Topology of planar singular curves resultant of two trivariate polynomials

Judit Recknagel

Topology of planar singular curves resultant of two trivariate polynomials

Bachelor Thesis

for attainment of the academic degree of

Bachelor of Science

presented by

Judit Recknagel

August 27, 2013

Martin-Luther-University
Halle-Wittenberg

Faculty of Natural Sciences III
Institute for Computer Science
Computer Graphics
Doz. Dr. Peter Schenzel (Supervisor)

Inria research centre
Nancy-Grand Est

Team VEGAS
PhD Marc Pouget (Supervisor)
PhD Guillaume Moroz (Supervisor)

Contents

1 Introduction

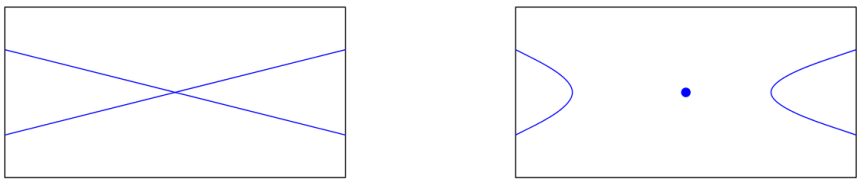
Scientific visualisation of curves and surfaces is needed in a great number of application fields, like personal calculators or robotic mechanisms. According to the use there are many aspects of a correct visualisation, it may be the correct geometrical (angles and lengths) or the correct topological representation of the curve, meaning the exact number of connected components with its self-intersections and isolated points.
If the curve is smooth, there exists several numerical tools to represent accurately its topology and geometry, for example by approximating the curve with a piece-wise linear graph, see [MKC-2009]. Such numerical methods are quite efficient and work locally well but it is not possible to use them to calculate the topology of the whole curve. A representative method is a curve tracking algorithm based on interval arithmetic or subdivision which obviously fails in singular curve points. Therefore, this method is useless to calculate the right topology of a curve which contains singular points. An option is to use an algebraic-symbolical approach, for example by using Gröbener bases, to calculate the exact topology of the curve. Such methods work globally but have a high complexity with the result that they are uneffective for complex curves in practice.
We are interested in the correct topological representation of plane curves, especially in the local topology of their singular points. Our approach is a combination of numerical and symbolical methods to recover the efficiency of the firsts ones with the accuracy of the second ones.

Considering two hypersurfaces given by the zero set of two trivariate polynomials f and g in $\mathbb{Q}[x, y, z]$, we are interested in the problem of computing the topology of the curve r which is given as the projection of the intersection of the hypersurfaces into $(z = 0)$-plane: $\mathbf{V}(r) = \text{proj}_{z=0}(\mathbf{V}(f) \cap \mathbf{V}(g))$. The curve r consists of all points $(X, Y) \in \mathbb{R}^2$ such that there exists an $Z \in \mathbb{R}$ with $f(X, Y, Z) = g(X, Y, Z) = 0$. An other way to regard the problem is to consider f and g as polynomials in z with two indeterminates x and y. Then the zero set of the curve r is exactly the set of all specialization (X, Y) such that $f(X, Y, z) = g(X, Y, z) = 0$ has at least one solution Z.
If we assume the space curve $\mathbf{V}(f) \cap \mathbf{V}(g)$ have no points at infinity, the projection r of this curve is given as the resultant of these two polynomials f, g with respect to z.

For a smooth planar curve r we have no difficulties in computing its topology since there are several adaptive numerical algorithms which accomplish this. But r in our situation as the projection of a space curve is usually not smooth. For example if there exist two different zeros $Z_1, Z_2 \in \mathbb{R}$ for a specialization (X, Y) of f and g, meaning $F(X, Y, Z_1) = G(X, Y, Z_1) =$

$F(X, Y, Z_2) = G(X, Y, Z_2) = 0$ while $Z_1 \neq Z_2$, then $r(X, Y) = 0$ and $\mathbf{V}(f) \cap \mathbf{V}(g)$ has at least two points over (X, Y). Hence the projection curve r intersects necessarily in (X, Y) and is therefore not smooth. Such an intersection point (X, Y) is one example for a singular point (also called singularity) of r.

We work on the problem of calculating the topology of singular curves by first determining their singular point set. The topology of non-singular curve segments can be easily computed by traditional algorithms, like path tracking. Afterwards, we calculate the local topology in a box containing exactly one singular point.



Two singularity enclosing boxes with different local topologies

There are several approaches to calculate the local topology in the boxes, for example by extracting also extremal points to distinguish between different local topologies in the singularities. The topology of non-singular curve segments and the local topology of singularity enclosing boxes give together the whole topology of the curve.

The aim of this work is to determine the singular point set V of r which is given by the solution set of the polynomial system

$$r(x, y) = 0, \quad \partial_x r(x, y) = 0, \quad \partial_y r(x, y) = 0$$

of three equations in two indeterminates. We want to use a subdivision fix point algorithm to compute boxes in $\mathbb{R}^2$ containing exactly one singular point of the system: Given a box $B \subset R^2$, we subdivide this box recursively in smaller boxes until all solutions of the system are separated in disjoint boxes. A standard numerical criterion for accepting a box containing exactly one regular solution of the system is the numerical Newton-Krawczyk-interval operator. Unfortunately, this operator handles (1) only systems with the same number of equations as indeterminates and (2) guarantees only the determination of regular solutions. To apply the Krawczyk operator to calculate the singular point set of the curve r, we have to transform our original system into a system with the same zero set which satisfies the formal assumptions of the operator. The new system must consists of two equations in two indeterminates. Furthermore, we have to prove the regularity of all solutions of the system.

A first transformation approach is to simplify the system by taking only two among the three equations and calculate their zero set, but this procedure fails in general because it introduces spurious solutions. Hence we try a second approach to create a new system with the same zero set via subresultant theory.

In the language of algebraic geometry, V is the corresponding affine variety to the ideal generated by the polynomials $r, \partial_x r, \partial_y r \in \mathbb{Q}[x, y]$. We are done if we can find a two member generating set of I, but unfortunately, this is not easy. If we consider only simple self-intersections of the curve r, we can prove instead the equality of V and the solution set W of the system

$$\sigma_{11}(x, y) = 0, \quad \sigma_{10}(x, y) = 0, \quad \sigma_{22}(x, y) \neq 0$$

consisting of two polynomial equations and one inequality. The polynomials σ_{11}, σ_{10} and σ_{22} are coefficients of the first and second polynomial subresultant of f and g. The inequality condition is exactly the condition of r having only simple self-intersections.

The overview of this work is as follows. In Chapter 2, we present the classical subdivision algorithm to determinate solutions of a bivariate system and we discuss its termination conditions in general. The algorithm used in this work bases on Krawczyk's criterion. In Chapter 3, we prove the equality of the affine variety V and the solution set of the system in terms of subresultants. We obtain a system of two equations in two indeterminates on which we can apply the subdivision algorithm. Chapter 4 addresses the termination conditions of the subdivision algorithm applied on our system to calculate the variety V. We conclude our work in Chapter 5. In the last chapter, we append the mathematical fundamentals and tools used in the previous chapters. We recall definitions and prove a great number of the theorems and propositions used in this work.

2 Numerical tools to solve bivariate systems

In this section, $f, g \in \mathbb{Q}[x, y]$ are two polynomials with rational coefficients. Let $F : \mathbb{R}^2 \to \mathbb{R}^2$ be the mapping which maps (x, y) to $(f(x, y), g(x, y))^T$ and let J_F denotes the Jacobian matrix of F. We are interested in all real solutions of the system $F(x, y) = 0$.

The idea is to use a subdivision algorithm meaning we start with a box

$$B = \left\{(x, y) \in \mathbb{R}^2 : \underline{B_1} \leq x \leq \overline{B_1}, \underline{B_2} \leq y \leq \overline{B_2}\right\}$$

denoted by $\left(\left[\underline{B_1}, \overline{B_1}\right], \left[\underline{B_2}, \overline{B_2}\right]\right)$ which will be recursively subdivided in a number of smaller boxes B_j until we know for sure that every box B_j either contains exactly one or no solution of $F(x, y) = 0$. For each box we have to check if weather (1) the box can't contain a solution or (2) there exists a unique solution in the box. If neither the first nor the second question can be answered, the given box will be subdivided in smaller boxes for which we will ask the same questions.

In the second section of this chapter, we define two criteria which answer the questions. First, we will give a short introduction to interval arithmetic and interval functions since working with box evaluation instead of set evaluating of functions is much more efficient. Also in the second section, we will present the classical subdivision algorithm based on the two criteria and afterwards, we will discuss the termination of the algorithm in general.

2.1 Interval arithmetic and interval polynomial functions

We follow the notation of interval vectors given in [MKC-2009] or [N-1990]. Elementary operations like $+, -, \cdot, /$ can be easily redefined as interval operations.

Definition 1. *Let $A = \left[\underline{A}, \overline{A}\right]$ and $B = \left[\underline{B}, \overline{B}\right]$ be two intervals in $\mathbb{R}$. Let $\circ$ be one of the following operations. Then we define the* ***sum*** *($\circ = +$), the* ***difference*** *($\circ = -$), the* ***product*** *($\circ = \cdot$) and the* ***quotient*** *($\circ = /$) of the intervals A and B as*

$$A \circ B = \{x \circ y : x \in A, y \in B\}$$

for respective $\circ$.
The quotient of A and B is restricted to the case $0 \notin B$.

Based on these definitions and restrictions, we easily obtain end point formulas for the arithmetic interval operations. For instance:

$$A + B = \left[\underline{A} + \underline{B}\ ,\ \overline{A} + \overline{B}\right],$$

$A - B = \left[\underline{A} - \overline{B}\ ,\ \overline{A} - \underline{B}\right]$ and

$A \cdot B = [\min S\ ,\ \max S]$ where $S := \{\underline{A}\underline{B}, \underline{A}\overline{B}, \overline{A}\underline{B}, \overline{A}\overline{B}\}$.

Now let $f : \mathbb{R}^n \to \mathbb{R}$ be a polynomial function and $U \subset \mathbb{R}^n$. Then we normally consider f as a set function, meaning $f(U) = \{f(x) : x \in U\}$. Anyhow, the calculation of the image set of U is mostly complex and in our situation unnecessary. Thus we want to regard f as interval function, meaning that we calculate only an interval containing the set $f(U)$. First, we extend the notation of an interval to the n-dimensional case.

Definition 2. *An **n-dimensional interval vector** or **box** is an ordered n-tuple of intervals*

$$(B_1, \ldots, B_n).$$

We denote boxes by capital letters $B = (B_1, \ldots, B_n)$ and intervals $B_i := \{x_i \in \mathbb{R} : \underline{B_i} \leq x_i \leq \overline{B_i}\}$ by $B_i = \left[\underline{B_i}, \overline{B_i}\right]$. We write $p := (X_{p1}, \ldots, X_{pn}) \in B = (B_1, \ldots, B_n)$ if $X_{pi} \in B_i$ for all $i \in [1, \ldots, n]$.

The elementary box operations are naturally component-wise defined as elementary interval operations. The **diameter** $\operatorname{diam}(B)$ of a box B is the largest diameter of the intervals $B_1, \ldots, B_n$. According to the end point formulas of intervals, we have the following estimates on the diameter of boxes.

Lemma 3. *Let A and B be boxes in $\mathbb{R}^n$, $m \in \mathbb{N}$ and $c \in \mathbb{R}$. Then*

(1) $\operatorname{diam}(A + B) \leq \operatorname{diam}(A) + \operatorname{diam}(B)$

(2) $\operatorname{diam}(c \cdot B) = |c| \cdot \operatorname{diam}(B)$

(3) $\operatorname{diam}(A \cdot B) \leq \max_{x \in B} |x| \cdot \operatorname{diam}(A) + \max_{y \in A} |y| \cdot \operatorname{diam}(B)$

(4) $\operatorname{diam}(B^m) \leq m \cdot \operatorname{diam}(B) \cdot (\max_{x \in B} |x|)^{m-1}$

Proof. (1) We have $\operatorname{diam}(I+J) = \operatorname{diam}(I)+\operatorname{diam}(J)$ for intervals $I, J \subset \mathbb{R}$. Since the addition of boxes is component-wise defined, we obtain $\operatorname{diam}(A+B) \leq \operatorname{diam}(A)+\operatorname{diam}(B)$ for boxes.

(2) Let $B = (B_1, \ldots, B_n)$. Then
$\operatorname{diam}(c \cdot B) = \max_{i \in \{1,\ldots,n\}} c \cdot \operatorname{diam}(B_i) = |c| \cdot \max_{i \in \{1,\ldots,n\}} \operatorname{diam}(B_i) = |c| \cdot \operatorname{diam}(B)$.

(3) Using the end point formula for intervals $I = \left[\underline{I}, \overline{I}\right], J = \left[\underline{J}, \overline{J}\right] \subset \mathbb{R}$, we obtain $I \cdot J = [st, uv]$ where s, u are suitable elements in $\left\{\underline{I}, \overline{I}\right\}$ and t, v are suitable elements in $\left\{\underline{J}, \overline{J}\right\}$. If $s = u$ or $t = v$ we have $\operatorname{diam}(I \cdot J) = |u| \cdot |v - t|$, resp. $\operatorname{diam}(I \cdot J) = |t| \cdot |u - s|$. If s, t, u, v are all different, we have $st \leq sv \leq uv$ thus $\operatorname{diam}(I \cdot J) = |s| \cdot |v - t| + |v| \cdot |u - s|$. Altogether we have $\operatorname{diam}(I \cdot J) \leq \max_{x \in J} |x| \cdot \operatorname{diam}(I) + \max_{y \in I} |y| \cdot \operatorname{diam}(J)$. Applying this result on the multidimensional case we obtain the above formula.

(4) Follows from (3) by induction.

□

Now we define the evaluation of functions by boxes.

Definition 4. *Let $f : \mathbb{R}^n \to \mathbb{R}$ be a polynomial function. Then we denote $\square f$ the map from boxes of $\mathbb{R}^n$ to intervals of R by replacing the elementary arithmetic operations and functions by the corresponding interval operations. We say that f is* ***evaluated by boxes****.*

There are several alternatives to evaluate a function by boxes. For example one technique to evaluate a polynomial $f \in \mathbb{R}[x_1, \ldots, x_n]$ by boxes is to evaluate per monomial.

Example. Let $f(x, y) = x^2 - y + xy \in \mathbb{R}[x, y]$ and let $B = ([1, 2], [1, 3]) \subset \mathbb{R}^2$. Then $\min_{(x,y)\in B} f = 1$ and $\max_{(x,y)\in B} = 7$ thus $f(B) \subset [1, 7]$.
If we evaluate f per monomial, we obtain $\square x^2(B) = [1, 4]$, $\square y(B) = [1, 3]$ and $\square xy(B) = [1, 6]$ thus $\square f(B) = [-1, 9]$. We see that $f(B) \subsetneqq \square f(B)$.
Now we additionally consider $g(x, y) = x^2 + y(x - 1)$. Mathematically f and g are equal, but when we evaluate g by boxes, we obtain $\square(x - 1)(B) = [0, 1]$ thus $\square(y(x - 1))(B) = [0, 3]$ and therefore $\square g(B) = [1, 7]$.

It turns out that the value of an interval function depends on the procedure of evaluating by boxes while the property $f(B) \subset \square f(B)$ is always verified. In the case of box evaluation per monomial, we have a linear dependence of $\operatorname{diam}(\square f(B))$ of the diameter of B.

Proposition 5. *Let $B \subset \mathbb{R}^2$ and $f \in \mathbb{R}[x, y]$. If $\square f$ is the evaluation of f per monomial, then*

$$\operatorname{diam}(\square f(B)) \leq d^3 |f_{\max}| \delta \cdot \operatorname{diam}(B)$$

where d is the degree of f, $f_{\max}$ is the coefficient of f with the largest absolute value and $\delta := \max\left\{1, \left(\max_{(x,y)\in B} \|(x, y)\|^{2d-1}\right)\right\}$.

Proof. Let $f(x, y) = \sum_{i+j\leq d} f_{ij} \cdot x^i y^j$ and $B = (B_1, B_2)$. We evaluate per monomial thus $\square f(B) = \sum_{i+j\leq d} f_{ij} \cdot B_1^i \cdot B_2^j$ and therefore by Lemma 3

$$\begin{aligned}
\operatorname{diam}(\square f(B)) &\leq \sum_{i+j\leq d} |f_{ij}| \cdot \operatorname{diam}(B_1^i \cdot B_2^j) \\
&\leq \sum_{i+j\leq d} |f_{ij}| \cdot \left(\max_{x\in B_1} |x|^i \operatorname{diam}(B_2^j) + \max_{y\in B_2} |y|^j \operatorname{diam}(B_1^i)\right) \\
&\leq \sum_{i+j\leq d} |f_{ij}| \cdot \left(j \max_{x\in B_1} |x|^i \max_{y\in B_2} |y|^{j-1} \operatorname{diam}(B_2) + i \max_{y\in B_2} |y|^j \max_{x\in B_1} |x|^{i-1} \operatorname{diam}(B_1^i)\right) \\
&\leq d \left(\max_{x\in B_1} |x| \cdot \operatorname{diam}(B_2) + \max_{y\in B_2} |y| \cdot \operatorname{diam}(B_1)\right) \cdot \sum_{i+j\leq d} |f_{ij}| \left(\max_{x\in B_1} |x|^{i-1} \max_{y\in B_2} |y|^{j-1}\right).
\end{aligned}$$

We take $\delta := \max\left\{1, \left(\max_{(x,y)\in B} \|(x,y)\|^{2d-1}\right)\right\}$. Then

$$\operatorname{diam}(\square f(B)) \leq d^3 \cdot \max_{i+j\leq d} |f_{ij}| \cdot \delta \cdot \operatorname{diam}(B)$$

□

2.2 Classical subdivision algorithm

We return to our problem which consists of finding all real solutions of $F(x,y) = 0$. The first criterion verifies the non-existence of zeros of F in a given box B.

Criterion 1. *Let B be a box in $\mathbb{R}^2$. If $\square f(B) \not\ni 0$ or $\square g(B) \not\ni 0$ then the system $F(x,y) = 0$ has no solution in B.*

Since $F(B) \subset f(B) \subset \square f(B)$ and $F(B) \subset g(B) \subset \square g(B)$ it is obvious that the criterion is true. The second criterion is based on the Newton-Krawczyk interval operator and ensures the existence of regular solutions of the equation $F(x,y) = 0$. A regular solution $(X,Y) \in \mathbb{R}^2$ is a solution of the system such that $\det(J_F(X,Y)) \neq 0$.

Criterion 2. *[MKC-2009, Theorems 8.2, 8.3] Let $B = (B_x, B_y)$ be a box in $\mathbb{R}^2$, $p_c = (X_c, Y_c)$ the center point of B and $\Delta B = (B_x - [X_c, X_c], B_y - [Y_c, Y_c])^T$ the box B translated in the origin. Let N be the mapping*

$$N(x,y) = \begin{pmatrix} x \\ y \end{pmatrix} - J_F^{-1}(p_c) \cdot F(x,y)$$

and K_F the Krawzcyk operator defined by

$$K_F(B) := N(p_c) + \square J_N(B) \cdot \Delta B.$$

If $K_F(B) \subset B$ then F has a unique regular solution in B.

The Krawczyk method first appeared in [K-1969, Section 8.2] in a monopolynomial version. Multipolynomial definitions can be found in [N-1990] and [MKC-2009, Theorems 8.2, 8.3] which ensure the convergence of the Krawczyk subdivision algorithm to a regular solution.

Now we can formulate the classical subdivision algorithm to isolate regular solutions of the system $F(x,y) = 0$ using these two criteria.

2.3 Termination of Krawczyk subdivision algorithm

First it is not clear that this algorithm will always terminate. The next proposition show that for boxes small enough containing a regular root of F, the Krawczyk criterion is always satisfied. For a box B_ϵ we denote by $B_{2\epsilon}$ the box with the same center as B_ϵ and the double diameter.

Algorithm 1 Krawczyk subdivision algorithm to isolate regular solutions

Input: $F = (f, g)$ a bivariate system with only regular solutions in a box B_0. K_F is the Krawczyk operator associated to F defined in Criterion 2.

Output: $L_{isolate}$ a list of boxes isolating the solutions

```
L := {B_0}
repeat
  B := L.pop
  if 0 ∉ F(B) (Criterion 1) then
    Discard B
  else
    if K_F(B) ⊂ B (Criterion 2) then
      Insert B in L_isolate
    else
      Subdivide B and insert its children in L
    end if
  end if
until L ≠ ∅
return L_isolate
```

Proposition 6. *Let (X, Y) be a regular root of F. There exists an $\eta > 0$ such that for every box B_ϵ of diameter smaller than η containing (X, Y), the box $B_{2\epsilon}$ satisfies:*

$$K_F(B_{2\epsilon}) \subset B_{2\epsilon}.$$

Proof. (X, Y) is a regular root of F, thus $F(X, Y) = 0$ and $J_F(X, Y)$ is invertible. Hence there exists $\eta > 0$ and $M > 0$ such that in every box B_η of diameter smaller than η which contains (X, Y) the coefficients of J_F are bounded by M.

Let $B_{\epsilon_1} \subset B_\eta$ be a box of diameter less than ϵ_1 with center point p_{c_1} which contains (X, Y). Then, using the Taylor remainder theorem at p_c, we have:

$$\begin{aligned} N(X,Y) &= N(p_{c_1}) + J_N(p_{c_1}) \cdot ((X,Y) - p_{c_1}) + O(\epsilon_1^2) \\ &= N(p_{c_1}) + (\mathbb{1} - J_F(p_{c_1})^{-1} J_F(p_{c_1})) \cdot ((X,Y) - p_{c_1}) + O(\epsilon_1^2) \\ &= N(p_{c_1}) + O(\epsilon_1^2). \end{aligned}$$

Furthermore, $N(X, Y) = (X, Y)^T - J_F^{-1}(p_{c_1}) \cdot F(X, Y) = (X, Y)^T$.
Hence there exists ξ_1 such that $|N(p_c) - (X, Y)^T| < \xi_1 \epsilon^2$ for all (X, Y) containing boxes $B_\epsilon \subset B_\eta$

with respective center point.

We recall that $B_{2\epsilon}$ denotes the box with the same center point as B_ϵ and double diameter. By Proposition 5 and retaining there given notations, there exists ξ_2 depending on $\deg(F)$, $F_{\max}$ and $\delta(B_\eta$ such that $\operatorname{diam}(\square J_N(B_{2\epsilon})) < \xi_2 \cdot \operatorname{diam}(B_{2\epsilon}) = \xi_2 \cdot 2\epsilon$ for all boxes $B_\epsilon \subset B_\eta$. By taking δ of the input box B_0 of the algorithm instead of $\delta(B_\eta)$, we can regard ξ_2 as a constant.
Since $p_c \in B_\epsilon \subset B_{2\epsilon}$ and $J_N(p_c) = 0$, we have $0 \in \square J_N(B_{2\epsilon})$ thus $\square J_N(B_{2\epsilon}) \subset [-\xi_2 \cdot 2\epsilon\,,\, \xi_2 \cdot 2\epsilon]^2$. As in the criterion de Krawczyk, we denote $\Delta B_{2\epsilon} = [-2\epsilon, 2\epsilon]^2$ the box $B_{2\epsilon}$ translated into the origin. Then $\square J_N(B_{2\epsilon}) \cdot \Delta B_{2\epsilon} \subset [-\xi_2 \cdot 4\epsilon^2\,,\, \xi_2 \cdot 4\epsilon^2]^2$.

We take $\xi := \xi_1 + 4\xi_2$. Then $N(p_c) - (X,Y)^T + \square J_N(B_{2\epsilon}) \cdot \Delta B_{2\epsilon} \subset [-\xi\epsilon^2, \xi\epsilon^2]$ and therefore

$$K_F(B_{2\epsilon}) = N(p_c) + \square J_N(B_{2\epsilon}) \cdot \Delta B_{2\epsilon} \subset (X,Y)^T + [-\xi\epsilon^2\,,\, \xi\epsilon^2]^2.$$

For $\epsilon < \xi$ we have $(X,Y)^T + [-\xi\epsilon^2\,,\, \xi\epsilon^2]^2 \subset B_{2\epsilon}$, thus $K_F(B_{2\epsilon}) \subset B_{2\epsilon}$. □

Due to the previous theorem, we can separate all regular solutions by disjoint isolating boxes as long as they don't lie on the boundary of the obtaining boxes. For solutions of the boundary we have to modify the subdivision algorithm, for example by changing the procedure of subdividing the boxes.
Now we will prove that the first criterion is always satisfied for boxes small enough containing no root of F.

Proposition 7. *Let $B \subset \mathbb{R}^2$ be a box containing no solution of $F(x,y) = 0$. Then there exists some $\eta > 0$ such that for every box $B_\eta \subset B$ of diameter less than η the first criterion is satisfied.*

Proof. Let $A := F(B)$ denotes the image of B which is also a box in $\mathbb{R}^2$. Then $A \subset \mathbb{R}_{>0}$ or $A \subset \mathbb{R}_{<0}$ and we take ζ the distance of A to the origin. By Lemma 3 we have $\operatorname{diam}(\square f(B)) \leq \xi \operatorname{diam}(B)$ for ξ depending on the polynomial F and the input box B_0 of the subdivision algorithm. Thus we can consider ξ as constant.
Now let $B_\epsilon \subset B$ be box of diameter less than ϵ. Then $\operatorname{diam}(\square f(B)) < \xi\epsilon$. We set $\eta := \frac{\zeta}{\xi}$. For every $\epsilon < \eta$ we have $\square f(B_\epsilon) \subset A + [-\xi\epsilon, \xi\epsilon]^2 \subset \big(A + [-\zeta, \zeta]^2\big) \setminus \{0\}$. Thus $0 \notin \square f(B_\epsilon)$ and hence the first criterion is satisfied for all boxes $B_\eta \subset B$ with diameter less than η. □

Given a box B of the real plane containing only regular solutions of $F(x,y) = 0$, by the previous Propositions 6 and 7, the subdivision algorithm will always terminate and enclose all the regular solutions of $F(x,y) = 0$ with disjoint isolating boxes.

3 Singularities of the resultant in terms of subresultants

In this chapter, we consider two polynomials $f, g \in \mathbb{Q}[x,y][z]$ as polynomials in z with coefficients in $\mathbb{A} := \mathbb{Q}[x,y]$ which is an integer domain. We write d_1 for the degree of f and d_2 for the degree of g both relative to z and we write f_{d_1} resp. g_{d_2} for their leading coefficients.
We set $r := \mathrm{Res}_z(f,g)$ the resultant of f and g and we write Sres_i for $\mathrm{Sres}_i(f,g)$ and σ_{ij} for $\sigma_{ij}(f,g)$ (see Chapter 6.2 for the definition and properties of the resultant and subresultants). To describe the topology of the curve r, we are interested in its singular point set which is given by

$$V := \{(x,y) \in \mathbb{C}^2 : r(x,y) = 0, \partial_x r(x,y) = 0, \partial_y r(x,y) = 0\} = \mathbf{V}(r, \partial_x r, \partial_y r).$$

Since this system consists of three equations in only two indeterminates it is not possible to apply the subdivision algorithm of the previous chapter directly to calculate this solution set. The aim of this chapter is to transform our system into a system with one less equation to allow the application of the presented subdivision algorithm. Our aim is to show the equality of V and the point set

$$W := \{(x,y) \in \mathbb{C}^2 : \sigma_{11}(x,y) = 0, \sigma_{10}(x,y) = 0, \sigma_{22}(x,y) \neq 0\} = \mathbf{V}(\sigma_{11}, \sigma_{10}) - \mathbf{V}(\sigma_{22})$$

which gives a system of two equations in two variables and one inequality. This system satisfies the formal conditions of algorithm 1 with an additional inequality condition.
If V verifies the three following basic preconditions, we can prove the coincidence of V and W:

Conditions.

$(*1)$ $\mathbf{V}(f_{d_1}, g_{d_2}) = \emptyset$.

$(*2)$ $\sigma_{22}(x,y) \neq 0$ for all $(x,y) \in \mathbf{V}(r, \partial_x r, \partial_y r)$.

$(*3)$ $\mathbf{V}(f) \cap \mathbf{V}(g)$ consists of only regular points.

Theorem 8. *Let $f, g \in \mathbb{Q}[x,y][z]$ polynomials in z with coefficients in $\mathbb{A} := \mathbb{Q}[x,y]$. We write d_1 for the degree of f and d_2 for the degree of g both relative to z and f_{d_1} resp. g_{d_2} for their leading coefficients. Let $r := \mathrm{Res}_z(f,g)$ be the resultant of f and g and let $\mathrm{Sres}_i = \mathrm{Sres}_i(f,g)$, $\sigma_{ij} = \sigma_{ij}(f,g)$ be the respective subresultants. Then*

(1) *$W \subset V$ and*

(2) *if additionally $(*1)$ to $(*3)$ are satisfied then $V \subset W$.*

The conditions $(*1)$ to $(*3)$ have natural geometrical interpretations and reasons. The first condition, $\mathbf{V}(f_{d_1}, g_{d_2}) = \emptyset$, is the assumption of Theorem 44 which says that the resultant of two polynomials f and g is the projection of the intersection of their varieties: $\mathbf{V}(\mathrm{Res}_z(f,g)) = \mathrm{proj}_{z=0}(\mathbf{V}(f) \cap \mathbf{V}(g)) = \mathrm{proj}_{z=0}(\mathbf{V}(f,g))$. This is exactly the assumption made in the first chapter and it is in fact equivalent to the requirement of f and g having no common point at infinity in the z-direction.
The second condition, $\sigma_{22}(X,Y) \neq 0$, for all $(X,Y) \in \mathbf{V}(r)$ implies that there exists at most two points in the intersection of $\mathbf{V}(f)$ and $\mathbf{V}(g)$ over every point (X,Y) of the curve r. This property is clear for regular points of the curve r, $(*2)$ guarantees this property also for the singular points of r. Hence we only consider singular curves whose singular points are intersection points of at least two curve segments (simple self-intersections). The third condition, $\mathbf{V}(f) \cap \mathbf{V}(g)$, consists of only regular points implies that the curve has a well-defined tangent in each of its points $(X,Y,Z) \in \mathbf{V}(f) \cap \mathbf{V}(g)$. We denote $F(x,y,z) = (f(x,y,z), g(x,y,z))^T$. A regular point of $\mathbf{V}(f) \cap \mathbf{V}(g)$, or in other words a regular solution of the system $F(x,y,z) = 0$, is a point $(X,Y,Z) \in \mathbf{V}(f) \cap \mathbf{V}(g)$ such that at least one of the three (2×2) minors of the Jacobien matrix of F does not vanish on (X,Y,Z). Then in each point $(X,Y,Z) \in \mathbf{V}(f) \cap \mathbf{V}(g)$ the tangent $t_{f \cap g}$ of the curve is well-defined as the cross product of the gradient vectors of f and g. In fact this third condition is equivalent to $\nabla(f)$ and $\nabla(g)$ are not parallel.

Now we turn to the proof of Theorem 8 which will be done in two steps.

3.1 Proof of the first inclusion $W \subset V$

The idea of the proof is to use the ideal–variety–correspondence (see Appendix, Theorem 38). Let I denotes the ideal $\langle r, \partial_x r, \partial_y r \rangle \subset \mathbb{A}$, then we have $V = \mathbf{V}(I)$. Due to Proposition 40 we can define an ideal corresponding to the smallest affine variety containing W: let J be the ideal $\langle \sigma_{11}, \sigma_{10} \rangle : \langle \sigma_{22} \rangle^{\infty} \subset \mathbb{A}$ then $\mathbf{V}(J) = \overline{\mathbf{V}(\sigma_{11}, \sigma_{10}) - \mathbf{V}(\sigma_{22})} = \overline{W} \supset W$ by Proposition 40. The aim of this section is to prove $I \subset J$, meaning we have to prove the existence of an integer $m > 0$ such that $\langle r, \partial_x r, \partial_y r \rangle \cdot \langle \sigma_{22} \rangle^m \subset \langle \sigma_{11}, \sigma_{10} \rangle$.
Additionally we can write $\langle r, \partial_x r, \partial_y r \rangle \cdot \langle \sigma_{22} \rangle^m$ as $\langle r{\sigma_{22}}^m, \partial_x r{\sigma_{22}}^m, \partial_y r{\sigma_{22}}^m \rangle$. Hence it remains to show the inclusion $\{r{\sigma_{22}}^m, \partial_x r{\sigma_{22}}^m, \partial_y r{\sigma_{22}}^m\} \subset \langle \sigma_{11}, \sigma_{10} \rangle$ for some particular m.

The proof of this property can be seen as a corollary of Theorem 4.1 in [K-2003] which is known as Habicht theorem (see [H-1948]). We present this theorem only in the particular case which will be used in this work (meaning part (ii) of the theorem by taking $j = 0$ and $i = 1$).

Lemma 9. *[K-2003, Theorem 4.1] We assume the coefficients of f and g as indeterminates and*

let $\mathbb{A}$ be the ring generated by these coefficients. Then for $f, g \in \mathbb{A}[z]$ two polynomials of degrees $d_1 \geq d_2$ and $d_1 \geq 3$ we have

$$\sigma_{22}{}^2 \cdot r = \mathrm{Res}(\mathrm{Sres}_2, \mathrm{Sres}_1).$$

□

Corollary 10. *$\sigma_{22}{}^2 \cdot r \in \langle \sigma_{10}, \sigma_{11} \rangle$ if $d_1 \geq d_2$ and $d_1 \geq 3$.*

Proof. The polynomial subresultants of f and g are given by $\mathrm{Sres}_1 = \sigma_{11} z + \sigma_{10}$ and $\mathrm{Sres}_2 = \sigma_{22} z^2 + \sigma_{21} z + \sigma_{20}$. Thus

$$\mathrm{Res}(\mathrm{Sres}_2, \mathrm{Sres}_1) = \begin{vmatrix} \sigma_{22} & \sigma_{11} & \\ \sigma_{21} & \sigma_{10} & \sigma_{11} \\ \sigma_{20} & & \sigma_{10} \end{vmatrix} = \sigma_{10}{}^2 \sigma_{22} + \sigma_{11}{}^2 \sigma_{20} - \sigma_{10}\sigma_{11}\sigma_{21} \in \mathbb{A}$$

which is in $\langle \sigma_{10}, \sigma_{11} \rangle_{\mathbb{A}}$. □

Using this corollary, we can prove the existence of some m such that $\{\partial_x r \sigma_{22}{}^m, \partial_y r \sigma_{22}{}^m\} \subset \langle \sigma_{11}, \sigma_{10} \rangle$

Lemma 11. *If $d_1 \geq d_2$, $d_1 \geq 3$ then $\sigma_{22}{}^3 \cdot \partial_x r$ and $\sigma_{22}{}^3 \cdot \partial_y r$ are elements $\langle \sigma_{10}, \sigma_{11} \rangle_{\mathbb{A}}$.*

Proof. We argument for $\sigma_{22}{}^3 \cdot \partial_x r$, but the other membership holds analogously.
By the proof of the previous corollary, we can write $\sigma_{22}{}^2 \cdot r$ as an element in $(\langle \sigma_{10}, \sigma_{11} \rangle_{\mathbb{A}})^2$: $\sigma_{22}{}^2 \cdot r = \alpha \sigma_{10}{}^2 + \beta \sigma_{10}\sigma_{11} + \gamma \sigma_{11}{}^2$ with $\alpha, \beta, \gamma \in \mathbb{A}$. Hence

$$\begin{aligned} \partial_x(\sigma_{22}{}^3 r) &= \partial_x((\alpha \sigma_{10}{}^2 + \beta \sigma_{10}\sigma_{11} + \gamma \sigma_{11}{}^2)\sigma_{22}) \\ &= \partial_x(\alpha \sigma_{10}{}^2 \sigma_{22}) + \partial_x(\beta \sigma_{10}\sigma_{11}\sigma_{22}) + \partial_x(\gamma \sigma_{11}{}^2 \sigma_{22}) \\ &= 2\sigma_{10}\partial_x\sigma_{10}\alpha\sigma_{22} + \sigma_{10}{}^2 \partial_x(\alpha\sigma_{22}) \\ &\quad + \sigma_{10}\partial_x\sigma_{11}\alpha\sigma_{22} + \sigma_{11}\partial_x\sigma_{10}\alpha\sigma_{22} + \sigma_{10}\sigma_{11}\partial_x(\alpha\sigma_{22}) \\ &\quad + 2\sigma_{11}\partial_x\sigma_{11}\alpha\sigma_{22} + \sigma_{11}{}^2\partial_x(\alpha\sigma_{22}) \\ &= \sigma_{10}\diamondsuit_1 + \sigma_{11}\diamondsuit_2 + \sigma_{10}\sigma_{11}\diamondsuit_3 \end{aligned}$$

with $\diamondsuit_1, \diamondsuit_2, \diamondsuit_3$ coefficients in $\mathbb{A}$. On the other hand we have

$$\begin{aligned} \partial_x(\sigma_{22}{}^3 r) &= 3\sigma_{22}{}^2 \partial_x \sigma_{22} r + \sigma_{22}{}^3 \partial_x r \\ &= 3\partial_x\sigma_{22}(\alpha\sigma_{10}{}^2 + \beta\sigma_{10}\sigma_{11} + \gamma\sigma_{11}{}^2) + \sigma_{22}{}^3\partial_x r \end{aligned}$$

by Corollary 10. Thus

$$\sigma_{22}{}^3 \partial_x r = \sigma_{10}(\diamondsuit_1 - 3\alpha\sigma_{10}\partial_x\sigma_{22}) + \sigma_{11}(\diamondsuit_2 - 3\gamma\sigma_{11}\partial_x\sigma_{22}) + \sigma_{10}\sigma_{11}(\diamondsuit_3 - 3\beta\partial_x\sigma_{22})$$

is contained in $\langle \sigma_{10}, \sigma_{11} \rangle_{\mathbb{A}}$. □

We can conclude $\{r{\sigma_{22}}^2, \partial_x r{\sigma_{22}}^3, \partial_y r{\sigma_{22}}^3\} \subset \langle \sigma_{11}, \sigma_{10} \rangle$ for polynomials of degrees $d_1 \geq d_2$, $d_1 \geq 3$, which implies $\langle r, \partial_x r, \partial_y r \rangle \cdot \langle \sigma_{22} \rangle^3 \subset \langle \sigma_{11}, \sigma_{10} \rangle$. Finally, the conditions on the degrees don't constrain the generality of the results: For $d_1 < d_2$ the resultant of f and g differs at most in some factor (-1) and for $d_1 < 3$ the scalar subresultant σ_{22} is equal to zero and therefore the inclusion is hold.
Hence $I \subset J$ which implies $W \subset \overline{W} \subset V$.

3.2 Proof of the second inclusion $V \subset W$

We recall that we require conditions $(*1)$ to $(*3)$ to prove this inclusion.
Let $(X, Y) \in V$, thus $r(X, Y) = \partial_x r(X, Y) = \partial_y r(X, Y) = 0$. Since $\sigma_{22}(x, y) \neq 0$ for all $(x, y) \in V$ by condition $(*2)$ it remains to show $\sigma_{11}(X, Y) = \sigma_{10}(X, Y) = 0$. If we consider $\sigma_{11}(X, Y) = 0$ the equality $\sigma_{10}(X, Y) = 0$ is an corollary of the gap structure theorem (Theorem 46).

Lemma 12. *For $(X, Y) \in \mathbb{A}$ such that $r(X, Y) = \sigma_{11}(X, Y) = 0$ it follows immediately that $\sigma_{10}(X, Y) = 0$.*

Proof. We fix $(X, Y) \in \mathbb{A}$ such that $r(X, Y) = \sigma_{11}(X, Y) = 0$ and consider f and g and their polynomial subresultants in $\mathbb{A}[z]$. It follows from the gap structure theorem that the minimal non-zero polynomial subresultant Sres_m of f and g has to be regular and subresultants of smaller degree identically vanish. Since $\mathrm{Sres}_0 = \mathrm{Res} = 0$ and $\sigma_{11} = 0$ and thus $\deg \mathrm{Sres}_1 < 1$, it follows $m \geq 2$. Thus $\sigma_{10} = 0$. □

Now we prove $\sigma_{11}(X, Y) = 0$ for which we use the tangent to the curve $\mathbf{V}(f) \cap \mathbf{V}(g)$. We denote by $\nabla f, \nabla g$ the gradient of f resp. g and we denote $t_{f \cap g} := \nabla f \times \nabla g$ the tangent to $\mathbf{V}(f) \cap \mathbf{V}(g)$ which exists by hypothesis $(*3)$. By hypothesis $(*1)$, there exists at least one (and by hypotheses $(*2)$ at most two) $Z \in \mathbb{C}$ such that $(X, Y, Z) \in \mathbf{V}(f, g)$. We distinguish two cases:

(1) $\mathbf{V}(f) \cap \mathbf{V}(g)$ has a non vertical tangent in (X, Y, Z) or

(2) $t_{f \cap g}(X, Y, Z)$ is vertical, meaning $t_{f \cap g}(X, Y, Z) \| (0, 0, 1)^T$.

To prove the equation in the first case we use theorem 5.1 of [BM-2007]. We will give a formulation in affine case while the author's version was in homogeneous case.

Lemma 13. *[BM-2007, Theorem 5.1] Let f_1 and f_2 be two polynomials of degrees d_1, resp d_2 in x and z with coefficients in an integer domain $\mathbb{A}_1$. Then we have in $\mathbb{A}_1[x]$:*

$$\partial_x \mathrm{Res}_z(f_1, f_2) = (-1)^{d_1+d_2} \begin{vmatrix} \partial_x f_1 & \partial_z f_1 \\ \partial_x f_2 & \partial_z f_2 \end{vmatrix} \sigma_{11} \mod \langle f_1, f_2 \rangle.$$

□

Corollary 14. *Let* $(X,Y) \in \mathbf{V}(r,\partial_x r,\partial_y r)$ *and* $Z \in \mathbb{C}$ *such that* $(X,Y,Z) \in \mathbf{V}(f,g)$ *and* $t_{f\cap g}(X,Y,Z)$ *not vertical. Then* $\sigma_{11}(X,Y) = 0$.

Proof. For every function h we write $\widehat{h}$ for the value of h at (X,Y,Z). Since

$$t_{f\cap g}(X,Y,Z) = \begin{pmatrix} \widehat{\partial_y f}\widehat{\partial_z g} - \widehat{\partial_z f}\widehat{\partial_y g} \\ \widehat{\partial_z f}\widehat{\partial_x g} - \widehat{\partial_x f}\widehat{\partial_z g} \\ \widehat{\partial_x f}\widehat{\partial_y g} - \widehat{\partial_y f}\widehat{\partial_x g} \end{pmatrix}$$

is not vertical, one of the first two components is not zero. W.l.o.g. let $\widehat{\partial_y f}\widehat{\partial_z g} - \widehat{\partial_z f}\widehat{\partial_y g} \neq 0$. By Lemma 13 we have

$$\partial_y r = (-1)^{d_1+d_2}\begin{vmatrix} \partial_y f & \partial_z f \\ \partial_y g & \partial_z g \end{vmatrix}\sigma_{11} + \alpha f + \beta g$$

for some polynomials $\alpha, \beta \in \mathbb{C}[x][y]$. If we apply this on (X,Y,Z) we obtain

$$\begin{aligned} \widehat{\partial_y r} &= (-1)^{d_1+d_2}(\widehat{\partial_y f}\widehat{\partial_z g} - \widehat{\partial_z f}\widehat{\partial_y g})\cdot\widehat{\sigma_{11}} + \widehat{\alpha}\widehat{f} + \widehat{\beta}\widehat{g} \\ &= (-1)^{d_1+d_2}(\widehat{\partial_y f}\widehat{\partial_z g} - \widehat{\partial_z f}\widehat{\partial_y g})\cdot\widehat{\sigma_{11}} \end{aligned}$$

which is zero since $(X,Y,Z) \in \mathbf{V}(r,\partial_x r,\partial_y r)$. Thus $\sigma_{11}(X,Y,Z) = 0$. □

This proof only works in the case of a non vertical tangent. If $t_{f\cap g}$ is parallel to the z-axis, we need the following lemma.

Proposition 15. *[K-2003, Lemma 3.1] Let* $(X,Y) \in \mathbb{C}^2$ *and* $\mathbb{A} = \mathbb{C}[x,y]$. *For* $h \in \mathbb{A}[z]$, *we denote* $h_* := h(X,Y,\cdot)$. *Let* $(*1)$ be satisfied, thus w.l.o.g. $f_{d_1*} \neq 0$ and $\deg f_* = \deg f = d_1$. Let $t := \deg g_*$. Then $(\mathrm{Sres}_i(f,g))_* = f_{d_1*}^{d_2-t}\mathrm{Sres}_i(f_*,g_*)$ for all $i \leq \deg t$. □

Now we can address us to the proof of the second case.

Lemma 16. *Let* $(X,Y,Z) \in \mathbf{V}(f,g)$ *such that* $(X,Y) \in \mathbf{V}(r,\partial_x r,\partial_y r)$ *and* $t_{f\cap g}$ *is vertical. Then* $\sigma_{11}(f,g)(X,Y) = 0$.

Proof. Using the notation in the proof of Proposition 14, we have

$$t_{f\cap g}(X,Y,Z) = \begin{pmatrix} \widehat{\partial_y f}\widehat{\partial_z g} - \widehat{\partial_z f}\widehat{\partial_y g} \\ \widehat{\partial_z f}\widehat{\partial_x g} - \widehat{\partial_x f}\widehat{\partial_z g} \\ \widehat{\partial_x f}\widehat{\partial_y g} - \widehat{\partial_y f}\widehat{\partial_x g} \end{pmatrix} = \begin{matrix} 0 \\ 0 \\ \neq 0 \end{matrix}$$

We consider two cases:

(1) One of the both $\widehat{\partial_z f}$ and $\widehat{\partial_z g}$, is not zero.
Let $\widehat{\partial_z g} \neq 0$. Then we can divide by $\widehat{\partial_z g}$ and obtain $\widehat{\partial_y f} = \frac{\widehat{\partial_z f}\widehat{\partial_y g}}{\widehat{\partial_z g}}$ and $\widehat{\partial_x f} = \frac{\widehat{\partial_z f}\widehat{\partial_x g}}{\widehat{\partial_z g}}$. But then $\widehat{\partial_x f}\widehat{\partial_y g} = \widehat{\partial_y f}\widehat{\partial_x g}$ which contradicts the inequality.

(2) $\widehat{\partial_z f} = 0$ and $\widehat{\partial_z g} = 0$.
Let $h = h_d z^d + \cdots + h_0$ be a polynomial in $\mathbb{C}[x,y][z]$, meaning $h_i \in \mathbb{C}[x,y]$ for all $i \in \{0,\ldots,d\}$. We write h_* for $h(X,Y,\cdot)$ as in Proposition 15 and h' for $\partial_z h$. Then

$$\begin{aligned}(h')_* &= (d \cdot h_d z^{d-1} + \cdots + h_1)(X,Y,\cdot) \\ &= d \cdot h_d(X,Y) \cdot z^{d-1} + \cdots + h_1(X,Y) \\ &= (h_d(X,Y) \cdot z^d + \cdots + h_1(X,Y)z + h_0(X,Y))' = (h_*)'.\end{aligned}$$

Since $(X,Y,Z) \in \mathbf{V}(f,g,\partial_z f,\partial_z g)$ we have $Z \in \mathbf{V}(f_*,g_*,(f')_*,(g')_*)$ which implies $(z-Z)$ divides f_*, g_*, $(f')_* = (f_*)'$ and $(g')_* = (g_*)'$.
We obtain $\deg(\gcd(f_*,g_*)) \geq \mathrm{mult}_Z(\gcd(f_*,g_*)) \geq 2$ and hence $\sigma_{11}(f_*,g_*) = 0$ by Theorem 47. By Proposition 15 we have $\sigma_{11}(f,g)(X,Y) = \diamondsuit \cdot \sigma_{11}(f_*,g_*) = 0$ for some factor $\diamondsuit \in \mathbb{C}$. Thus $\sigma_{11}[f,g](X,Y) = 0$.

□

By Corollary 14 and Lemma 16 we have $\sigma_{11}(X,Y) = 0$ and Lemma 12 implies $\sigma_{10}(X,Y) = 0$. Thus $V \subset W$ which concludes the proof of Theorem 8, (2).

4 Krawczyk termination conditions for the transformed system

In this chapter, we discuss the termination conditions of the subdivision algorithm of Chapter 2 on our transformed system of Chapter 3. Thus we assume the conditions $(*1)$ to $(*3)$ to be satisfied. We keep the notation of the preceding chapter, thus we consider two hypersurfaces in $\mathbb{R}^3$ given as the zero set of two polynomials $f, g \in \mathbb{Q}[x, y, z]$. Let r be the projection of the intersection of these hypersurfaces which is the resultant $\mathrm{Res}_z(f, g)$ by Theorem 44. As before we denote $V = \mathbf{V}(r, \partial_x r, \partial_y r)$ the set of singularities of r. In Chapter 3, we proved that under conditions $(*1)$ to $(*3)$ the set of all complex solutions of the system

$$\sigma_{11}(x, y) = 0, \quad \sigma_{10}(x, y) = 0, \quad \sigma_{22}(x, y) \neq 0$$

is exactly the set of complex solutions of

$$r(x, y) = 0, \quad \partial_x r(x, y) = 0, \quad \partial_y r(x, y) = 0$$

hence the real solutions of the two systems also coincide. Thus we want to apply the classical subdivision algorithm of the previous section to the system

$$\sigma_{11}(x, y) = 0, \quad \sigma_{10}(x, y) = 0.$$

Because of the additional inequality, we have to modify our algorithm to check in the end if σ_{22} does not vanish in the calculated solution containing isolation boxes, see the remarks in the end of this chapter.
Since the algorithm only recognizes regular solutions, we will show in this chapter that generically our system of equations has only regular solutions. The proof will be done in three steps:

(1) We first show that $\mathrm{mult}^{\cap}_{(X,Y)}(r, \partial_x r, \partial_y r) = 1$ for all $(X, Y) \in \mathbf{V}(r, \partial_x r, \partial_y r)$, which

(2) implies $\mathrm{mult}^{\cap}_{(X,Y)}(\sigma_{11}, \sigma_{10}) = 1$ for all $(X, Y) \in \mathbf{V}(r, \partial_x r, \partial_y r) = \mathbf{V}(\sigma_{11}, \sigma_{10})$.

(3) We further show that for $f_1, \ldots, f_n \in \mathbb{R}[x_1, \ldots, x_n]$ and $(X_1, \ldots, X_n) \in \mathbf{V}(f_1, \ldots, f_n) \cap \mathbb{R}^n$ such that $\mathrm{mult}^{\cap}_{(X_1,\ldots,X_n)}(f_1, \ldots, f_n) = 1$ the Jacobien $\det J_F(X_1, \ldots, X_n)$ does not vanish (here $F = (f_1, \ldots, f_n)$).

For the first two steps, we will work over the field of complex numbers before we return to only real solutions in the third step. This last step is a known fact which we recall here for the sake of completeness. The focus in this section is on the first step.

4.1 All points in the variety V have intersection multiplicity one in $\langle r, \partial_x r, \partial_y r\rangle$

The intersection multiplicity is only defined for zero-dimensional ideals. Thus our ideal $\langle r, \partial_x r, \partial_y r\rangle$ has to be zero-dimensional. The idea of the proof is to use Teissier's formula which was first mentioned by Teissier in [T-1973, Chapter II, Theorem 5].

Theorem 17. *[BR-1990, Lemma D.3.4] Let $r \in \mathbb{C}[x, y]$. For an x-critical point (X, Y) of $\mathbf{V}(r)$ (meaning $\partial_y r(X, Y) = 0$) it holds that*

$$\mathrm{mult}_Y(r(X, y)) = \mathrm{mult}^{\cap}_{(X,Y)}(r, \partial_y r) - \mathrm{mult}^{\cap}_{(X,Y)}(\partial_x r, \partial_y r) + 1.$$

□

This formula allows us to calculate intersection multiplicities by calculating (intersection) multiplicities for easier ideals. These multiplicities are only defined for ideals satisfying the following additional conditions.

Conditions.

(∗4) $\langle \partial_x r, \partial_y r\rangle$ is zero dimensional.

(∗5) $\langle r, \partial_x r\rangle$ or $\langle r, \partial_y r\rangle$ is zero dimensional.

The fourth condition, $\langle \partial_x r, \partial_y r\rangle$ is zero-dimensional, is the assumption of the well-definedness of the intersection multiplicity $\mathrm{mult}^{\cap}_{(X,Y)}(\partial_x r, \partial_y r)$. Furthermore, the finiteness of the dimension of the ideal $\mathbb{R}[x, y]_{\langle x-X, y-Y\rangle}/\langle \partial_x r, \partial_y r\rangle \mathbb{R}[x, y]_{\langle x-X, y-Y\rangle}$ already implies the finiteness of the dimension of the ideal $\mathbb{R}[x, y]_{\langle x-X, y-Y\rangle}/\langle r, \partial_x r, \partial_y r\rangle \mathbb{R}[x, y]_{\langle x-X, y-Y\rangle}$. Thus $\langle r, \partial_x r, \partial_y r\rangle$ is a zero-dimensional ideal and $\mathrm{mult}^{\cap}_{(X,Y)}(r, \partial_x r, \partial_y r) \leq \mathrm{mult}^{\cap}_{(X,Y)}(\partial_x r, \partial_y r)$ is well-defined.
The last condition, $\langle r, \partial_x r\rangle$ or $\langle r, \partial_y r\rangle$ is zero dimensional, is needed for $\mathrm{mult}^{\cap}_{(X,Y)}(r, \partial_x r)$ resp. $\mathrm{mult}^{\cap}_{(X,Y)}(r, \partial_y r)$ to be well-defined. Here we suppose $\langle r, \partial_x r\rangle$ to be zero dimensional. It follows directly that r and $\partial_x r$ have no common factor and hence r has to be square-free which can be proved by contraposition: If we consider r_1 as a common factor of r and $\partial_x r$, we can write $r = r_1 \cdot \diamondsuit_1$ and $\partial_x r = r_1 \cdot \diamondsuit_2$ with $r_1 \in \mathbb{R}[x, y]$ of degree at least 1. But then $\mathbf{V}(r_1) \subset \mathbf{V}(r, \partial_x r)$ which is of dimension at least 1 which contradicts $\langle r, \partial_x r\rangle$ to be zero dimensional.

We first mention three further formulas which will be used in the proof. The first one is a combination of two theorems in [BM-2007]. We will formulate the statement in affine notation while the authors originally gave a homogeneous formulation.

Lemma 18. *[BM-2007, Proposition 5.4, Theorem 5.6] Let $\mathbb{U}$ denotes the universal ring of coefficients of two polynomials of degrees d_1, resp. d_2. Let $f_1, f_2 \in \mathbb{U}[y, z]$ be two polynomials of*

degrees d_1 resp. d_2 in y and z. Then

$$\mathrm{Res}_y(\mathrm{Res}_z(f_1,f_2),\partial_y\mathrm{Res}_z(f_1,f_2)) = \pm\diamondsuit_1\cdot\diamondsuit_2^2$$

where $\diamondsuit_1,\diamondsuit_2$ are irreducible polynomials in $\mathbb{U}$. Furthermore the bi-degrees of $\diamondsuit_1$ and $\diamondsuit_2$ with respect to the coefficients of the polynomials f_1 and f_2 are $(2d_2d_1+d_2^2-3d_2, 2d_1d_2+d_1^2-3d_1)$ for $\diamondsuit_1$ and $(2d_2^2d_1-2d_2d_1-d_2^2+d_2, 2d_1^2d_2-2d_1d_2-d_1^2+d_1)$ for $\diamondsuit_2$. □

The next two formulas handle multiresultants, we formulate them in affine situation. The first one connects multiresultants and intersection multiplicities, the second one gives a restatement of the preceding multiresultant. We write $\mathrm{Res}_{d_1,\ldots,d_n}^{x_n=u_0}(f_1,\ldots,f_n)$ for the affine multipolynomial resultant of the polynomials $f_1,\ldots,f_n$ in variables $x_1,\ldots,x_{n-1}$ by taking $x_n=u_0$ as a constant.

Proposition 19. *[CLO2-2000, Chapter 4, Proposition 2.8] Let $\mathbb{F}$ be algebraically closed, let $f_1,\ldots,f_n\in\mathbb{F}[x_1,\ldots,x_n]$ have total degrees at most $d_1,\ldots,d_n$ and no solution at ∞. If $f_0 = u_0+u_1x_1+\cdots+u_nx_n$, where $u_0,\ldots,u_n$ are independent variables, then there is a nonzero constant C such that*

$$\mathrm{Res}_{1,d_1,\ldots,d_n}(f_0,\ldots,f_n) = C\prod_{p\in\mathbf{V}(f_1,\ldots,f_n)}(u_0+u_1X_{1p}+\cdots+u_nX_{np})^{\mathrm{mult}_p^{\cap}(f_1,\ldots,f_n)}$$

where a point $p\in\mathbf{V}(f_1,\ldots,f_n)$ is written $p=(X_{1p},\ldots,X_{np})$. □

Lemma 20. *[CLO2-2000, Chapter 3, Proposition 5.15] Let $\mathbb{F}$ be algebraically closed, let the polynomials $f_1,\ldots,f_n\in\mathbb{F}[x_1,\ldots,x_n]$ have total degrees at most $d_1,\ldots,d_n$ and no solutions at ∞. Then we have*

$$\mathrm{Res}_{d_1,\ldots,d_n}^{x_n=u_0}(f_1,\ldots,f_n) = \pm\mathrm{Res}_{1,d_1,\ldots,d_n}(u_0-x_n,f_1,\ldots,f_n)$$

where $\mathrm{Res}_{d_1,\ldots,d_n}^{x_n=u_0}(f_1,\ldots,f_n)$ is the resultant of $f_1,\ldots,f_n$ with respect to $x_1,\ldots,x_{n-1}$ by considering x_n as a constant u_0. □

Now we can prove our theorem.

Theorem 21. *All points in the complex variety $\mathbf{V}(r,\partial_x r,\partial_y r)$ have generically intersection multiplicity one:*

$$\mathrm{mult}_{(X,Y)}^{\cap}(r,\partial_x r,\partial_y r)\le 1 \text{ for all } (X,Y)\in\mathbf{V}(r,\partial_x r,\partial_y r).$$

Proof. We work over the complex field $\mathbb{C}$ (which is algebraically closed).
If we consider hypotheses (4) and (5), we can apply Teissiers formula and obtain

$$\mathrm{mult}_{(X,Y)}^{\cap}(r,\partial_x r,\partial_y r)\le\mathrm{mult}_{(X,Y)}^{\cap}(\partial_x r,\partial_y r) = \mathrm{mult}_{(X,Y)}^{\cap}(r,\partial_y r)-\mathrm{mult}_Y(r(X,y))+1.$$

For $h \in \mathbb{C}[x,y]$ we denote by $\widetilde{h}$ the polynomial $h(X,\cdot)$ in y. We have $(X,Y) \in \mathbf{V}(r,\partial_x r,\partial_y r)$ thus $\widetilde{r}(Y) = \widetilde{\partial_y r}(Y) = 0$. By $\widetilde{\partial_y r} = \partial_y \widetilde{r}$ and Proposition 51 we have $\mathrm{mult}_Y(r(X,y)) = \mathrm{mult}_Y(\widetilde{r}) \geq 2$. Let $f_1 := r$ of degree d and $f_2 := \partial_y r$ which has degree $d-1$. As usual consider f_1 and f_2 to have no solutions at ∞. We take $f_0 := u_0 + u_1 x + u_2 y$ for $u_0 = 0$, $u_1 = -1$ and $u_2 = 0$. Then there exists a non zero constant C such that $\mathrm{Res}_{1,d,d-1}(u-x,f_1,f_2) = C\prod_{p\in\mathbf{V}(f_1,f_2)}(u-X_p)^{\mathrm{mult}_p^{\cap}(f_1,f_2)}$. Recalling the formula given in Lemma 20, we have $\mathrm{Res}_{d,d-1}^{x=u}(f_1,f_2) = \pm\mathrm{Res}_{1,d,d-1}(u-x,f_1,f_2)$. Thus

$$\pm C \prod_{p\in\mathbf{V}(r,\partial_y r)} (x-X_p)^{\mathrm{mult}_p^{\cap}(r,\partial_y r)} = \mathrm{Res}_y(r,\partial_y r) = \pm\diamondsuit_1 \cdot \diamondsuit_2^2$$

with irreducible polynomials $\diamondsuit_1, \diamondsuit_2$ of bi-degrees $(3d^2-7d+4, 3d^2-5d)$ for $\diamondsuit_1$ and $(2d^3 - 7d^2+6d-2, 2d^3-5d^2+3d)$ in the coefficient ring by Proposition 18. Furthermore $\diamondsuit_1 \neq \diamondsuit_2$ by the degrees. If we consider $\diamondsuit_1$ and $\diamondsuit_2$ to stay irreducible and different by evaluation, we obtain $\mathrm{mult}_{(X,Y)}^{\cap}(r,\partial_y r) \leq 2$.

Both formulas together imply in the generic case:

$$\begin{aligned}
\mathrm{mult}_{(X,Y)}^{\cap}(r,\partial_x r,\partial_y r) &\leq \mathrm{mult}_{(X,Y)}^{\cap}(\partial_x r,\partial_y r) \\
&= \mathrm{mult}_{(X,Y)}^{\cap}(r,\partial_y r) - \mathrm{mult}_Y(r(X,y)) + 1 \\
&\leq 2 - 2 + 1 = 1
\end{aligned}$$

□

4.2 All points in the variety V have intersection multiplicity one in σ_{11}, σ_{10}

Theorem 22. *Assuming hypotheses* (∗1) to (∗5) the ideals $I = \langle r,\partial_x r,\partial_y r\rangle$ and $J = \langle \sigma_{11},\sigma_{10}\rangle$: ${\sigma_{22}}^{\infty}$ coincide. Furthermore $\mathrm{mult}_{(X,Y)}^{\cap}(\sigma_{11},\sigma_{10}) = 1$ for all $(X,Y) \in \mathbf{V}(r,\partial_x r,\partial_y r)$.

Proof. By Theorem 21 and Proposition 55 the ideal I is radical: $I = \sqrt{I}$. By Theorem 8, Corollary 39 and the proof in Chapter 3.1 we have $I \subset J$ and $\sqrt{J} \subset \sqrt{I}$. All together we obtain $\sqrt{J} \subset \sqrt{I} = I \subset J$, thus $\sqrt{J} = J$ by Proposition 27. We also obtain $I = J$ and by Proposition 55 all intersection multiplicities $\mathrm{mult}_{(X,Y)}^{\cap}(\sigma_{11},\sigma_{10})$ are equal to 1. □

4.3 Multiplicity one implies non-zero Jacobien

Theorem 23. *Let* $I := \langle f_1,\ldots,f_n\rangle \subset \mathbb{R}[x_1,\ldots,x_n]$ *and let* $F : \mathbb{R}^n \to \mathbb{R}^n$ *denotes the mapping* $(x_1,\ldots,x_n) \mapsto (f_1(x_1,\ldots,x_n),\ldots,f_n(x_1,\ldots,x_n))^T$. *Let* $p = (X_{1p},\ldots,X_{np}) \in \mathbf{V}(f_1,\ldots,f_n)$ *such that* $\mathrm{mult}_p^{\cap}(f_1,\ldots,f_n) = 1$. *Then* $\det J_F(p) \neq 0$.

Proof. We denote by $\mathcal{O}$ the localization of $\mathbb{R}[x_1,\dots,x_n]$ at $\langle x_1-X_1,\dots,x_n-X_n\rangle$:

$$\mathcal{O}=\mathbb{R}[x_1,\dots,x_n]_{\langle x_1-X_1,\dots,x_n-X_n\rangle}.$$

Since $\mathrm{mult}_p^{\cap}(f_1,\dots,f_n)=1$ we have $x_i\in I\mathcal{O}$ for all $i\in\{1,\dots,n\}$, hence there exists polynomials $\alpha_k^i\in\mathcal{O}$, $i,k\in\{1,\dots,n\}$ such that every x_i has a notation $x_i=\sum_{k=1}^n \alpha_k^i\cdot f_k$. For $j\in\{1,\dots,n\}$ we have $\partial_j x_i=1$ if and only if $i=j$ and otherwise 0. On the other hand we have $\partial_j x_i=\partial_j(\sum_{k=1}^n\alpha_k^i\cdot f_k)=\sum_{k=1}^n\partial_j\alpha_k^i\cdot f_k+\sum_{k=1}^n\alpha_k^i\cdot\partial_j f_k$.
We denote the evaluation of a polynomial $h\in\mathbb{R}[x_1,\dots x_n]$ in p by $\widehat{h}$. Then $\widehat{\partial_j x_i}=\sum_{k=1}^n\widehat{\alpha_k^i}\cdot\widehat{\partial_j f_k}$ since $p\in\mathbf{V}(f_1,\dots,f_n)$.
Therefore

$$\mathbb{1}=\begin{pmatrix}1&&\\&\ddots&\\&&1\end{pmatrix}=\begin{pmatrix}\widehat{\partial_1x_1}&\dots&\widehat{\partial_1x_n}\\\vdots&\ddots&\vdots\\\widehat{\partial_nx_1}&\dots&\widehat{\partial_nx_n}\end{pmatrix}=\begin{pmatrix}\sum\widehat{\alpha_k^1}\widehat{\partial_1f_k}&\dots&\sum\widehat{\alpha_k^n}\widehat{\partial_1f_k}\\\vdots&\ddots&\vdots\\\sum\widehat{\alpha_k^1}\widehat{\partial_nf_k}&\dots&\widehat{\sum\alpha_k^n\partial_nf_k}\end{pmatrix}$$

$$=\begin{pmatrix}\widehat{\partial_1f_1}&\dots&\widehat{\partial_1f_n}\\\vdots&\ddots&\vdots\\\widehat{\partial_nf_1}&\dots&\widehat{\partial_nf_n}\end{pmatrix}\cdot\begin{pmatrix}\widehat{\alpha_1^1}&\dots&\widehat{\alpha_1^n}\\\vdots&\ddots&\vdots\\\widehat{\alpha_n^1}&\dots&\widehat{\alpha_n^n}\end{pmatrix}=\widehat{J_F}\cdot\begin{pmatrix}\widehat{\alpha_1^1}&\dots&\widehat{\alpha_1^n}\\\vdots&\ddots&\vdots\\\widehat{\alpha_n^1}&\dots&\widehat{\alpha_n^n}\end{pmatrix}$$

thus $\widehat{J_F}$ is invertible. □

4.4 Post process

By Theorems 22 and 23, the system

$$\sigma_{11}(x,y)=0,\quad \sigma_{10}(x,y)=0$$

has only regular solutions. Applying the Krawczyk subdivison algorithm, we obtain by Propositions 6 and 7 a complete list $L_{isolate}$ of boxes isolating all solutions of this system.
To determine among these boxes those containing a singularity of r, we have to check for every box if the second scalar subresultant vanishes or not. This can also be done by using box functions: A box $B\in L_{isolate}$ contains a singularity of r if $0\notin\square\sigma_{22}(B)$. In the case when $0\in\square\sigma_{22}(B)$, we refine the box using the Krawczyk operator until either $0\notin\sigma_{22}(B)$ or $0\notin r(B)$. Note that it is enough to check that one of the two functions does not vanish, and we do not need to check that the other actually vanishes. Using interval arithmetic, it is important to avoid vanishing tests since they require to reach some theoretical bounds, see [BCGY-2008].

5 Conclusion

In the challenge to design numerical calculation algorithms for the topology of singular curves, we focused on the case of a real plane curve defined as the projection of the intersection of two surfaces. The contribution of this work was the design of a numerical algorithm to isolate the singular points of such a curve.

We regarded curves with no common point at infinity in z-direction. This is for example the case for constant leading coefficients of the hypersurface describing polynomials. We showed that under suitable generic conditions, the singular points can be encoded via subresultant coefficients. In addition, it is shown that this representation enables the use of a classical efficient numerical subdivision algorithm for the isolation.
Combined with a numerical path tracking algorithm to follow regular parts of the curve, this work yields a numeric algorithm for the topology of such a curve.

In further work we want to generalize our results by weakening the five conditions. A first approach is to prove the applicability of the algorithm also for polynomials with coprime leading factors. In a second approach we want to determine dependencies among the conditions.

6 Appendix: Mathematical fundamentals

In this chapter, we give an overview of notation and results which are used in this work. Most of the results also stand isolated of the context and are basic theorems in algebraic geometry. We prove most of the mentioned theorems and propositions, if not we will clearly propose a reference instead. Good references for all discussed properties are [CLO1-2007], [CLO2-2000] and [BPR-2006].
We suppose that the reader is familiar with the definition of fields, rings, ideals and their main properties. We take $\mathbb{F}$ an arbitrary field and $\mathbb{A}$ a commutative ring.
For matrices we consider free spaces filled with zeros.

6.1 Basics of ideal theory and algebraic geometry

We start with some common notation and properties of ideals of polynomial rings.

6.1.1 Ideals

Definition 24. *Let $f_1, f_2, \ldots$ be polynomials in $\mathbb{A}$. Then we write $\langle f_1, f_2, \ldots \rangle_{\mathbb{A}}$ (and $\langle f_1, f_2, \ldots \rangle$ if $\mathbb{A}$ is clear from the context) for the ideal I generated by these polynomials:*

$$I := \langle f_1, f_2, \ldots \rangle_{\mathbb{A}} = \left\{ \sum_{i \geq 1} h_i f_i : h_i \in \mathbb{A}, h_i \neq 0 \text{ for only finite many ideals} \right\}.$$

*I is **finitely generated** if there exists a positive integer s such that $I = \langle f_1, \ldots, f_s \rangle$.*

In some particular rings we know more about the number of generator of the ideals. In polynomial rings we have the following theorem whose proof can be found in the literature, such as [CLO1-2007, Chapter 2, §5, Theorem 4].

Theorem 25 (Hilbert Basis Theorem)**.** *Every ideal in $\mathbb{F}[x_1, \ldots, x_n]$ is finitely generated.* □

Now we turn to some specific ideals.

Definition 26. *Let $I \subset \mathbb{A}$ be an ideal. The **radical** of I is defined as*

$$\sqrt{I} := \{ f \in \mathbb{A} : f^m \in I \text{ for some integer } m > 0 \}.$$

*An ideal is called **radical** if for all $f \in \mathbb{A}$ the membership f^m in I for some integer $m > 0$ implies $f \in I$.*

Radicals are related to radical ideals through the following properties.

Proposition 27. (1) *The radical of an ideal is an ideal.*

(2) *Each ideal is contained in its radical.*

(3) *An ideal is a radical ideal if and only if it is his own radical.*

Proof. Let $I \subset \mathbb{A}$ be an ideal.

(1) $0_{\mathbb{A}}$ is in I and therefore in $\sqrt{I}$. Let $f, g \in \sqrt{I}$ and $\alpha, \beta \in \mathbb{A}$. Then there exists positive integers m and l such that $f^m \in I$ and $g^l \in I$. Thus $(\alpha f + \beta g)^{m+l-1} \in I$ which implies $\alpha f + \beta g \in \sqrt{I}$. Thus $\sqrt{I}$ is an ideal.

(2) If $f \in I$ the $f \in \sqrt{I}$ by definition.

(3) Let I be a radical ideal and $f \in \sqrt{I}$. Then there exists $m > 0$ such that $f^m \in I$ which implies $f \in I$ since I is radical.
Let $I = \sqrt{I}$. Then for all $f \in \mathbb{A}$ the membership $f^m \in I$ for some $m > 0$ implies $f \in \sqrt{I} = I$.

□

We suppose the reader to be familiar with the basic ideal operations like intersection, union, sum, multiplication, and division (see for example [CLO1-2007] for definitions). Here we define the saturation of an ideal with respect to an other which can be seen as a generalization of the division. The saturation has a nice geometrical analogy which we will present in the next section.

Definition 28. *Let I and J be two ideals in $\mathbb{A}$. Then the **saturation** of I with respect to J is defined as*

$$I{:}J^{\infty} := \{f \in \mathbb{A} : \text{ it exists } m > 0 \text{ such that } fJ^m \subset I\}$$

Now we prove two main properties of the saturation of ideals.

Proposition 29. *The set $I{:}J^{\infty}$ is an ideal containing I itself.*

Proof. If $f \in I$, then $fJ \subset I$ thus $f \in \sqrt{I}$ by definition. This implies $O_{\mathbb{A}} \in \sqrt{I}$. Let $f, g \in I$ and $\alpha, \beta \in \mathbb{A}$. Then there exists positive integers m and m' such that $f \cdot J^m \subset I$ and $g \cdot J^{m'} \subset I$. Hence $(\alpha f + \beta g) \cdot J^l \subset I$ with $l = \max\{m, m'\}$. Thus $I{:}J^{\infty}$ is an ideal. □

Proposition 30. *Let I, J, K be ideals in $\mathbb{F}[x_1, \ldots x_n]$. Then $I \subset K{:}J^{\infty}$ if and only if there exists a positive integer m such that $I \cdot J^m \subset K$.*

Proof. Let $\{f_1, \ldots, f_s\}$ be a basis of I (which can be considered as finite by the Hilbert Basis Theorem).
First we consider $I \subset K{:}J^{\infty}$. Then for every f_i there exists an m_i such that $f_i \cdot J^{m_i} \subset K$.

Let $m := \max\{m_i : 1 \leq i \leq s\}$. Then for every $f = \sum_{i=1}^{s} h_i f_i \in I$, $h_i \in \mathbb{F}[x_1, \ldots, x_s]$ we have $f \cdot J^m \subset K$ by the ideal property and thus $I \cdot J^m \subset K$.
Now let $I \cdot J^m \subset K$ for some $m > 0$. Then $f \cdot J^m \subset K$ for all $f \in I$ and we have $I \subset K{:}J^\infty$ by definition. □

Before we give the definition of affine varieties in the next section, we introduce an ideal corresponding to a point set of $\mathbb{F}^n$.

Proposition 31. *Let $U \subset \mathbb{F}^n$. Then the set*

$$\mathbf{I}(U) := \{f \in \mathbb{F}[x_1, \ldots, x_n] : f(p) = 0 \text{ for all } p \in U\}$$

is an ideal of $\mathbb{F}[x_1, \ldots, x_n]$ and will be called the ideal of U.

Proof. The zero polynomial is obviously contained in $\mathbf{I}(U)$. Let $f, g \in \mathbf{I}(U)$, i.e. $f(p) = g(p) = 0$ for all $p \in U$. Let $\alpha, \beta \in \mathbb{F}[x_1, \ldots, x_n]$ and $p \in U$. Then $(\alpha f + \beta g)(p) = \alpha(p) \cdot f(p) + \beta(p) \cdot g(p) = 0$ thus $\alpha f + \beta g \in \mathbf{I}(U)$. Hence $\mathbf{I}(U)$ is an ideal. □

The ideal of a point set U is the set of all polynomials which vanish on all points of U at the same time. In the next section, we will specify the converse: The set of all zeros of a given set of polynomials.

6.1.2 Affine Varieties

Definition 32. *Let $\{f_1, \ldots, f_s\}$ be a set of polynomials in $\mathbb{F}[x_1, \ldots, x_n]$. Then the **affine variety** $\mathbf{V}(f_1, \ldots, f_s)$ of $f_1, \ldots, f_s$ is the point set on which the polynomials $f_1, \ldots, f_s$ vanish simultaneously:*

$$\mathbf{V}(f_1, \ldots, f_s) = \{p \in \mathbb{F}^n : f_i(p) = 0 \text{ for all } i \in \{1, \ldots, s\}\}.$$

An affine variety in $\mathbb{F}^n$ is always given as the zero set of a set of polynomials in $\mathbb{F}[x_1, \ldots, x_n]$. We obviously have $\mathbf{V}(f_1, \ldots, f_s) = \mathbf{V}(\langle f_1, \ldots, f_s \rangle)$.

Definition 33. *Let $\mathbb{F} \subset \mathbb{C}$ and $I \subset \mathbb{F}[[x_1, \ldots, x_n]$ an ideal. We say I is **zero-dimensional** if the affine variety $\mathbf{V}(I)$ consists of only finitely many points in $\mathbb{F}^n$.*

Affine varieties are our centre of interest. While ideals are algebraic mathematical objects, varieties are geometrical mathematical objects. There is a nice correspondence between varieties and particular ideals, which will be discussed in this section.
We consider $\mathbf{I}$ as in the last proposition as a map from the set of point sets in $\mathbb{F}^n$ into the set of ideals of $\mathbb{F}[x_1, \ldots, x_n]$. Similarly, $\mathbf{V}$ is seen as a map from the set of ideals of $\mathbb{F}[x_1, \ldots, x_n]$ into the set of affine varieties in $\mathbb{F}^n$. Hereinafter we prove some basic properties of these maps.

Proposition 34. *The maps* $\mathbf{I}$ *and* $\mathbf{V}$ *are inclusion-reversing, i.e.*

(1) *if* $V \subset W$ *are two affine varieties in* $\mathbb{F}^n$ *then* $\mathbf{I}(V) \supset \mathbf{I}(W)$ *and*

(2) *if* $I \subset J$ *are two ideals in* $\mathbb{F}[x_1, \ldots, x_n]$ *then* $\mathbf{V}(I) \supset \mathbf{V}(J)$.

Proof. The proof in both cases is straight forward: Let $V \subset W$ and $f \in \mathbf{I}(W)$. Then f vanishes in all points of W and therefore in all points of V. Thus $f \in \mathbf{I}(V)$.
If $I \subset J$ and $p \in \mathbf{V}(J)$ then all polynomials in J and thus in I vanish on p. Hence $\mathbf{V}(I) \supset \mathbf{V}(J)$. □

The next theorem is one of the most important theorems in algebraic geometry which helps us to extend the above properties.

Theorem 35 (Hilbert's Nullstellensatz)**.** *Let* $\mathbb{F}$ *be algebraically closed.*
If $f, f_1, \ldots, f_s \in \mathbb{F}[x_1, \ldots, x_n]$ *are such that* $f \in \mathbf{I}(\mathbf{V}(f_1, \ldots, f_s))$*, then there exists an integer* $m \geq 1$ *such that* $f^m \in \langle f_1, \ldots, f_s \rangle$ *(and conversely).* □

We don't prove this theorem but refer the reader to [CLO1-2007, Chapter 4, §1, Theorem 2] which gives a good comprehensive proof. In this work we will use two other versions of the Nullstellensatz which are direct corollaries of the previous one.

Corollary 36 (Strong Nullstellensatz)**.** *Let* $\mathbb{F}$ *be algebraically closed and* $I \subset \mathbb{F}[x_1, \ldots, x_n]$ *an ideal. Then*

$$\sqrt{I} = \mathbf{I}(\mathbf{V}(I)).$$

Proof. Let $f \in \sqrt{I}$ and $m > 0$ such that $f^m \in I \subset \mathbf{I}(\mathbf{V}(I))$. Thus $0 = f^m(p) = (f(p))^m$ for all $p \in \mathbf{V}(I)$ which implies $f(p) = 0$ for all $p \in \mathbf{V}(I)$ since $\mathbb{F}$ is a field. Thus $f \in \mathbf{I}(\mathbf{V}(I))$.
Let $f \in \mathbf{I}(\mathbf{V}(I))$. By Hilbert's Nullstellensatz there exists a positive integer m such that $f^m \in I$. Hence $f \in \sqrt{I}$ by definition. □

Corollary 37. *Let* $\mathbb{F}$ *be algebraically closed and* $I \subset \mathbb{F}[x_1, \ldots, x_n]$ *an ideal. Then there exists an integer* l *such that* $(\sqrt{I})^l \subset I$.

Proof. Let $I = \langle f_1, \ldots, f_s \rangle$. By the strong Nullstellensatz $\sqrt{I} = \mathbf{I}(\mathbf{V}(I))$ which is an ideal in $\mathbb{F}[x_1, \ldots, x_n]$ thus admits a finite basis $\{g_1, \ldots, g_t\}$ by Hilbert's Basis Theorem. By Hilbert's Nullstellensatz there exists exponents m_i such that $g_i^{m_i} \in I$ for all i. For g an arbitrary element of $\sqrt{I}$ we have $g^m \in I$ for $m := 1 + \sum_{i=1}^{t}(m_i - 1)$. □

Now we are prepared to formulate the correspondence of ideals and varieties.

Theorem 38 (Ideal–Variety–Correspondence)**.** *Let* $V \subset \mathbb{F}^n$ *be an affine variety and* $I \subset \mathbb{F}[x_1, \ldots, x_n]$ *be an ideal. Then we have*

(1) $\mathbf{V}(\mathbf{I}(V)) = V$ *and*

(2) $\mathbf{I}(\mathbf{V}(I)) \supset I$. *If additionally the ideal I is radical, then in fact the equality is hold.*

Proof. We first prove (2) since this property will be used for the proof of (1).

(2) Let I be an ideal of $\mathbb{F}[x_1, \ldots, x_n]$ and let $f \in I$. Then $f(p) = 0$ for all $p \in \mathbf{V}(I)$, i.e. $f \in \mathbf{I}(\mathbf{V}(I))$. Hence $I \subset \mathbf{I}(\mathbf{V}(I))$.

(1) First let U be a subset $\mathbb{F}^n$, not necessarily an affine variety. We are going to show that $U \subset \mathbf{V}(\mathbf{I}(U))$. Let $p \in U$. Then $f(p) = 0$ for all $f \in \mathbf{I}(U)$. But by definition we can conclude $p \in \mathbf{V}(\mathbf{I}(U))$ thus the first inclusion is even hold for subsets instead of ideals.
Now let V be an affine variety, thus $V = \mathbf{V}(H)$ for a subset $H = \{f_1, \ldots, f_s\}$ of polynomials in $\mathbb{F}[x_1, \ldots, x_n]$. By (2) we have $H \subset \mathbf{I}(\mathbf{V}(H))$ and since the latter is an ideal we even have $\langle H \rangle \subset \mathbf{I}(\mathbf{V}(H))$. Now by Proposition 34 and Definition 32 and we have $V = \mathbf{V}(H) = \mathbf{V}(\langle H \rangle) \supset \mathbf{V}(\mathbf{I}(\mathbf{V}(H))) = \mathbf{V}(\mathbf{I}(V))$ which proves the second inclusion.

If I is radical, we have $I = \sqrt{I} = \mathbf{I}(\mathbf{V}(I))$ as a direct conclusion of the Strong Nullstellensatz. □

It is clear from the proof that for an arbitrary point set $U \subset \mathbb{F}^n$ we still have the inclusion $U \subset \mathbf{V}(\mathbf{I}(U))$.

Theorem 38 is an improvement of Proposition 34 so that we can now formulate the correspondence between arbitrary ideals and affine variety. Furthermore, the theorem even gives a one-to-one-correspondence between affine varieties and radical ideals.

Corollary 39. *For $V, W \subset \mathbb{F}^n$ two affine varieties and $I, J \in \mathbb{F}[x_1, \ldots, x_n]$ two ideals we have the following correspondence:*

(1) *if $V \subset W$ then $\mathbf{I}(V) \supset \mathbf{I}(W)$ and conversely*
if $\mathbf{I}(V) \supset \mathbf{I}(W)$ then $V = \mathbf{V}(\mathbf{I}(V)) \subset \mathbf{V}(\mathbf{I}(W)) = W$.

(2) *if $I \subset J$ then $\mathbf{V}(I) \supset \mathbf{V}(J)$ but conversely*
if $\sqrt{I} = \mathbf{I}(\mathbf{V}(I)) \subset \mathbf{I}(\mathbf{V}(J)) = \sqrt{J}$ then $\mathbf{V}(I) = \mathbf{V}(\sqrt{I}) \supset \mathbf{V}(\sqrt{J}) = \mathbf{V}(J)$.

□

In the end of this section, we prove a proposition to compute the variety of the saturation of ideals.

Proposition 40. *Let I and J be ideals in $\mathbb{F}[x_1, \ldots, x_n]$. Then*

$$\mathbf{V}(I{:}J^\infty) = \overline{\mathbf{V}(I) - \mathbf{V}(J)}$$

where $\overline{U}$ for an affine set $U \subset \mathbb{F}^n$ is the smallest affine variety containing U and is called the ***Zariski closure*** *of U.*

Proof. We first show $I{:}J^\infty \subset \mathbf{I}(\mathbf{V}(I) - \mathbf{V}(J))$. Let $f \in I{:}J^\infty$ and let $p \in \mathbf{V}(I) - \mathbf{V}(J)$. Then $p \in \mathbf{V}(I)$ but $p \notin \mathbf{V}(J)$. Thus there exists $g \in J$ such that $g(p) \neq 0$. By definition we have $fg^m \in I$ for some $m > 0$. Thus $(fg^m)(p) = f(p) \cdot (g(p))^m = 0$. This implies $f(p) = 0$ since $\mathbb{F}$ is a field and $g(p) \neq 0$. Thus $f \in \mathbf{I}(\mathbf{V}(I) - \mathbf{V}(J))$.
Now by Proposition 34 and Theorem 38, we have $\mathbf{V}(I) - \mathbf{V}(J) \subset \mathbf{V}(\mathbf{I}(\mathbf{V}(I) - \mathbf{V}(J))) \subset \mathbf{V}(I{:}J^\infty)$ which proves $\overline{\mathbf{V}(I) - \mathbf{V}(J)} \subset V(I{:}J^\infty)$ since the latter is an algebraic variety.

Now we prove $\mathbf{V}(I{:}J^\infty) \subset \overline{\mathbf{V}(I) - \mathbf{V}(J)}$.
The first step is to show $\overline{\mathbf{V}(I) - \mathbf{V}(J)} = \mathbf{V}(\mathbf{I}(\mathbf{V}(I) - \mathbf{V}(J)))$. The inclusion $\overline{\mathbf{V}(I) - \mathbf{V}(J)} \subset \mathbf{V}(\mathbf{I}(\mathbf{V}(I) - \mathbf{V}(J)))$ is clear since $\mathbf{V}(\mathbf{I}(\mathbf{V}(I) - \mathbf{V}(J)))$ is a variety containing $\mathbf{V}(I) - \mathbf{V}(J)$ by Theorem 38. For the other direction, consider W an arbitrary variety containing $\mathbf{V}(I) - \mathbf{V}(J)$. Then by Proposition 34 an Theorem 38, we have $\mathbf{V}(\mathbf{I}(\mathbf{V}(I) - \mathbf{V}(J))) \subset \mathbf{V}(\mathbf{I}(W)) = W$ which is also true for the special choice $W = \overline{\mathbf{V}(I) - \mathbf{V}(J)}$.
Now we prove $\mathbf{V}(I{:}J^\infty) \subset \mathbf{V}(\mathbf{I}(\mathbf{V}(I) - \mathbf{V}(J)))$ by using Corollary 39. Let $f \in \sqrt{\mathbf{I}(\mathbf{V}(I) - \mathbf{V}(J))}$. Then there exists $m > 0$ such that f^m vanishes on $\mathbf{V}(I) - \mathbf{V}(J)$ which also implies that f vanishes on $\mathbf{V}(I) - \mathbf{V}(J)$ (since $\mathbb{F}$ is a field). We have to show that a power of f is included in $I{:}J^\infty$. Let g_1 be an arbitrary polynomial in J. Then fg_1 vanishes on $V(I)$ since f vanishes on $\mathbf{V}(I) - \mathbf{V}(J)$ and g_1 on $V(J)$. Hence $fg_1 \in \mathbf{I}(\mathbf{V}(I)) = \sqrt{I}$. By Corollary 37 there exists an integer $l > 0$ such that $(\sqrt{I})^l \subset I$. Thus for all $g \in J^l$ we have $f^l \cdot g(\sqrt{I})^l \subset I$ and therefore $f^l \in I{:}J^\infty$. Hence $f \in \sqrt{I{:}J^\infty}$. □

6.2 Resultants and Subresultants

In this section, we study resultants and subresultants of polynomials. The goal is to decide whether a set of polynomials has a common non trivial factor. For two polynomials with coefficients in a GCD domain this question is similar to compute their greatest common divisor. We will see that the subresultants have similar nice properties.
From now on we consider $\mathbb{A}$ to be an integral domain.
First we will focus on the most important case for this work, the resultant and subresultants of two polynomials in affine notation. We will prove some properties and handle some special cases when the polynomial coefficents are in a field. In the second section, we will give the homogeneous version of the resultant to extend the definition on more polynomials.

6.2.1 Resultant and subresultants of two polynomials

In this section, let $f = f_{d_1}z^{d_1} + \cdots + f_1 z + f_0$, $g = g_{d_2}z^{d_2} + \cdots + g_1 z + g_0$ be two polynomials in $\mathbb{A}[z]$ with non-zero leading coefficients.

Definition 41. *Then we call the determinant of the Sylvester matrix of f and g the* ***resultant*** *of these polynomials:*

$$\mathrm{Res}(f,g) := \det \begin{pmatrix} f_{d_1} & & & & g_{d_2} & & & \\ f_{d_1-1} & f_{d_1} & & & \vdots & g_{d_2} & & \\ \vdots & \vdots & \ddots & & g_1 & \vdots & \ddots & \\ \vdots & \vdots & & f_{d_1} & g_0 & \vdots & & \ddots \\ \vdots & \vdots & & \vdots & & g_0 & & \\ f_0 & \vdots & & \vdots & & & \ddots & \\ & f_0 & & \vdots & & & & g_{d_2} \\ & & \ddots & \vdots & & & & \vdots \\ & & & f_0 & & & & g_0 \end{pmatrix} \begin{matrix} \\ \\ \\ \\ \\ \\ \\ \\ \end{matrix} \begin{matrix} \\ \\ \\ \\ \\ \\ \\ \\ \end{matrix}$$

$$\underbrace{\qquad\qquad}_{d_2} \qquad\qquad \underbrace{\qquad\qquad}_{d_1}$$

We consider polynomials $f, g \in \mathbb{F}[x_1, \ldots, x_n, z]$ as univariate polynomials in z with coefficients in $\mathbb{A} = \mathbb{F}[x_1, \ldots, x_n]$. In this case we write $\mathrm{Res}_z(f,g)$ to emphasize the indeterminate in respect to which we calculate the resultant of f and g.

By definition the resultant is an element in the coefficient ring $\mathbb{A}$. Beyond that the resultant is a linear combination of f and g in $\mathbb{A}[z]$:

Proposition 42. $\mathrm{Res}(f,g) \in \langle f, g \rangle_{\mathbb{A}[z]}$.

Proof. The proof is based on a nice construction seen in [GL-2007]. Multiplying the $(d_1+d_2-j)^{\text{th}}$ row by z^j and adding to the last row of the Sylvester matrix we obtain the $(d_1+d_2)\times(d_1+d_2)$

matrix

$$\begin{pmatrix}
f_{d_1} & & & & g_{d_2} & & & & & \\
f_{d_1-1} & f_{d_1} & & & \vdots & g_{d_2} & & & & \\
\vdots & \vdots & \ddots & & g_1 & \vdots & \ddots & & & \\
\vdots & \vdots & & f_{d_1} & g_0 & \vdots & & \ddots & & \\
\vdots & \vdots & & \vdots & & g_0 & & & \ddots & \\
f_0 & \vdots & & \vdots & & & \ddots & & & g_{d_2} \\
 & f_0 & & \vdots & & & & \ddots & & \vdots \\
 & & \ddots & \vdots & & & & & \ddots & \vdots \\
z^{d_2-1}f & \dots & \dots & f & z^{d_1-1}g & \dots & \dots & \dots & \dots & g
\end{pmatrix}$$

which has the same determinant as the Sylvester matrix by linearity property. We use Leibnitz formula to calculate this determinant. From the last row it is clear that each summand is either a multiple of f or of g in $\mathbb{A}[z]$, furthermore, each f-coefficient in $\mathbb{A}[z]$ has at most degree $d_2 - 1$ and each g-coefficient at most degree $d_1 - 1$. Thus there exists $\alpha, \beta \in \mathbb{A}[z]$, $\deg \alpha < d_2$ and $\deg \beta < d_1$, such that $\mathrm{Res}(f, g) = \alpha f + \beta g$. □

If f and g are polynomials with field coefficients we have the following stronger property:

Proposition 43. *[CLO1-2007, Chapter 3, §5 Proposition 8] Two polynomials $f, g \in \mathbb{F}[z]$ of positive degree have a common factor h in $\mathbb{F}[z]$ if and only if $\mathrm{Res}_z(f, g) = 0$.* □

A common factor $h \in \mathbb{F}[z]$ of f and g is a polynomial of positive degree which divides f and g. The original formulation of this proposition is for polynomials f, g with coefficients in an integer domain and a common factor h in its field of fractions but in this work we only need the statement with field coefficients. If $\mathbb{F}$ is algebraically closed then every polynomial of degree at least 1 has a zero by the fundamental theorem of algebra. In this case, f and g have a common factor in $\mathbb{F}[z]$ is equivalent to f and g have a common zero in F.

Now we give the following geometrical interpretation of the resultant of two polynomials.

Theorem 44. *Let $f, g \in \mathbb{A}[z]$ notated as above where $\mathbb{A} = \mathbb{F}[x_1, \dots, x_n]$. The f_i and g_i are polynomials in $\mathbb{F}[x_1, \dots, x_n]$ and we consider $\mathbf{V}(f_{d_1}, g_{d_2}) = \emptyset$. Then*

$$\mathbf{V}(\mathrm{Res}_z(f, g)) = \mathrm{proj}_{z=0}(\mathbf{V}(f) \cap \mathbf{V}(g)) = \mathrm{proj}_{z=0}(\mathbf{V}(f, g)).$$

Proof. First we take $p := (X_{p1}, \dots, X_{pn}) \in \mathrm{proj}_{z=0}(\mathbf{V}(f) \cap \mathbf{V}(g))$ and we denote by (p, Z) the point $(X_{p1}, \dots, X_{pn}, Z)$. Then there exists some $Z \in \mathbb{F}$ such that $f(p, Z) = g(p, Z) = 0$.

By Proposition 42 we can write $\mathrm{Res}_z(f,g) = \alpha f + \beta g$, by considering $\mathrm{Res}_z(f,g)$ as a polynomial in $\mathbb{F}[x_1,\ldots,x_n,z]$ we obtain $\mathrm{Res}_z(f,g)(p,Z) = \alpha(p,Z)f(p,Z) + \beta(p,Z)g(p,Z) = 0$, so $\mathrm{Res}_z(f,g)(p) = 0 \in \mathbb{F}[x_1,\ldots,x_n]$ and hence $p \in \mathbf{V}(\mathrm{Res}_z(f,g))$.
Now we denote $r := \mathrm{Res}_z(f,g) \in \mathbb{F}[x_1,\ldots,x_n]$ and let $p \in \mathbf{V}(r)$. We set $f_* := f(p,\cdot) \in \mathbb{F}[z]$ and $g_* := g(p,\cdot) \in \mathbb{F}[z]$. Then $r_* := \mathrm{Res}_z(f_*,g_*) = r(p) = 0 \in \mathbb{F}$. Let $f_{d_1*} = f_{d_1}(p)$ and $g_{d_2*} = g_{d_2}(p)$. Since $\mathbf{V}(f_{d_1},g_{d_2}) = \emptyset$ the coefficients f_{d_1*} and f_{d_2*} are not both zero. By Proposition 43 we are done if both coefficients don't vanish on p. (Then f_* and g_* have a non-constant common factor h and for an algebraically closed field $\mathbb{F}$ we find a zero Z of h. Thus $f_*(Z) = g_*(Z) = 0$ and therefore $f(p,Z) = g(p,Z) = 0$.
If one of the coefficient polynomials, w.l.o.g. g_*, is zero, we can use a base change argument to prove the existence of such a Z: $\langle f,g\rangle = \langle f, g + z^m f\rangle$ for all $m > 0$. If we choose m such that $\deg_z(g + z^m f) > \deg_z(g)$ thus $g + z^m f$ has the non-zero leading coefficient f_{d_1}. The previous argument gives us a $Z \in \mathbb{F}$ such that $(p,Z) \in \mathbf{V}(f, g + z^m f) = \mathbf{V}(f,g)$. For details we refer the reader to [CLO1-2007, Chapter 3, §6, Theorem 4] .
In both cases we obtain a Z such that $(p,Z) \in \mathbf{V}(f) \cap \mathbf{V}(g)$ and thus $p \in \mathrm{proj}_{z=0}(\mathbf{V}(f) \cap \mathbf{V}(g)) = \mathbf{V}(f,g)$. □

Theorem 44 and Proposition 43 already describe the correspondence between the zero sets of f and g and their resultant. Now we want to describe the greatest common divisor of $f,g \in \mathbb{F}[z]$ for which we introduce subresultants of f and g.

Definition 45. *Let $f,g \in \mathbb{A}[z]$ as usual. For $0 \le k \le \min\{d_1,d_2\}$ and $0 \le i \le k$ let M_{ki} denotes the matrix obtained by deleting columns $(d_1-k+1),\ldots,d_1$, $(d_1+d_2-k+1),\ldots,(d_1+d_2)$ and the last $2k+1$ rows except row (d_1+d_2-k-i) of the Sylvester matrix of f and g:*

$$M_{ki} := \begin{pmatrix} f_{d_1} & & & & g_{d_2} & & & \\ f_{d_1-1} & f_{d_1} & & & \vdots & g_{d_2} & & \\ \vdots & & \ddots & & \vdots & & \ddots & \\ \vdots & & & f_{d_1} & \vdots & & & g_{d_2} \\ \vdots & & & \vdots & \vdots & & & \\ f_{2k-d_2+2} & & & f_{k+1} & g_{2k-d_1+2} & & & g_{k+1} \\ \underbrace{f_{i+k-d_2+1} \quad \cdots \quad \cdots \quad f_i}_{d_2-k} & & & & \underbrace{g_{i+k-d_1+1} \quad \cdots \quad \cdots \quad g_i}_{d_1-k} & & & \end{pmatrix}.$$

*This matrix is a $(d_1+d_2-2k)\times(d_1+d_2-2k)$-matrix and we write $\sigma_{ki}(f,g)$ for its determinant. The polynomial $\mathrm{Sres}_k(f,g) := \sum_{i=0}^{k} \sigma_{ki}(f,g)z^i \in \mathbb{A}[z]$ is called the **kth polynomial subresultant** and its leading coefficient $\sigma_{kk}(f,g)$ the **kth scalar subresultant** of f and g.*

It is clear that the zeroth polynomial subresultant of f and g is in fact their resultant. We have $\mathrm{Sres}_0(f,g) = \sigma_{00}(f,g) = \mathrm{Res}(f,g)$.
By the linearity of the determinant we can write $\mathrm{Sres}_k(f,g)$ directly as the determinant of the matrix

$$M_k^* := \begin{pmatrix} f_{d_1} & & & & g_{d_2} & & & \\ f_{d_1-1} & f_{d_1} & & & \vdots & g_{d_2} & & \\ \vdots & & \ddots & & \vdots & & \ddots & \\ \vdots & & & f_{d_1} & \vdots & & & g_{d_2} \\ \vdots & & & \vdots & \vdots & & & \\ f_{2k-d_2+2} & & & f_{k+1} & g_{2k-d_1+2} & & & g_{k+1} \\ z^{d_2-k-1}f & \dots & \dots & f & z^{d_1-k-1}g & \dots & \dots & g \end{pmatrix}.$$

The exact degree of the k-th polynomial subresultant is at most k and depends only on the coefficients of f and g. The next well-known theorem, give a more detailed result.
The theorem can be found in the literature in several versions. We recall a version based on Theorem 2.1 in [LRS-2001] and Theorem 4.3 in [K-2003].

Theorem 46 (Gap Structure Theorem)**.** *Let $f, g \in \mathbb{A}[z]$ be polynomials such that $\deg \mathrm{Sres}_j = j$. Then:*

(1) *If Sres_{j-1} is zero then $\mathrm{Sres}_{j-2} = \cdots = \mathrm{Sres}_0 = 0$*

(2) *If Sres_{j-1} is of degree $0 \le k < j-1$ then $\mathrm{Sres}_{j-2} = \cdots = \mathrm{Sres}_{k+1} = 0$ and*

$$\sigma_{jj}{}^{j-k-1}\mathrm{Sres}_k = \sigma_{j-1,k}{}^{j-k-1}\mathrm{Sres}_{j-1}.$$

Furthermore, Sres_k has degree k.

□

For polynomials with field coefficients we further know:

Theorem 47. *[BPR-2006, Proposition 4.35] Let $f, g \in \mathbb{F}[z]$ with $\deg(f) \ge \deg(g)$. Let $d \le \deg(f) - 1$. Then $\deg(\gcd(f,g)) = d$ if and only if d is the smallest i such that $\sigma_{ii}(f,g) \neq 0$.* □

By the preceding theorem, d is therefore the smallest i such that $\mathrm{Sres}_i(f,g) \neq 0$.
In this reference, the theorem is formulated in a more general version for polynomials with coefficients in an integer domain $\mathbb{A}$ and their greatest common divisor in the fraction field of $\mathbb{A}$ since the greatest common divisor is not defined for no GCD domains.

6.2.2 Multipolynomial resultants

In the previous section, we studied the resultant of two polynomials f, g in one single variable. Instead we can also work with *homogeneous* polynomials in two variables z and ϑ. A polynomial is homogeneous if every monomial summand has the same degree. If we take $f = f_{d_1} z^{d_1} + \cdots + f_0 \in \mathbb{A}[z]$ with coefficients $f_i \in \mathbb{A}$ we can homogenize f by an indeterminate ϑ and obtain the homogeneous polynomial

$$F = f_{d_1} z^{d_1} + f_{d_1-1} z^{d_1-1}\vartheta + \cdots + f_1 z\vartheta^{d_1-1} + f_0\vartheta^{d_1}.$$

It is clear that a zero Z of f turns to the zero $(Z, 1)$ of F.
For two homogeneous polynomials $F, G \in \mathbb{A}[z, \vartheta]$ obtained by homogenization of $f, g \in \mathbb{A}[z]$ we define the resultant using the same determinant as in Definition 41 and denote

$$\mathrm{Res}_{d_1,d_2}(F, G) = \mathrm{Res}_z(f, g).$$

The resultant $\mathrm{Res}(F, G)$ is an integer polynomial in the coefficients of F and G. If $\mathbb{A}$ is the field of complex numbers we have $\mathrm{Res}(F, G) = 0$ if and only if F and G have a common nontrivial solution in $\mathbb{C}$.
Now we extend this concept to n homogeneous polynomials in n variables.

Let $x = (x_1, \ldots, x_n)$. For an n-dimensional exponent vector $\alpha = (\alpha_1, \ldots, \alpha_n)$ we denote $x^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ and $\mid \alpha \mid = \sum_{i=1}^n \alpha_i$. We consider n homogeneous polynomials F_i of total degrees d_i. For every combination of i and α such that $\mid \alpha \mid = d_i$ we introduce an indeterminate u_α^i. Generally an homogeneous polynomial $F_i \in \mathbb{C}[x_1, \ldots, x_n]$ of degree d_i can be written as a specialization of the u_α^i in $\mathbb{C}$:

$$F_i = \sum_{|\alpha|=d_i} u_\alpha^i x^\alpha.$$

Theorem 48. *[CLO2-2000, Chapter 3, Theorem 2.3] If we fix positive degrees $d_1, \ldots, d_n$, then there is a unique polynomial $\mathrm{Res}_{d_1,\ldots,d_n} \in \mathbb{Z}[u_\alpha^i]$ depending only on $d_1, \ldots, d_n$ with the following properties:*

(1) *If $F_1, \ldots, F_n \in \mathbb{C}[x_1, \ldots, x_n]$ are homogeneous of degrees $d_1, \ldots, d_n$, then they have a common nontrivial solution over $\mathbb{C}$ if and only if $\mathrm{Res}_{d_1,\ldots,d_n}(F_1, \ldots, F_n) = 0$.*

(2) $\mathrm{Res}_{d_1,\ldots,d_n}(x_1^{d_1}, \ldots, x_n^{d_n}) = 1$.

(3) $\mathrm{Res}_{d_1,\ldots,d_n}$ *is irreducible, even when regarded as a polynomial in $\mathbb{C}[u_\alpha^i]$.*

Considering $F_1, \ldots, F_n$ having no common solution at infinity we can dehomogenize $F_1, \ldots, F_n$ by equaling one variable with 1. Here we set $x_1 = 1$ and obtain n affine polynomials $f_i =$

$F_i(1, x_2, \ldots, x_n)$ in $(n-1)$ variables. According to the resultant of two affine polynomials we write $\mathrm{Res}_{d_1,\ldots,d_n}(f_1, \ldots, f_n)$ instead of $\mathrm{Res}_{d_1,\ldots,d_n}(F_1, \ldots, F_n)$ to emphasize that we work in the affine situation.
Multipolynomial subresultants have a number of useful properties which can be used in elimination theory and for solving polynomial equation systems, but unfortunately it is not so easy to compute them. For us the most important property is the connection of multipolynomial resultants and intersection multiplicities which is of algebraic interest.

6.3 Some tools of differential geometry and computations in local rings

Definition 49. *Let $f \in \mathbb{F}[x_1, \ldots, x_n]$. A **singular point** $p := (X_{p1}, \ldots, X_{pn})$ of f is a solution of $f(x_1, \ldots, x_n) = 0$ such that the partial derivatives of f vanish simultaneously:*

$$f(p) = \partial_1 f(p) = \cdots = \partial_n f(p) = 0.$$

To discuss the possibility of a point to be singular we will introduce multiplicities of polynomials. As usual we first handle the univariate case.

Definition 50. *Let $f \in \mathbb{F}[z]$. The greatest power p such that $(z-Z)^p$ is a divisor of f in $\mathbb{F}[z]$ is called **multiplicity** of Z in f and is denoted by* $\mathrm{mult}_Z(f)$.

The multiplicity counts the number of derivations of f for which Z is a zero (starting by f itself). Here we only need the formulations for $\mathrm{mult}_Z(f) \geq 2$.

Proposition 51. *Let $f \in \mathbb{F}[z]$. Then $(z-Z)$ divides both f and $f' := \partial_z f$ if and only if $(z-Z)^2$ divides f (meaning* $\mathrm{mult}_Z(f) \geq 2$*).*

Proof. Let $f = (z-Z)^2 \cdot f_1$. Then $(z-Z)$ divides f and $f' = 2(z-Z)f_1 + (z-Z)f_1'$.
Let $f = (z-Z)f_1$ and $f' = (z-Z)f_2$. Then $f' = (z-Z)f_1' + f_1$ and thus $(z-Z) \mid f_1$ since $f'(Z) = 0$. Hence $(z-Z)^2 \mid f$. □

In fact if $\mathbb{F}$ is algebraically closed the sum of all multiplicities of zeros of f is the degree of f. Especially the number of different zeros of f can be less than the degree of f.
Now we extend this concept on multivariate polynomials. For a zero dimensional ideal $I = \langle f_1, \ldots, f_n \rangle \subset \mathbb{F}[x_1, \ldots, x_n]$ with $\mathbb{F}$ algebraically closed it sometimes happens that $\mathbf{V}(I)$ contains fewer distinct points than the dimension of $\mathbb{F}[x_1, \ldots, x_n]/I$. Thus we like to compute a sort of algebraic multiplicity, here called intersection multiplicity, that can be computed locally on each point $p \in \mathbf{V}(I)$ with the property that the sum of all multiplicities is equal to the dimension.

Definition 52. *Let $p = (X_{1p}, \ldots, X_{np}) \in \mathbb{F}^n$ and denotes M the maximal ideal $\mathbf{I}(p) = \langle x_1 - X_{1p}, \ldots, x_n - X_{np} \rangle \in \mathbb{F}[x_1, \ldots, x_n]$. We denote by $\mathbb{F}[x_1, \ldots, x_n]_M$ the collection of all rational functions $\frac{f}{g}$ in $x_1, \ldots, x_n$ with $g(p) \neq 0$:*

$$\mathbb{F}[x_1, \ldots, x_n]_M := \left\{ \frac{f}{g} : f, g \in \mathbb{F}[x_1, \ldots, x_n], g(p) \neq 0 \right\}.$$

The construction in this definition is a special case of a general procedure called **localization**. We say $\mathbb{F}[x_1, \ldots, x_n]$ is **localized** by M. The obtained ring $\mathbb{F}[x_1, \ldots, x_n]_M$ is a local ring, meaning that it has exactly one maximal ideal, the ideal M. Based on this construction we can now define the intersection multiplicity of polynomials.

Definition 53. *Let $I = \langle f_1, \ldots, f_s \rangle$ be a zero dimensional ideal in $\mathbb{F}[x_1, \ldots, x_n]$ (meaning that $\mathbf{V}(I)$ consists of finitely many points in $\mathbb{F}^n$), and assume that $p = (X_{1p}, \ldots, X_{np})$ is one of them. Let M be the maximal ideal $\mathbf{I}(p) = \langle x_1 - X_{1p}, \ldots, x_n - X_{np} \rangle$. Then the **intersection multiplicity** of the variety $\mathbf{V}(f_1, \ldots, f_s)$ in p is defined as*

$$\mathrm{mult}_p^{\cap}(f_1, \ldots, f_s) := \dim_{\mathbb{F}} \mathbb{F}[x_1, \ldots, x_n]_M / I \cdot \mathbb{F}[x_1, \ldots, x_n]_M.$$

If $\mathbb{F}$ is algebraically closed we have the formula of the dimension of $\mathbb{F}[x_1, \ldots, x_n]/I$ beeing the sum of intersection multiplicities and furthermore, we can use multiplicities to give a criterion for an ideal to be radical.

Proposition 54. *[CLO2-2000, Chapter 4, Corollary 2.5] Let $\mathbb{F}$ be algebraically closed and let I be a zero-dimensional ideal in $\mathbb{F}[x_1, \ldots, x_n]$. Let $\mathbf{V}(I)$ be the set $\{p_1, \ldots, p_s\}$. Then $\dim \mathbb{F}[x_1, \ldots, x_n]/I$ is the number of points of $\mathbf{V}(I)$ counted with multiplicity, explicitly:*

$$\dim \mathbb{F}[x_1, \ldots, x_n]/I = \sum_{i=1}^{s} \mathrm{mult}_{p_i}^{\cap}(I).$$

□

Proposition 55. *[CLO2-2000, Chapter 4, Corollary 2.6] Let $\mathbb{F}$ be algebraically closed. Then a zero-dimensional ideal $I \subset \mathbb{F}[x_1, \ldots, x_n]$ is radical if and only if every point in the variety of I has intersection multiplicity* 1. □

References

[BPR-2006] S. Basu, R. Pollack, M.-F. Roy, *Algorithms in real algebraic geometry*, Second Edition, Springer, 2006.

[BR-1990] R. Benedetti, J.J. Risler, *Real algebraic and semi-algebraic sets*, Actualites Mathematiques, Hermann, 1990.

[BCGY-2008] M. Burr, S.W. Choi, B. Galehouse, C. Yap, *Complete subdivision algorithms, ii: Isotopic meshing of singular algebraic curves*, International Symposium on Symbolic and Algebraic Computation, 2008.

[BM-2007] L. Busé, B. Mourrain, *Explicit factors of some iterated resultants and discriminants*, Mathematics of Computation of the American Mathematical Society 78, 2009, 345–386.

[CLO1-2007] D. Cox, J. Little, D. O'Shea, *Ideals, Varieties, and Algorithms, An introduction to computational algebraic geometry and commutative algebra*, Third Edition, Springer, 2007.

[CLO2-2000] D. Cox, J. Little, D. O'Shea, *Using algebraic geometry*, Second Edition, Springer, 2000.

[H-1948] W. Habicht, *Eine Verallgemeinerung des Sturmschen Wurzelzahlverfahrens*, Commun. Math. Halvetici 21, 1948, 99–116.

[GL-2007] J. von zur Gathen, T. Lücking, *Subresultants revisited*, Theoretical Computer Science 297, 2003, 199–239.

[K-2003] M. El Kahoui, *An elementary approach to subresultants theory*, Journal of Symbolic Computation 35, 2003, 281–292.

[K-1969] B. Krawczyk, *Newton-Algorithmen zur Bestimmung von Nullstellen mit Fehlerschranken*, Computing 4, 1969, 187–201.

[LRS-2001] H. Lombardi, M.-F. Roy, M. Safey, *New structure theorem for subresultants*, Special Issue Symbolic Computation in Algebra, Analysis, and Geometry, Journal of Symbolic Computation 29, 2000, 663–690.

[MKC-2009] R. E. Moore, R. B. Kearfott, M. C. Cloud, *Introduction into intervall analysis*, Society for Industrial and Applied Mathematics Philadelphia, 2009.

[N-1990] A. Neumaier, *Intervall methods for systems of equations*, Encyclopedia of Mathematics and its Applications, Cambridge University Press, 1990.

[T-1973] B. Teissier, *Cycles évanescents, section planes et conditions de Whitney*, Astérisque 7 et 8, 1973.