloš Božek, CSc.

Theses

Bátorová, M.: *Singular points of planar algebraic curves, their structure, invariants and deformations*. Project of dissertation. Comenius University, 2011.

Bátorová, M.: *Desingularization of curves in projective plane* (in Slovak; Desingularizácia kriviek v projektívnej rovine). Rigorous thesis (RNDr.). Comenius University, 2009.

Bátorová, M.: *Resolution of singularities of plane curves* (in Slovak; Rozklad singularít rovinných kriviek). MSc. thesis (Mgr.). Comenius University, 2009.

Awards

Best Presentation Award (3rd place, based on public voting). Spring Conference on Computer Graphics 2013.

Dean's Award, 2009.

MSc. degree with Honors, 2009.

ŠVOČ (Student Scientific Conference, Czechoslovak international round), Chair's Award, 2009.

ŠVK (Student Scientific Conference), Winner (3rd place), 2009.