12-17-2014 12:00 AM

Computing Intersection Multiplicity via Triangular Decomposition

Paul Vrbik
The University of Western Ontario

Supervisor
Dr. Marc Moreno Maza
The University of Western Ontario Joint Supervisor
Dr. Eric Schost
The University of Western Ontario

Graduate Program in Computer Science
A thesis submitted in partial fulfillment of the requirements for the degree in Doctor of Philosophy

Computing Intersection Multiplicity via Triangular Decomposition

(Thesis format: Monograph)

by

Paul Vrbik

Graduate Program in Computer Science

A thesis submitted in partial fulfillment
of the requirements for the degree of
Doctor of Philosophy

The School of Graduate and Postdoctoral Studies
The University of Western Ontario
London, Ontario, Canada

Abstract

Fulton's algorithm is used to calculate the intersection multiplicity of two plane curves about a rational point. This work extends Fulton's algorithm first to algebraic points (encoded by regular chains) and then, with some generic assumptions, to ℓ many hypersurfaces.

Out of necessity, we give a standard-basis free method (i.e. practically efficient method) for calculating tangent cones at points on curves.

Keywords. Algebraic geometry, Computer Algebra, Intersection Multiplicity, Intersection Number, Fulton's Algorithm, Tangent Cone.

For DLM — hero of listening.

Acknowledgments

I wish to thank...

My co-supervisors Dr. Marc Moreno Maza and Dr. Éric Schost who have spent a sensational amount of time and energy training me. For their patience, wisdom, and guidance I am deeply grateful.

Marc for choosing a good problem — the fact we were able to develop a comprehensive solution is a testament to his good judgement and intuition.

Éric for shaping my loose ideas into algorithms and my 'proofs' into proofs — I truly benefited from his extensive experience and keen eye.

My long-time friend Dr. Steffen Marcus. His role as our (very) pure mathematician consultant was critical for this work.

Dr. Michael Monagan for flying me out to Vancouver each summer and Roman Pearce for buying me dinner at every conference we have attended together.

The good people of ORCCA and the department's support staff: thanks for putting up with me.

Contents

Abstract ii

Dedication iii

Acknowledgments iv

Table of Contents vii

0 Introduction 1

0.1 First Example . . . 2
0.2 Contributions . . . 3
0.3 Review of Literature . . . 5
0.4 Summary . . . 6

1 Ideals and Varieties 7

1.1 Polynomials . . . 7
1.1.1 Monomial Orderings . . . 8
1.1.2 Operations on Polynomials . . . 9
1.1.3 Polynomial Remainder Sequences . . . 11
1.1.4 Solving Polynomials . . . 13
1.2 Ideals and Varieties . . . 14
1.2.1 Varieties . . . 14
1.2.2 Ideals . . . 15
1.2.3 The Ideal Variety Correspondence . . . 16
1.2.4 Prime Ideals and Irreducible Varieties . . . 17
1.3 The Dimension of an Ideal . . . 18

2 Regular Chains 19

2.1 Solving 19
2.2 Triangular Sets 21
2.2.1 Properties of Triangular Sets 22
2.3 Regular Chains 23
2.3.1 Shedding Bad Initials 24
2.3.2 Specializing at Regular Chains 26
2.4 Triangularization 26
2.5 Splitting and the D5 Principle 28
2.5.1 Regularize 29

3 Intersection Multiplicity **32**
3.1 Bivariate Intersection Multiplicity 32
3.2 Fulton's Properties 35
3.3 Extending Fulton's Properties 37

4 Fulton's Algorithm for Regular Chains **45**
4.1 Descriptions 45
4.2 Valuations 47
4.3 Maximal Ideals 49
4.4 Non-Splitting Case 50
4.5 Splitting Case 55

5 Tangent Cones **58**
5.1 Singularities 58
5.2 Homogeneous Components 60
5.2.1 Classical Tangent Cone Definition 62
5.2.2 Secants 64
5.3 Tangent Cone Algorithm 64
5.3.1 Equations of Tangent Cones 71
5.3.2 Examples 72

6 Extended Fulton's Algorithm **77**
6.1 Transversality 77
6.2 Cylindrification 81
6.3 Algorithms 84

7 Experiments **89**
7.1 Examples from literature 92
7.1.1 Characteristic 101 92
7.1.2 Characteristic 962 592 769 95
7.1.3 Characteristic 0 99
7.2 Random Case Testing (Bivariate) 103
7.3 Comparison to other systems 106
7.3.1 Magma 106

Chapter 0

Introduction

In algebraic geometry, the intersection multiplicity of two planar curves is an important quantity for it provides valuable information about the number of times these curves meet. This notion extends to the study of three surfaces and generalizes to ℓ hypersurfaces in an ℓ-dimensional space. It is useful to use this number to confirm all solutions are accounted for when solving a polynomial system, where the geometry may not be apparent.

As pointed out by Fulton in his "Intersection Theory" [14] the intersection multiplicities of two plane curves satisfy a series of seven properties which uniquely define this number at each of the common points of these curves. Moreover, the proof of this (remarkable) fact is constructive, yielding (what we call) *Fulton's algorithm*. This construction, however, is not given in spaces of dimension greater than two or at points that lie outside the (usually rational) coefficient field.

There are some barriers towards realizing a practical implementation of this algorithm. The main one is that computer algebra systems efficiently manipulate multivariate polynomials only when their coefficients are in the field of rational numbers or in a prime field. Nonetheless there are efficient algorithms [8] for decomposing algebraic varieties which rely only on field-operations and avoid explicit implementation of non-rational numbers.

In this manuscript: we extend Fulton's algorithm to work at any point, rational or not; give algorithmic criteria for reducing the case of ℓ variables to the (known) bivariate case; and (out of necessity) give a standard

basis free algorithm for calculating tangent cones to make our reduction condition computational tractable to determine.

§0.1 First Example

Consider the intersection of the parabola $y = x^2$ with a line $(y - b) = m(x - a)$. The line and parabola meet at two distinct points *except* at the point $p = (a, b)$ when $m = 2a$. Here the line is the tangent at p of the parabola and the intersection multiplicity of the two curves at p equals two.

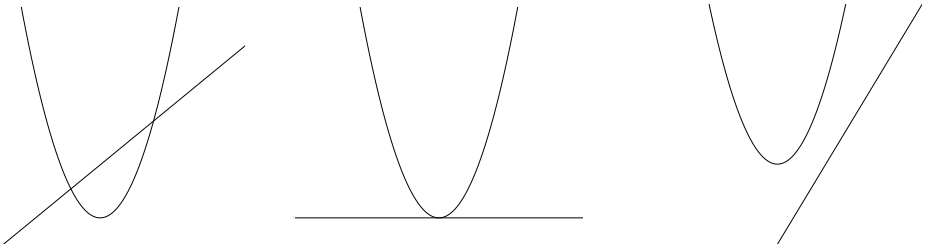


Figure 1: The various intersections of a line and parabola corresponding to (resp.): two intersections of intersection multiplicity 1, one tangential intersection of intersection multiplicity 2, and two complex intersections with intersection multiplicity 1.

Within the pure-mathematical spectrum the intersection multiplicity provides insight into the local geometry of zero dimensional varieties. In this setting, the invariant is defined as the number of tangent lines at each point of intersection. The (practical) difficulty this introduces is the necessity to determine transversality with tangent *cones* at points with non-simple intersection (i.e. where more than one tangent is needed to locally approximate the zero-dimensional variety under study).

This transversality testing was a significant obstacle as there was (up to our knowledge) no efficient symbolic algorithms for computing tangent cones. That is to say, all alternatives required an expensive Gröbner basis calculation in some way.

§0.2 Contributions

There are three main contributions of this work:

We extend Fulton's algorithm to work about zero-dimensional regular chains which enables the calculation of intersection multiplicities at points in the algebraic closure of the coefficient field. Three procedures for calculating the intersection multiplicity of two planar curves are given. The first is designed to work at a point p, the second at an irreducible zero-dimensional regular chain, and the last at arbitrary zero-dimensional regular chains.

We also extend Fulton's seven properties from two variables to $\ell + 1$ variables and provide an algorithmic criterion which allows for recursing the calculation of the intersection multiplicity in $\ell + 1$ variables to ℓ variables. As a caveat our criterion involves the manipulation of a tangent cone which is often computationally prohibitive to obtain.

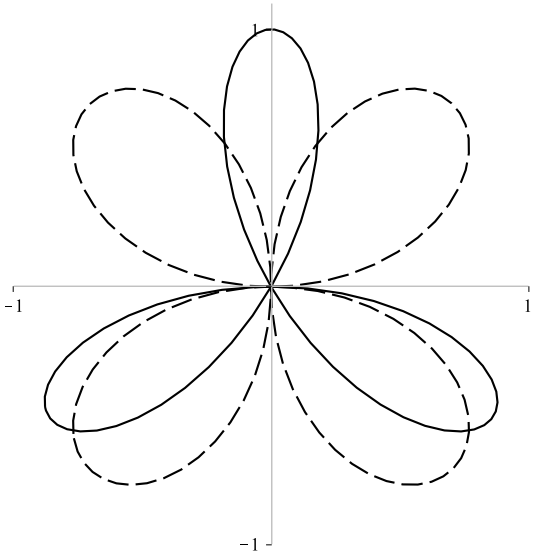
Fortunately, we give a standard-basis free method (i.e. practically efficient method) for calculating tangent cones at points on curves. This, in itself, is an important contribution as there was no efficient method for calculating tangent cones before.

These algorithms have been implemented in the MAPLE language as a sub-package of the `RegularChains` library. The Maple sessions in Table 1 and Table 2 illustrate computations with this package.

Consequently, we obtain a practical algorithm for computing intersection multiplicities of zero-dimensional varieties. The novelty of our approach is attributed to an important feature which is conducive to performance. Since we only require a triangular decomposition of a variety V — computed by *any* available method — we can operate without trying to 'preserve' any multiplicity information. Once V is decomposed, we are able to work 'locally' at each regular chain.

There are special cases where our algorithmic criterion for reducing computations with $\ell + 1$ variables to ℓ variables does not apply and, thus, where our algorithm fails. However, these exceptional cases are highly degenerate and rarely occur naturally.

```
> with(RegularChains):
> with(RegularChains:-AlgebraicGeometryTools):
> h := [ (x^2 + y^2)^2 + 3x^2*y - y^3, (x^2 + y^2)^3 - 4x^2*y^2 ]:
> plots[implicitplot](h, x = -2..2, y = -2..2);
```




```
> R := PolynomialRing( [x, y], 101 ):
> TriangularizeWithMultiplicity( h, R ):
```

$$\left[\left[1, \left\{ \begin{array}{c} x-1 \\ y+14 \end{array} \right\}\right], \left[1, \left\{ \begin{array}{c} x+1 \\ y+14 \end{array} \right\}\right], \left[1, \left\{ \begin{array}{c} x-47 \\ y-14 \end{array} \right\}\right], \left[1, \left\{ \begin{array}{c} x+47 \\ y-14 \end{array} \right\}\right], \left[14, \left\{ \begin{array}{c} x \\ y \end{array} \right\}\right]\right]$$

Table 1: MAPLE worksheet.

```
> with(RegularChains):
> with(RegularChains:-AlgebraicGeometryTools):
> h := [x^2 + y + z - 1, x + y^2 + z - 1, x + y + z^2 - 1]:
> R := PolynomialRing([x, y, z], 101):
> TriangularizeWithMultiplicity(h, R):
```

$$\left[\left[1, \left\{ \begin{array}{l} x - z \\ y - z \\ z^2 + 2z - 1 \end{array} \right\}\right], \left[2, \left\{ \begin{array}{l} x \\ y \\ z - 1 \end{array} \right\}\right], \left[1, \left\{ \begin{array}{l} x \\ y - 1 \\ z \end{array} \right\}\right], \left[2, \left\{ \begin{array}{l} x - 1 \\ y \\ z \end{array} \right\}\right]\right]$$

Table 2: MAPLE worksheet.

We note that the question of computing intersection numbers in space of dimension greater than two is known to be highly challenging, even from a theoretical point of view, as noted in [34].

§0.3 Review of Literature

The authors of [9] and [21] report algorithms with similar specifications to ours. The first is only applicable to the case of two input polynomials whereas [21] is not complete in the sense that it may not compute the intersection multiplicities of all regular chains in a triangular decomposition of the input system (even in the bivariate case).

There are also methods that do not use triangularization which work in the ℓ-variate setting: Mora gave an algorithm for calculating standard bases using weak normal forms which can be used to calculate the intersection multiplicity *at the origin* via its classical definition (i.e. the dimension of the local quotient ring) [26, 1, 25]. One could use a method from Mourrain [29, §4.2] which uses repeated linear system solving to calculate a basis of the local ring. This is sufficient to deduce the intersection multiplicity but again only for those points at the origin. In all cases, these methods are limited to those ideals for which a Gröbner basis can be obtained. This is problematic especially if one introduces an additional variable to shift the input system to the origin.

Finally the computer algebra systems MAGMA and SINGULAR provide (resp.) `IntersectionNumber` [22, Example H84E6] and `iMult` [31] which calculate intersection multiplicities using (resp.) [16, Chapter I, Exercise 5.4] and standard basis techniques. However in both cases *only the sum of the intersection multiplicities* are counted and in fact some tangent lines may be counted twice, leading to over-counting.

§0.4 Summary

This manuscript is organized as follows:

1. Chapter 1 is introduces the definitions and notations required to describe the theory;
2. Chapter 2 is an overview of triangular sets, regular chains, and triangular decomposition;
3. Chapter 3 recounts a general introduction of intersection theory (in particular the intersection multiplicity) and contains the algorithm for computing intersection multiplicity at points from an algebraic closure;
4. Chapter 4 builds the extension to Fulton's algorithm which works at irrational points;
5. Chapter 5 describes the tangent cone, its (classical) computation using standard basis, and our alternate method which uses triangular decomposition;
6. Chapter 6 contains our criterium for recursing the calculation of an intersection multiplicity in $\ell + 1$ variables to ℓ variables; and finally
7. Chapter 7 reports experimental results.

Chapter 1

Ideals and Varieties

This chapter introduces the definitions and notations required to describe the theory in such a way to make implementation clear. The basic concepts and operations on rings, ideal, and varieties are defined as well as the notion of the dimension of an ideal and variety.

§1.1 Polynomials

In what follows, for the entirety of this work, $\mathscr{R}$ is a ring, $\mathscr{F}$ is a field, and $\overline{\mathscr{F}}$ is the algebraic closure of $\mathscr{F}$.

Polynomials are comprised of finite sums of monomials, which are in turn finite products of variables. So let $\mathbb{N}$ be the natural numbers and

$$\mathbf{x} := \{x_0, \ldots, x_\ell\} : \ell \in \mathbb{N}$$

be a finite set of variables.

An arbitrary (but finite) product of variables is a *monomial*.

Definition 1.1 (Monomials)**.** The *monomials* over variables $\mathbf{x}$:

$$[\mathbf{x}] := \left\{ x_0^{d_0} \cdots x_\ell^{d_\ell} : (d_0, \ldots, d_\ell) \in \mathbb{N}^{\ell+1} \right\} = \left\{ \mathbf{x}^{\mathbf{d}} : \mathbf{d} \in \mathbb{N}^{\ell+1} \right\}.$$

(Note: $1 \in [\mathbf{x}]$ and $0 \notin [\mathbf{x}]$.)

The product of a monomial m and c from the ring $\mathscr{R}$ (called m's *coefficient*) is a *term*.

Definition 1.2 (Terms)**.** The *terms* with monomials from $[\mathbf{x}]$ and coefficients from the ring $\mathscr{R}$ are given by

$$[\mathbf{x}]_{\mathscr{R}} := \{cm : c \in \mathscr{R},\ m \in [\mathbf{x}]\}.$$

And finally, a finite sum of terms is a *polynomial*, the comprehensive set of which form a ring.

Definition 1.3 (Polynomial Ring)**.** Polynomials with variables $\mathbf{x}$ over the coefficient ring $\mathscr{R}$:

$$\mathscr{R}[\mathbf{x}] := \{\sum_{t \in \mathbf{t}} t : \mathbf{t} \subseteq [\mathbf{x}]_{\mathscr{R}} \text{ and } |\mathbf{t}| < \infty\}.$$

Equivalent and more common representations of the polynomial ring are:

$$\mathscr{R}[\mathbf{x}] = \{f_0 + \cdots + f_s : f_0, \ldots, f_s \in [\mathbf{x}]_{\mathscr{R}} \text{ and } s < \infty\}$$

and $\mathscr{R}[\mathbf{x}] = \sum c_\alpha x_0^{\alpha_0} \cdots x_\ell^{\alpha_\ell}$ for $c_\alpha \in \mathscr{R}$.

§Monomial Orderings

To impose some canonical form on our polynomials we strive to write terms in *descending* degree as in

$$5x^3 + 2x^2 + 7x + 3.$$

The same can be done with arbitrary polynomials from $\mathscr{R}[\mathbf{x}]$ provided all but one variable is 'demoted' to the coefficient ring. (The subsequent one variable polynomial is said to be *univariate*.)

Example 1.1. The polynomial

$$xyz + y^3 + x^3 + x^2z \in \mathscr{R}[x, y, z]$$

re-written as a univariate polynomial in x with descending degree:

$$x^3 + (z)x^2 + (yz)x + \left(y^3\right) \in \mathscr{R}[y, z][x].$$

The brackets on (z), (yz), and (y^3) are meant to emphasize these 'monomials' are taken from the *coefficient* ring $\mathscr{R}[x, y]$.

Operations on univariate polynomials can be extended to multivariate polynomials provided the coefficients still form a ring. So, viewing multivariate polynomials as univariate (in what we later call the *main variable*) is something we do frequently.

Generally, any total ordering $\prec$ of $[\mathbf{x}]$ (that is, an order satisfying

$$\begin{aligned} u \prec v \text{ and } v \prec u &\implies u = v && \text{antisymmetry,} \\ u \prec v \text{ and } v \prec w &\implies u \prec w && \text{transitivity, and} \\ [\, u \prec v \text{ or } v \prec u \,] &\equiv \top && \text{totality} \end{aligned}$$

$\forall\, u, v, w \in [\mathbf{x}]$) is a *monomial ordering* when the ordering respects multiplication and has 1 ordered least.

Definition 1.4 (Monomial ordering)**.** Let u, v and w be monomials from $[\mathbf{x}]$ and $\succ : [\mathbf{x}] \to \{\top, \bot\}$ be an ordering. The predicate $\succ$ is a monomial ordering when $\succ$ is a *total ordering* and

1. $\forall\, w \in [\mathbf{x}];\ u \succ v \implies uw \succ vw$, and
2. $\forall\, u \in [\mathbf{x}];\ u \succ 1$.

(As with the degree function we extend monomial orderings to terms by ignoring their coefficients.)

§Operations on Polynomials

Definition 1.5 (deg)**.** The *total degree* of

1. a monomial $x_0^{d_0} \cdots x_\ell^{d_\ell} \in [\mathbf{x}]$ is

$$\deg(x_0^{d_0} \cdots x_\ell^{d_\ell}) := d_0 + \cdots + d_\ell;$$

2. a term $cm \in [\mathbf{x}]_{\mathscr{R}}$ such that $c \neq 0$ is

$$\deg(cm) := \deg(m);$$

3. a polynomial $c_0m_0 + \cdots + c_sm_s$ with $m_i \neq m_j$ and $c_i \neq 0$ is

$$\deg(c_0m_0 + \cdots + c_sm_s) := \max(\deg(c_0m_0), \ldots, \deg(c_sm_s)),$$

and following convention $\deg(0) := -\infty$.

Example 1.2. In $\mathscr{R}[x, y, z]$

$$\deg\big(x^3 + y^2 + xy^2z\big) = \max\big(\deg\big(x^3\big), \deg\big(y^2\big), \deg\big(x^2yz\big)\big) = 4.$$

We may also take the degree of a polynomial $h \in \mathscr{R}$ in x for any $x \in \mathbf{x}$. This is simply the total degree of h when taken as univariate in x. Denote this value by $\deg_x(h)$.

Example 1.3. $h = x^3 + y^2 + xy^2z \in \mathscr{R}[x, y, z]$ has $\deg_x(h) = 3$, $\deg_y(h) = 2$, and $\deg_z(h) = 1$.

Let us devote some notation for deconstructing and identifying the pieces of a polynomial.

Definition 1.6. Assume $c_0, \ldots, c_s \in \mathscr{R} - \{0\}$, $\{m_0, \ldots, m_s\} \subseteq [\mathbf{x}]$, $m \in [\mathbf{x}]$, and $f = c_0m_0 + \cdots + c_sm_s \in \mathscr{R}[\mathbf{x}]$. Let

1. $\text{terms}(f) := \{c_0m_0, \ldots, c_sm_s\}$ be the *terms* of f,
2. $\text{monos}(f) := \{m_0, \ldots, m_s\}$ be the *monomials* of f, and
3. $\text{indets}(m) := \big\{x \in \mathbf{x} : x \,\big|\, m\big\}$ be the *indeterminates* of a monomial m, and
4. $\text{indets}(f) := \cup(\text{indets}(m) : m \in \text{monos}(f))$ be the indeterminates of the polynomial f.

Example 1.4. Let $f = x^3 + 2y^2 + 3xy^2z$ then $\text{terms}(f) = \{x^3, 2y^2, 3xy^2z\}$, $\text{monos}(f) = \{x^3, y^2, xy^2z\}$, and $\text{indets}(f) = \{x, y, z\}$.

The leading term of a polynomial is then the 'largest' term with respect to a monomial ordering; the leading coefficient is the coefficient from the leading term.

Definition 1.7 (Leading Term)**.** The *leading term* and *leading monomial* of a polynomial $f \in \mathscr{R}[\mathbf{x}]$ with respect to a monomial ordering $\succ$ are given by

$$\ell t(f) := \max_{\succ}(t : t \in \text{terms}(f)) \quad \text{and} \quad \ell m(f) := \max_{\succ}(m : m \in \text{monos}(f))$$

and the *leading coefficient* is

$$\ell c(f) := \frac{\ell t(f)}{\ell m(f)}.$$

Example 1.5. Let $f = x^3 + 2y^2 + 3xy^2z$ be taken univariate in y with coefficients from $\mathscr{R}[x, z]$, that is $y \succ x \succ z$, then

$$\ell t(f) = 2y^2 + 3xy^2z, \qquad \ell m(f) = y^2, \quad \text{and} \quad \ell c(f) = 3xz + 2.$$

§Polynomial Remainder Sequences

We enumerate the basic polynomial remainder sequences.

Proposition 1.1. Let $\mathscr{F}$ be a field and g a nonzero polynomial in $\mathscr{F}[x]$. For any $f \in \mathscr{F}[x]$ there are *unique* q, $r \in \mathscr{F}[x]$ such that

$$f = q \cdot g + r : \deg_x(r) < \deg_x(g).$$

Proof. See [11, Ch. 1 §5 Proposition 2.] where the division algorithm is outlined. □

Definition 1.8 (Quotient and Remainder)**.** The polynomials q and r from Proposition 1.1 are called the *quotient* and *remainder* and are denoted by $\text{quo}(f, g; x)$ and $\text{rem}(f, g; x)$. They satisfy

$$f = \text{quo}(f, g; x) \cdot g + \text{rem}(f, g; x) : \deg_x(\text{rem}(f, g; x)) < \deg_x(g).$$

Notation (French long division)**.** Let f, g, q, $r \in \mathscr{F}[x]$ then

$$\begin{array}{r|l} f & g \\ \hline r & q \end{array} \iff f = qm + r \text{ and } \deg(r) < \deg_{\cdot}(m)$$

We sometimes require that $\mathscr{F}$ is the fraction field of a domain $\mathscr{R}$; for instance, $\mathscr{R}$ may be the polynomial ring $\mathbb{Q}[y]$, and $\mathscr{F}$ is the rational function field $\mathbb{Q}(y)$. In this case, even if f and g are in $\mathscr{R}[x]$, the quotient and remainder may lie in $\mathscr{F}[x]$.

For instance, let $f = x^4 + 1$ and $g = xy^2 + 1$ and note

$$f = \frac{x^3y^6 - x^2y^4 + xy^2 - 1}{y^8} \cdot g + \frac{y^8 - 1}{y^8}$$

where thereby

$$\operatorname{rem}(f,\, g;\, x) = \frac{y^8 - 1}{y^8} \quad \text{and} \quad \operatorname{quo}(f,\, g;\, x) = \frac{x^3y^6 - x^2y^4 + xy^2 - 1}{y^8}.$$

A premultiplication can be done to preclude this possibility. We call the quotient and remainder calculated using premultiplications the *pseudo-remainder* and *pseudo-quotient*.

Proposition 1.2. Let f, $g \in \mathscr{R}[\mathbf{x}]$ and let $x \in \mathbf{x}$. Assume $\deg_x(f) < \deg_x(g)$ and $g \neq 0$. There are *unique* $q \in \mathscr{R}[\mathbf{x}]$ and $r \in \langle f,\, g \rangle$ such that

$$m \cdot f = q \cdot h + r : \deg_x(r) < \deg_x(b)$$

where $m = \ell c_x(g)^{\deg_x(f) - \deg_x(g) + 1}$

Proof. See [11, Ch. 6 §6 Proposition 1] where the pseudo-division algorithm is outlined. □

Definition 1.9 (Pseudo-quotient and Pseudo-Remainder)**.** Take the settings of Proposition 1.2. The polynomial r is called the *pseudo-remainder* in x and is denoted by $\operatorname{prem}(f,\, g;\, x)$. Thus

$$m \cdot f = \operatorname{quo}(f,\, g;\, x) \cdot g + \operatorname{prem}(f,\, g;\, x) : \deg_x(r) < \deg_x(g),$$

where $m = \ell c_x(g)^{\deg_x(f)-\deg_x(g)+1}$.

Example 1.6 (Pseudo-Remainder)**.** Let $f = x^4 + 1$ an $g = xy^2 + 1$ and note

$$\big(y^3\big) \cdot f = \big(xy^2 - y\big) \cdot g + \big(y^3 - y\big).$$

Thus $\operatorname{prem}(f,\, g;\, x) = (y^3 - y)$.

§Solving Polynomials

Polynomials define *polynomial mappings* from *affine spaces* into *base fields*.[1]

Definition 1.10 (Affine Space)**.** For $\mathscr{F}$ a field,

$$\mathbb{A}^{\ell+1}(\mathscr{F}) := \underbrace{\mathscr{F} \times \cdots \times \mathscr{F}}_{\ell+1\text{-times}}$$

is called an *affine space*.

For these mappings we adopt the familiar *function notation*. That is, when $f \in \mathscr{F}[\mathbf{x}]$ and $p = (p_0,\, \ldots, p_\ell) \in \mathbb{A}^{\ell+1}(\mathscr{F})$ we take

$$f(p) := f(p_0, \ldots, p_\ell)$$

and let a polynomial map be given by the following.

Definition 1.11 (Polynomial Mapping)**.** For $\mathscr{F}$ a field and $f \in \mathscr{F}[\mathbf{x}]$, the *polynomial map* given by f is

$$\begin{aligned} f : \mathbb{A}^{\ell+1}(\mathscr{F}) &\to \mathscr{F} \\ p &\mapsto f(p). \end{aligned}$$

Recall the *kernel* of a mapping is the subset of its domain which maps to zero. *Solving* a polynomial typically means deducing some or perhaps all of this *kernel* (also called the *nullspace*).

[1] Really base rings, but in our setting this is never required.

Definition 1.12 (Kernel)**.** Let $\mathscr{F}$ be a field and $f \in \mathscr{F}[\mathbf{x}]$. Let

$$\ker(f) := \big\{p \in \mathbb{A}^{\ell+1}(\mathscr{F}) : f(p) = 0\big\}.$$

Importantly, the kernel depends on the coefficient field. For instance $f = (x^2 - 2)(x^2 + 1) \in \mathscr{F}[x]$ can have zero, two, or four roots:

$\mathscr{R}$	$\ker(f)$
$\mathbb{Q}$	$\varnothing$
$\mathbb{R}$	$\{\pm\sqrt{2}\}$
$\mathbb{C}$	$\{\pm\sqrt{2},\ \pm i\}$

.

§1.2 Ideals and Varieties

Much in the same way vector spaces are comprised of linear combinations of vectors, ideals are comprised of polynomial combinations of polynomials. They were first introduced by Richard Dedekind in 1876 as a generalization of ideal numbers [33].

Varieties arise as the kernel of these ideals and correspond to sets of points where the polynomials of the ideal vanish (i.e. become zero) simultaneously. It is important that ideals are representable by computers while simultaneously representing infinitely large kernels. The broader ideal/variety correspondence allows for the conversion between geometric and algebraic points of view.

§Varieties

Any subset of affine space which is the solution set of a system of polynomials is called a variety. A variety can be viewed as a function from $\mathscr{P}(\mathscr{F}[\mathbf{x}])$ (*powerset* of A) to $\mathbb{A}^{\ell+1}(\mathscr{F})$ which computes the set of points where a finite set of polynomials vanish simultaneously:

$$\ker(f_0) \cap \cdots \cap \ker(f_s).$$

This is the natural way of extending the kernel to that of systems of polynomials.

Definition 1.13 (Variety)**.** Let $\mathbf{f} = \{f_0, \ldots, f_s\} \subseteq \mathscr{F}[\mathbf{x}]$, for $\mathscr{F}$ a field, and

$$\mathbf{V}(f_0, \ldots, f_s) := \ker(f_0) \cap \cdots \cap \ker(f_s).$$

$V \subseteq \mathbb{A}^{\ell+1}(\mathscr{F})$ is called a *variety* when $\exists\, \mathbf{f} \subseteq \mathscr{F}[\mathbf{x}] : V = \mathbf{V}(\mathbf{f})$.

Example 1.7. Let $\mathbf{f} = \{y - x^2,\, y - x\} \subseteq \mathscr{F}[x, y]$ (the parabola and line through the origin).

$$\begin{aligned}\mathbf{V}\big(y - x^2,\, y - x\big) &= \ker\big(y - x^2\big) \cap \ker(y - x) \\ &= \big\{\big(p,\, p^2\big) : p \in \mathscr{F}\big\} \cap \{(p,\, p) : p \in \mathscr{F}\} \\ &= \{(0, 0),\, \{1, 1\}\}.\end{aligned}$$

It is these varieties we wish to encode, and their points/elements we wish to classify.

§Ideals

Observe $\ker : \mathscr{F}[\mathbf{x}] \to \mathbb{A}^{\ell+1}(\mathscr{F})$ is *not* injective; there can be many (if not infinitely many) polynomials with equivalent kernel:

$$\ker(x - 1) = \ker(2x - 2) = \ker(3x - 3) = \cdots = \{1\}.$$

Not only this, we also require polynomials whose kernels *inlude* $\{1\}$.

Definition 1.14 (Ideal)**.** Let $I \subseteq \mathscr{F}[\mathbf{x}]$. I is an *ideal* when

1. $0 \in I$,
2. $f,\, g \in I \implies f + g \in I$,
3. $f \in I$ and $h \in \mathscr{F}[\mathbf{x}] \implies hf \in I$.

Definition 1.15 (Ideal Brackets)**.** Let $V \subseteq \mathbb{A}^{\ell+1}(\mathscr{F})$ and $\mathbf{I}(V)$, *the ideal defined by* V, be the set of all polynomials which vanish on V:

$$\mathbf{I}(V) := \{f \in \mathscr{F}[\mathbf{x}] : V \subseteq \ker(f)\}.$$

We use *ideal brackets* to represent these infinite sets. That is when $\mathbf{f} \subseteq \mathscr{F}[\mathbf{x}]$:

$$\langle \mathbf{f} \rangle := \Big\{ \sum_{f \in \mathbf{f}} c_f f : c_f \in \mathscr{F}[\mathbf{x}] \Big\}.$$

Proposition 1.3. For any $\mathbf{f} = \{f_0, \ldots, f_\ell\} \subseteq \mathscr{F}[\mathbf{x}]$ we have $\langle \mathbf{f} \rangle$ is an ideal.

Proof. See [11, Ch. 1 §4 Lemma 1.]. □

For more on Ideals, Varieties, and Algorithms see [11].

§The Ideal Variety Correspondence

The correspondence between varieties and ideals is important as it translates problems of geometry into problems of algebra. The practical upshot of this is an encoding of geometric problems with objects that can be manipulated with computers. Hilbert's Nullstellensatz (German for "theorem of zeros" or more literally "zero-locus-theorem") along with its weak and strong versions gives the precise relationship between algebra and geometry.

Theorem 1.1 (Hilbert's Nullstellensatz)**.** Let $\mathbf{f} \subseteq \overline{\mathscr{F}}[\mathbf{x}]$ then

$$f \in \mathbf{I}(\mathbf{V}(\mathbf{f})) \iff \exists\, m \in \mathbb{N}^{>0} : f^m \in \langle \mathbf{f} \rangle$$

Proof. [10, Ch. 4 §1 Theorem 1]. □

When $f^m \in \langle \mathbf{f} \rangle$ for $m \in \mathbb{N}$ implies $f \in \langle \mathbf{f} \rangle$ the ideal is said to be *radical* and any ideal can be made radical by simply including those required f's in the ideal — the resulting set is still an ideal.

Definition 1.16 (Radical)**.** Let $\mathbf{f} \subseteq \mathscr{F}[\mathbf{x}]$ and $\langle \mathbf{f} \rangle$ be an ideal. The *radical of* $\langle \mathbf{f} \rangle$ is given as follows.

$$\sqrt{\langle \mathbf{f} \rangle} := \left\{ f : \exists\, m \in \mathbb{N}^{>0};\, f^m \in \langle \mathbf{f} \rangle \right\}$$

This enables us to write the *Strong Nullstellensatz* which states the ideal-variety correspondence is exact for radical ideals.

Theorem 1.2 (Strong Nullstellensatz)**.** Let $\mathbf{f} \subseteq \overline{\mathscr{F}}[\mathbf{x}]$ then

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

Proof. [10, Ch. 4 §2 Theorem 6]. □

§Prime Ideals and Irreducible Varieties

Definition 1.17 (Irreducible Variety)**.** A variety V is irreducible if and only if when $V = V_0 \cup V_1$ then either $V = V_0$ or $V = V_1$.

For instance $\mathbf{V}(xz,\, yz)$ is *not* an irreducible variety because $\mathbf{V}(xz,\, yz) = \mathbf{V}(x) \,\cup\, \mathbf{V}(z,\, y)$. Whereas the variety $\mathbf{V}(y - x^2,\, z - x^3)$ *is* irreducible, though this takes some work to prove. The key is to move from a geometric point of view to an algebraic one. This transformation leads to the notion of *prime ideals* which correspond to irreducible varieties.

Definition 1.18 (Prime Ideal)**.** An ideal $\langle \mathbf{f} \rangle$ of $\mathscr{F}[\mathbf{x}]$ is *prime* if whenever $gh \in \langle \mathbf{f} \rangle$ then $g \in \langle \mathbf{f} \rangle$ or $h \in \langle \mathbf{f} \rangle$.

Proposition 1.4. Let V be an affine variety of $\mathbb{A}^{\ell+1}\big(\overline{\mathscr{F}}\big)$. V is irreducible if and only if $\mathbf{I}(V)$ is prime ideal.

Proof. See [11, Ch. 4 §5 Proposition 3]. □

When working over an algebraically closed field $\overline{\mathscr{F}}$ then the correspondence between prime ideals and irreducible varieties is one-to-one.

Finally, *maximal ideals* are ones whose only proper superset is the entire polynomial ring it resides in.

Definition 1.19 (Maximal Ideal)**.** Let $\mathbf{f} \subseteq \mathscr{F}[\mathbf{x}]$ with $\langle \mathbf{f} \rangle \neq \mathscr{F}[\mathbf{x}]$. The ideal $\langle \mathbf{f} \rangle$ is *maximal* when for any $\mathbf{g} \subseteq \mathscr{F}[\mathbf{x}]$ where $\langle \mathbf{f} \rangle \subseteq \langle \mathbf{g} \rangle$ either $\langle \mathbf{f} \rangle = \langle \mathbf{g} \rangle$ or $\langle \mathbf{g} \rangle = \mathscr{F}[\mathbf{x}]$.

Importantly, any ideal of the form $\langle \mathbf{x} - \mathbf{p} \rangle = \langle x_0 - p_0, \ldots, x_\ell - p_\ell \rangle$ is maximal in $\mathscr{F}[\mathbf{x}]$ (e.g. $\langle x - 2, y - 4 \rangle$ is maximal in $\mathscr{F}[\mathbf{x}]$).

§1.3 The Dimension of an Ideal

Hilbert's insight was characterizing the dimension of an ideal by the number of monomials *not* in the ideal (i.e. in the ideals complement) [11, Ch. 9 §3].

This number is given by the so-called *Hilbert Polynomial* whose degree is already a definition for the dimension of a variety. Crucially, the *monomial* ideal $\langle \ell t(h : h \in \langle \mathbf{h} \rangle) \rangle$ has the same Hilbert Polynomial as $\langle \mathbf{h} \rangle$ when the leading terms are taken with a *graded* monomial ordering (e.g. one that orders by total degree first and breaks ties somehow).

However, for our purposes it is sufficient to take [11, Ch. 9 §5 Corollary 3.] as definition for dimension.

Definition 1.20. Let $V \subseteq \mathbb{A}^{\ell+1}(\mathscr{F})$ be an affine variety and assume $\mathbf{I}(V) \subseteq \mathscr{F}[\mathbf{x}]$. The dimension of V is given by the largest (by cardinality) $\mathbf{y} \subseteq \mathbf{x}$ satisfying $\mathbf{I}(V) \cap \mathscr{F}[\mathbf{y}] = \{0\}$. That is to say, there are no polynomials in $\mathbf{I}(V)$ with variables in $\mathbf{y}$ other than the zero polynomial.

> The Zariski closure of a subset $S \subseteq \mathbb{A}^{\ell+1}(\mathscr{F})$ is the smallest (by set inclusion) affine variety $\mathbf{V}(\mathbf{h}) : \mathbf{h} \subseteq \mathscr{F}[\mathbf{x}]$ which is a superset to it. $\overline{S}$ denotes the Zariski closure of S and $\mathbf{V}(\mathbf{I}(S)) = \overline{S}$.

Geometrically, the intersection $\mathbf{I}(V) \cap \mathscr{F}[\mathbf{y}]$ is $\{0\}$ only when the projection of V given by $\mathbf{x} \mapsto \mathbf{y}$ being almost surjective. Almost in this setting means that the image of the projection is Zariski dense, that is the Zariski closure of the projection fills the affine space which $\mathbf{y}$ defines.

Chapter 2

Regular Chains

The subsequent chapter develops the notion of a triangular set and regular chain from the basic goal of 'solving' a system of polynomials — in fact, even the idea of solving requires consideration. Among the options for encoding the solutions are Gröbner basis, triangular sets, and (of course) regular chains. The utility of using regular chains is that they satisfy conditions of algorithmic importance. In particular, using regular chains enables the exploitation of efficient "splitting algorithms" [6].

Triangular sets, but more specifically their specialization into regular chains, are the principal objects of study of this work. They are critically important to computer algebra systems for their part in solving systems of polynomials and cylindrical algebraic decomposition.

See [4, 17, 36] for a general overview of the theory of triangular sets and regular chains.

§2.1 Solving

'Solving' a system of polynomials, say $\mathbf{h} \subseteq \mathscr{F}[\mathbf{x}]$ for $\mathscr{F}$ a field, means different things in different contexts. In each case however the goal is the same: encode the zeros of the polynomial system somehow.

For proofs, one typically wants either a *primary decomposition* of $\langle \mathbf{h} \rangle$ or a *unique irreducible decomposition* of $\mathbf{V}(\mathbf{h})$. Though such a decomposition can be desirable, computing them is akin to multivariate factorization

which is computationally difficult. Additionally, these decompositions may not even be helpful for explicitly constructing points in $\mathbf{V}(\mathbf{h})$ and are not unique [15].

Example 2.1. Let $\mathbf{h} = \{x^2 + y + z - 1,\, x + y^2 + z - 1,\, x + y + z^2 - 1\} \subseteq \mathscr{F}[\mathbf{x}]$. A primary decomposition of $\langle \mathbf{h} \rangle$ is given by

$$\begin{aligned}
\langle \mathbf{h}'_0 \rangle &= \big\langle z - 1,\, z^2 + x + y - 1,\, x + y^2 + z - 1,\, x^2 + y + z - 1 \big\rangle, \\
\langle \mathbf{h}'_1 \rangle &= \big\langle z^2 + 2z - 1,\, z^2 + x + y - 1,\, x + y^2 + z - 1,\, x^2 + y + z - 1 \big\rangle, \\
\langle \mathbf{h}'_2 \rangle &= \big\langle y,\, z,\, z^2 + x + y - 1,\, x + y^2 + z - 1,\, x^2 + y + z - 1 \big\rangle, \\
\langle \mathbf{h}'_3 \rangle &= \big\langle z,\, y - 1,\, z^2 + x + y - 11,\, x + y^2 + z - 1,\, x^2 + y + z - 1 \big\rangle,
\end{aligned}$$

where $\langle \mathbf{h} \rangle = \langle \mathbf{h}'_0 \rangle \cap \cdots \cap \langle \mathbf{h}'_3 \rangle$.

Note that the bad shape of these ideals (as produced by Maple) makes them unsuitable for back substitution.

An alternative is to use Gröbner bases. Buchberger's algorithm allows for the computation of $\mathbf{g} \subseteq \mathscr{F}[\mathbf{x}]$ such that $\langle \mathbf{g} \rangle = \langle \mathbf{h} \rangle$ and (crucially) $\langle \ell t(h) : h \in \langle \mathbf{h} \rangle \rangle = \langle \ell t(g) : g \in \mathbf{g} \rangle$ for an arbitrary monomial ordering. Moreover, when reduced, these Gröbner bases are unique representations of the ideal.

Provided the basis is over a lexical monomial ordering, $\mathbf{g}$ satisfies the elimination condition that $\langle \mathbf{g} \rangle \cap \mathscr{F}[x_{n+1}, \ldots, x_\ell]$ is a Gröbner basis of the n-th elimination ideal. This property allows for a Gaussian-like back substitution.

Example 2.2. Let $\mathbf{h} = \{x^2 + y + z - 1,\, x + y^2 + z - 1,\, x + y + z^2 - 1\} \subseteq \mathscr{F}[x, y, z]$. A Gröbner basis of $\langle \mathbf{h} \rangle$ is

$$\begin{aligned}
\{&z^2 + x + y - 1, \\
&y^2 - z^2 - y + z, \\
&z^4 + 2yz^2 - z^2, \\
&z^6 - 4z^4 + 4z^3 - z^2\}.
\end{aligned}$$

Note the second step of back substitution here requires calculating the

roots of $y^2 - z^2 - y + z$ and $z^4 + 2yz^2 - z^2$ *simultaneously* for some $z \in \mathbf{V}(z^6 - 4z^4 + 4z^3 - z^2)$.

A third option and our preference is to use *triangular decomposition*. These decompositions are comparable to 'minimal' factorizations in the sense that only as many factors as necessary are calculated.

§2.2 Triangular Sets

Intuitively, triangular sets are comprised of polynomials with mutually different leading terms. The practical consequence of this is *back substitution* as it allows us to eliminate variables from the systems one by one. Regular chains emerge by enforcing increasingly stronger conditions on these triangular sets.

Definition 2.1 (Main Variable)**.** Let $\succ$ be an ordering of $\mathbf{x}$. The *main variable* of a term $t \in [\mathbf{x}]_{\mathscr{F}}$, and by extension a polynomial $f \in \mathscr{F}[\mathbf{x}]$, is given recursively

$$\begin{aligned} \operatorname{mvar}(t) &:= \max_{\succ}(v : v \in \operatorname{indets}(t)), \\ \operatorname{mvar}(f) &:= \max_{\succ}(\operatorname{mvar}(t) : t \in \operatorname{terms}(f)). \end{aligned}$$

Definition 2.2 (Triangular Set)**.** A set of polynomials with mutually different main variable is a *triangular set*. Let $\mathbb{T}(\mathscr{F}[\mathbf{x}])$ denote the class of *triangular sets* of $\mathscr{F}[\mathbf{x}]$, then

$$\mathbf{f}_{\triangle} \in \mathbb{T}(\mathscr{F}[\mathbf{x}]) \overset{\text{Defn.}}{\iff} \forall\, g, h \in \mathbf{f}_{\triangle} : g \neq h;\ \operatorname{mvar}(g) \neq \operatorname{mvar}(h),$$

and in particular when $|\mathbf{f}_{\triangle}| = |\mathbf{x}|$ we say $\mathbf{f}_{\triangle}$ is a *square triangular set*.

Example 2.3. A square triangular set of $\mathscr{F}[x \prec y \prec z \prec t]$.

$$\mathbf{f}_{\triangle} = \begin{cases} (yz-1)t + y^2 & \in \mathscr{F}[x,\, y,\, z,\, t] \\ xz^2 - 2yz + 1 & \in \mathscr{F}[x,\, y,\, z] \\ (x-1)y^2 - x & \in \mathscr{F}[x, y] \\ (x-1)(x+1) & \in \mathscr{F}[x]. \end{cases}$$

The shape of the polynomial rings as written form a triangle—the motivation for the name "triangular sets."

Triangular sets and regular chains are recursive so notation for breaking triangular sets into the 'top' and 'bottom' is prudent.

Notation. When $\mathbf{f}_{\triangle} \in \mathbb{T}(\mathscr{F}[\mathbf{x}])$ let

$$\mathbf{f}_{\triangle}^{\top} := \max_{\text{mvar}}(f : f \in \mathbf{f}_{\triangle}), \qquad \mathbf{f}_{\triangle}^{\uparrow} := \mathbf{f}_{\triangle} - \{\mathbf{f}_{\triangle}^{\perp}\},$$
$$\mathbf{f}_{\triangle}^{\downarrow} := \mathbf{f}_{\triangle} - \{\mathbf{f}_{\triangle}^{\top}\}, \qquad \mathbf{f}_{\triangle}^{\perp} := \min_{\text{mvar}}(f : f \in \mathbf{f}_{\triangle}).$$

Note $\{\mathbf{f}_{\triangle}^{\top}\} \cup \mathbf{f}_{\triangle}^{\downarrow} = \mathbf{f}_{\triangle}^{\uparrow} \cup \{\mathbf{f}_{\triangle}^{\perp}\} = \mathbf{f}_{\triangle}$.

§Properties of Triangular Sets

The history of triangular sets dates back to at least 1932 when Joseph Fels Ritt demonstrated one can compute a triangular set equivalent to a given irreducible variety [7].

Let us first define the *Iterated Pseudo-remainder*.

Definition 2.3 (Iterated Pseudo-remainder)**.** Let $h \in \mathscr{F}[\mathbf{x}]$ and $\mathbf{f}_{\triangle} \in \mathbb{T}(\mathscr{F}[\mathbf{x}])$ be a triangular set. The *iterated pseudo-remainder* is given (recursively) by

$$\begin{aligned} &\text{prem}^*(h,\, \varnothing;\, \varnothing) := h, \\ &\text{prem}^*(h,\, \mathbf{f}_{\triangle};\, \mathbf{x}) := \text{prem}^*(\, \text{prem}(h,\, \mathbf{f}_{\triangle}^{\top};\, x_\ell),\, \mathbf{f}_{\triangle}^{\downarrow};\, \mathbf{x}^{\downarrow}\,). \end{aligned}$$

Similarly we have the *iterated pseudo-quotient*.

Theorem 2.1 (Ritt, 1932)**.** For any $\mathbf{h} \subseteq \mathscr{F}[\mathbf{x}]$ such that $\mathbf{V}(\mathbf{h})$ is an irreducible variety one can construct a triangular set $\mathbf{f}_{\triangle} \in \mathbb{T}(\mathscr{F}[\mathbf{x}])$ satisfying

$$\forall\, h \in \langle \mathbf{h} \rangle;\ \mathrm{prem}^*(h,\, \mathbf{f}_{\triangle};\, \mathbf{x}) = 0.$$

A set given by Theorem 2.1 is called a *Ritt characteristic set* and the utility of this construction is that it enables an ideal membership test on $\mathbf{h}$.

Because irreducible components are often difficult to calculate, Wen-Tsun Wu in 1987 devised a method for computing triangular sets for *arbitrary* varieties [37]. Such sets are called *Wu characteristic sets* and can be calculated using fully Gröbner basis free methods [3].

Theorem 2.2 (Wu, 1987)**.** For any $\mathbf{h} \subseteq \mathscr{F}[\mathbf{x}]$ one can compute a triangular set $\mathbf{f}_{\triangle} \subseteq \langle \mathbf{h} \rangle$ such that

$$\forall\, h \in \mathbf{h};\ \mathrm{prem}^*(h,\, \mathbf{f}_{\triangle};\, \mathbf{x}) = 0.$$

Although certainly more widely applicable, Wu's method cannot detect empty varieties. Empty varieties are those corresponding to polynomial systems with no solutions. The stronger restrictions imposed on triangular sets make them regular chains.

§2.3 Regular Chains

Being a triangular set, despite having the right shape, provides no assurance to back substitution being "well behaved." In Example 2.3 for instance, substituting $x = 1$ into $(x-1)y^2 - x = 0$ implies $x = 0 = 1$ and contradiction. The extra restrictions on triangular sets, like ensuring leading coefficients are invertible, yield regular chains and eliminate this and other problems.

§Shedding Bad Initials

When a leading coefficient vanishes so doe, more disastrously, the leading term. Geometrically, shedding these bad substitution points simply means removing points from the variety where leading coefficients (or initials) vanish.

Definition 2.4 (Initial)**.** The initial of $f \in \mathscr{F}[\mathbf{x}]$ is the leading coefficient of f when taken as univariate in its main variable.

$$\operatorname{init}(f) := \operatorname{lcoeff}_{\operatorname{mvar}(f)}(f).$$

The *quasi-component* of a regular chain $\mathbf{f}_\triangle$ corresponds to the removal of points where an initial of some $f \in \mathbf{f}_\triangle$ vanishes.

Definition 2.5 (Quasi Component)**.** Let $\mathbf{f}_\triangle \in \mathbb{T}(\mathscr{F}[\mathbf{x}])$, then

$$\mathbf{W}(\mathbf{f}_\triangle) := \mathbf{V}(\mathbf{f}_\triangle) - \mathbf{V}\Big(\prod \operatorname{init}(f) : f \in \mathbf{f}_\triangle\Big)$$

is called the *quasi component* of $\mathbf{f}_\triangle$.

Algebraically removing bad initials from an ideal is less obvious. Here we must remove initials which are zero divisors modulo a 'chain' of regular chains. The *saturation ideal*, as it turns out, does this. Saturating an ideal has the desired effect of algebraically shedding bad initials.

Definition 2.6 (Colon Ideal)**.** Let $\mathbf{f}, \mathbf{g} \subseteq \mathscr{F}[\mathbf{x}]$.

$$\langle \mathbf{f} \rangle : \langle \mathbf{g} \rangle := \{h : \forall\, g \in \mathbf{g};\ hg \in \langle \mathbf{f} \rangle\}.$$

Definition 2.7 (Saturation Ideal)**.** Let $\mathbf{f}_\triangle \in \mathbb{T}(\mathscr{F}[\mathbf{x}])$ and the product of the initials be

$$\operatorname{init}(\mathbf{f}_\triangle) := \prod (\operatorname{init}(f) : f \in \mathbf{f}_\triangle).$$

The *saturation* of $\mathbf{f}_\triangle$ is the ideal

$$\begin{aligned} \langle \operatorname{sat}(\mathbf{f}_\triangle) \rangle &:= \langle \mathbf{f}_\triangle \rangle : \langle \operatorname{init}(\mathbf{f}_\triangle)^0 \rangle + \langle \mathbf{f}_\triangle \rangle : \langle \operatorname{init}(\mathbf{f}_\triangle)^1 \rangle + \cdots \\ &= \langle \mathbf{f}_\triangle \rangle : \operatorname{init}(\mathbf{f}_\triangle)^\infty. \end{aligned}$$

In other words, $f \in \langle \text{sat}(\mathbf{f}_\triangle)\rangle \overset{\text{Defn.}}{\iff} \exists\, n \in \mathbb{N}^{>0} : \text{init}(\mathbf{f}_\triangle)^n f \in \langle \mathbf{f}_\triangle \rangle$.

Notice saturating an ideal may make it larger.

Example 2.4. Let $\mathbf{f}_\triangle = \begin{cases} zx + t \\ ty + z \end{cases} \in \mathbb{T}(\mathscr{F}[x,\, y,\, z,\, t])$

$$\langle \mathbf{f}_\triangle \rangle = \langle z,\, t\rangle \cap \langle -xy + 1,\, ty + z\rangle, \text{ and}$$
$$\langle \text{sat}(\mathbf{f}_\triangle)\rangle = \langle 1 - xy,\, ty + z\rangle.$$

It is well known that the quasi-component and saturation ideal are related in the following manner [10].

Theorem 2.3. Let $\mathbf{f}_\triangle \in \mathbb{T}(\mathscr{F}[\mathbf{x}])$ and $\overline{\mathbf{W}(\mathbf{f}_\triangle)}$ be the *Zariski closure* of quasi-component of $\mathbf{f}_\triangle$. Then

$$\overline{\mathbf{W}(\mathbf{f}_\triangle)} = \mathbf{V}(\langle \text{sat}(\mathbf{f}_\triangle)\rangle).$$

And finally, a *regular chain* is a triangular set whose top is regular (i.e. not a zero-divisor) modulo its bottom.

Definition 2.8 (Regular Element)**.** Let $f \in \mathscr{F}[\mathbf{x}]$, $\mathbf{f} \subseteq \mathscr{F}[\mathbf{x}]$, and $\mathbb{U}\langle \mathbf{f}\rangle$ denote the set of *regular elements* among $\mathscr{F}[\mathbf{x}]/\langle \mathbf{f}\rangle$. Then

$$f \in \mathbb{U}\langle \mathbf{f}\rangle \overset{\text{Defn.}}{\iff} \forall\, g \in \mathscr{F}[\mathbf{x}];\; fg \equiv 0 \bmod \langle \mathbf{f}\rangle \implies g \equiv 0 \bmod \langle \mathbf{f}\rangle.$$

Moreover, let $f \notin \mathbb{U}\langle \mathbf{f}\rangle$ be called a *zero-divisor*.

Definition 2.9 (Regular Chain)**.** Denote by $\mathbb{T}_{\text{reg}}(\mathscr{F}[\mathbf{x}])$ the class of regular chains of $\mathscr{F}[\mathbf{x}]$ and let $\mathbb{T}_{\text{reg}}(\mathscr{F}[\mathbf{x}]) \subseteq \mathbb{T}(\mathscr{F}[\mathbf{x}])$. Then

$$\mathbf{f}_\triangle \in \mathbb{T}_{\text{reg}}(\mathscr{F}[\mathbf{x}]) \overset{\text{Defn.}}{\iff} \begin{cases} \mathbf{f}_\triangle = \varnothing, \text{ or} \\ \mathbf{f}_\triangle^{\downarrow} \in \mathbb{T}_{\text{reg}}(\mathscr{F}[\mathbf{x}]) \text{ and } \text{init}(\mathbf{f}_\triangle^{\top}) \in \mathbb{U}\langle \mathbf{f}_\triangle^{\downarrow}\rangle. \end{cases}$$

Among the things that make regular chains interesting is that the dimension of the Zariski closure of quasi-component is the expected number of variables minus the number of equations.

Proposition 2.1. When $\mathbf{f}_\triangle \in \mathbb{T}_{\mathrm{reg}}(\mathscr{F}[\mathbf{x}])$ the dimension of $\overline{\mathbf{W}(\mathbf{f}_\triangle)}$ is given by

$$\dim \overline{\mathbf{W}(\mathbf{f}_\triangle)} = \ell + 1 - |\mathbf{f}_\triangle|.$$

Proof. See [35]. □

§Specializing at Regular Chains

When working over the complex numbers for instance specialization at maximal ideals corresponds to evaluation,

$$x^2 + y \bmod \langle x - 1,\, y - 2 \rangle = x^2 + y\big|_{x=1,\, y=2} = 3$$

whereas more arbitrary ideals specialize at algebraic points

$$x^2 - 4 \bmod \left\langle x^2 - 2 \right\rangle = x^2 - 4\big|_{x=\pm\sqrt{2}} = -2$$

and so naturally at complex points as well

$$x^4 \bmod \left\langle x^2 + 1 \right\rangle = x^4\big|_{x=\pm\sqrt{-1}} = 1.$$

In any case, "modding out" a polynomial g by some ideal $\langle \mathbf{f} \rangle$ has the effect of *simultaneously* evaluating g at each point of $\mathbf{V}(\mathbf{f})$. Thus, modular images can be (and are) used instead of explicit function evaluation.

§2.4 Triangularization

In general there are two ways to decompose $\langle \mathbf{h} \rangle$ into regular chains. One can either describe the *generic points* of the ideal (a Kalkbrenner decomposition) or all the zeros of the corresponding variety (a Lazard decomposition). There are various algorithms available for triangular decompositions in either sense.

> All the proofs for this section can be found within [35] and the references therein.

Theorem 2.4 (Kalkbrenner Decomposition)**.** For any $\mathbf{h} \subseteq \mathscr{F}[\mathbf{x}]$ there are regular chains $\{\mathbf{f}_{\triangle,0}, \ldots, \mathbf{f}_{\triangle,e}\} \subseteq \mathbb{T}_{\text{reg}}(\mathscr{F}[\mathbf{x}])$ such that

$$\sqrt{\langle \mathbf{h} \rangle} = \sqrt{\langle \text{sat}(\mathbf{f}_{\triangle,0}) \rangle} \cap \cdots \cap \sqrt{\langle \text{sat}(\mathbf{f}_{\triangle,r}) \rangle}$$

where $e \in \mathbb{N}$ and, using the Ideal-Variety correspondence and Theorem 2.3, we also have

$$\mathbf{V}(\mathbf{h}) = \overline{\mathbf{W}(\mathbf{f}_{\triangle,0})} \cup \cdots \cup \overline{\mathbf{W}(\mathbf{f}_{\triangle,e})}.$$

Additionally, there is an algorithm for computing a Kalkbrenner decomposition. We take this algorithm as black-box and simply let $\triangle(\mathbf{h})$ be the computed triangularization.

Definition 2.10 (Triangularize)**.** For any ideal $\mathbf{h}$ an ideal of $\mathscr{F}[\mathbf{x}]$ let the *triangularization* of $\mathbf{h}$ be a mapping from the ideals of $\mathscr{F}[\mathbf{x}]$ into sets of regular chains from $\mathscr{F}[\mathbf{x}]$ given by

$$\begin{aligned} \triangle : \mathscr{P}(\mathscr{F}[\mathbf{x}]) &\to \mathscr{P}(\mathbb{T}_{\text{reg}}(\mathscr{F}[\mathbf{x}])) \\ \langle \mathbf{h} \rangle &\mapsto \{\mathbf{f}_{\triangle,0}, \ldots, \mathbf{f}_{\triangle,e}\} : \mathbf{V}(\mathbf{h}) = \overline{\mathbf{W}(\mathbf{f}_{\triangle,0})} \cup \cdots \cup \overline{\mathbf{W}(\mathbf{f}_{\triangle,e})}. \end{aligned}$$

where $r \in \mathbb{N}$.

Moreover, Moreno Maza and Wang (simultaneously) in 2000 [32][28] gave the following guarantee regarding the decomposition of varieties into a disjoint union of quasi-components independent of the Zariski closure.

Theorem 2.5 (Lazard Decomposition)**.** For any $\mathbf{h} \subseteq \mathscr{F}[\mathbf{x}]$ there are regular chains $\{\mathbf{f}_{\triangle,0}, \ldots, \mathbf{f}_{\triangle,r}\} \subseteq \mathbb{T}_{\text{reg}}(\mathscr{F}[\mathbf{x}])$ such that

$$\mathbf{V}(\mathbf{h}) = \mathbf{W}(\mathbf{f}_{\triangle,0}) \sqcup \cdots \sqcup \mathbf{W}(\mathbf{f}_{\triangle,e})$$

where $\sqcup$ is the disjoint union and $r \in \mathbb{N}$.

Proof. See [19]. □

Because Kalkbrenner decompositions are typically faster than Lazard decompositions, in practice the former is the default setting when using the `Triangularize` command in Maple. In particular, this is the case for our algorithms.[23]

Example 2.5. Let $\mathbf{h} = \{x^2 + y + z - 1,\, x + y^2 + z - 1,\, x + y + z^2 - 1\} \subseteq \mathscr{F}[\mathbf{x}]$. A Kalkbrenner decomposition of $\langle \mathbf{h} \rangle$ is given by

$$\triangle(\mathbf{h}) = \left\{ \begin{cases} x - z \\ y - z \\ z^2 + 2z - 1 \end{cases}, \begin{cases} x \\ y \\ z - 1 \end{cases}, \begin{cases} x \\ y - 1 \\ z \end{cases}, \begin{cases} x - 1 \\ y \\ z \end{cases} \right\}$$

§2.5 Splitting and the D5 Principle

The intuition behind triangular decomposition algorithms is to "follow the one variable polynomial division algorithm as closely as possible"[11, Ch. 6 §5]. The difference being a 'splitting' step that handles degenerate-cases where the leading coefficients of the divisors are zero divisors.

In the univariate, unlike the multivariate, case the polynomial division algorithm produces *unique* remainders. Accordingly, when $m \in \mathscr{F}[x]$, $\mathscr{F}[x]/\langle m \rangle$ can be identified with $\{\mathrm{rem}(f,\, m;\, x) : f \in \mathscr{F}[x]\}$.

Consider $x+3 \in \mathscr{F}[x]$. This element is a zero divisor modulo $\langle m \rangle$ with $m = x^2 + 5x + 6$ because there is $x + 2 \in \mathscr{F}[\mathbf{x}]$ such that $(x+2)(x+3) \equiv 0 \bmod \langle m \rangle$. Now, if we wanted to do a 'univariate' division in $\mathscr{R}[y]$ with $\mathscr{R} = \mathscr{F}[x]/\langle m \rangle$, say

$$y^2 + (x+1)y + 2 \;\Big|\; \underline{(x+3)^2 y + y + x}\,,$$

we are unable to because $x+3$ cannot be inverted modulo $\langle (x+3)(x+2) \rangle$.

Instead of giving up though, the computation can be split into two

separate divisions. The first modulo $\langle x+3\rangle$:

$$\begin{array}{r|l} y^2+(x+1)y+2 & y+x \\ \hline y-3 & y^2-2y+2 \end{array}$$

and the second modulo $\langle x+2\rangle$:

$$\begin{array}{r|l} y^2+(x+1)y+2 & y+y+x \\ \hline \frac{1}{2}y & 2 \end{array}$$

This is possible because

$$\mathscr{R} = \mathscr{F}[x]/\langle (x+3)(x+2)\rangle \cong \mathscr{F}[x]/\langle x+2\rangle \otimes \mathscr{F}[x]/\langle x+3\rangle$$

where $\otimes$ is the direct product and $\mathscr{R}$ is a product of fields.

§Regularize

Loosely speaking, any algorithm that works over a field can be made to work over a product of fields. However, in the very least the product of fields should be defined by zero-dimensional regular chains. This is the essence of the D5 principle.

Let $m \in \mathscr{F}[x]^{\neq \mathscr{F}}$. Any element $\alpha \in \mathscr{F}[x]/\langle m\rangle$ has a canonical representation in $\mathscr{F}[x]/\langle m\rangle$. Moreover, when α has a trivial gcd with m we can retrieve with the *extended* Euclidean algorithm u, $v \in \mathscr{F}[x]$ such that

$$u\cdot\alpha + v\cdot m = \gcd(\alpha,\, m) = 1 \implies u\cdot\alpha \equiv 1 \bmod \langle m\rangle.$$

Elements with inverses (naturally) are called *invertible* but more generally in our setting they are regular elements. Conversely, if the gcd is not a unit then $m = \gcd(\alpha,\, m)\cdot m'$ and thus α is a zero divisor. Indeed $m = \gcd(\alpha,\, m)\cdot m'$, $\alpha = \gcd(\alpha,\, m)\cdot\alpha'$, and multiplying the first by α' we deduce $\alpha\cdot m' \equiv 0 \bmod \langle m\rangle$. Because m' is not zero modulo m (using a degree argument) we conclude α is a zero divisor.

The intuition behind 'Regularization' is to decompose m into as few

Function Regularize(m; h)

Input: A squarefree $m \in \mathscr{F}[x]$ and $h \in \mathscr{F}[x]$.

Output: $\mathbf{m} \subseteq \mathscr{F}[x]$ such that

1. $m = \prod(m' : m' \in \mathbf{m})$, and
2. $\forall\, m' \in \mathbf{m}$; $h \in \mathbb{U}\langle m' \rangle$ xor $h \equiv 0 \bmod \langle m' \rangle$.

if $\gcd(m, h) \in \mathscr{F}$ **then**
  return $\{m\}$;
Otherwise $m = \gcd(m, h) \cdot m'$;
$m' \leftarrow \mathrm{quo}(m, \gcd(m, h); x)$;
return $\{\gcd(m, h)\} \cup$ Regularize(m'; h)

Algorithm 1: Regularize for univariate polynomials.

factors as possible so that either α is regular or zero (but not any other zero divisor) modulo the factors. The Regularize function propagates through our algorithms mostly by virtue of zero testing. That is, we must assume all zero-testing modulo a regular chain will require splitting to distinguish regular elements from those simply multiplied by zero.

The general version of Regularize is similar to this except that the gcd works over triangular sets rather than a field. It itself uses Regularize, though in one variable less, and because of this recurses to the (known) univariate case. We take the greatest common divisor and subsequently the multivariate Regularize algorithm for regular chains as black-box and instead refer the reader to [6, §3.2].

Example 2.6. Let $\mathbf{f}_\triangle = \{y^2 - y,\, z(z-1)\} \in \mathscr{F}[x,\, y,\, z]$ and consider the regularization of $h = xz + y$. Note

$$\text{Regularize}(\mathbf{f}_\triangle;\, h) = \Big\{ \begin{cases} y - 2 \\ z \end{cases}, \begin{cases} y \\ z - 1 \end{cases}, \begin{cases} y - 2 \\ z - 1 \end{cases}, \begin{cases} y \\ z \end{cases} \Big\}.$$

and that $h \equiv 2 \bmod \langle y - 2,\, z \rangle$, $h \equiv x \bmod \langle y,\, z - 1 \rangle$, and $h \equiv x + 2 \bmod$

1 **Function** Regularize($\mathbf{f}_\triangle$; $\mathbf{h}$)

Input: $\mathbf{f}_\triangle \in \mathbb{T}_{\text{reg}}(\mathscr{F}[\mathbf{x}])$ a zero-dimensional regular chain such that $\text{sat}(\mathbf{f}_\triangle)$ is radical and $\mathbf{h} \subseteq \mathscr{F}[\mathbf{x}]$ a set of polynomials.

Output: A Kalkbrenner decomposition of $\mathbf{f}_\triangle$ given by

$$\mathbf{f}_{\triangle,0}, \ldots, \mathbf{f}_{\triangle,e} \in \mathbb{T}_{\text{reg}}(\mathscr{F}[\mathbf{x}])$$

such that for any $h \in \mathbf{h}$ and any regular chain $\mathbf{f}_{\triangle,0}, \ldots, \mathbf{f}_{\triangle,e}$, h is either zero or regular modulo $\mathbf{f}_{\triangle,i}$. That is to say

$$\begin{aligned} h \bmod \langle \mathbf{f}_{\triangle,0} \rangle &\in \mathbb{U}\langle \mathbf{f}_{\triangle,0} \rangle \cup \{0\}, \\ &\vdots \\ h \bmod \langle \mathbf{f}_{\triangle,e} \rangle &\in \mathbb{U}\langle \mathbf{f}_{\triangle,e} \rangle \cup \{0\}. \end{aligned}$$

Specification 1: Regularize for multivariate polynomials.

$\langle y-2, z-1 \rangle$ are all units. Conversely $h \equiv 0 \bmod \langle y, z \rangle$.

Chapter 3

Intersection Multiplicity

The *intersection multiplicity* is an invariant of algebraic geometry which weighs points of algebraic varieties according to their importance (measured by the dimension of their corresponding tangent spaces). Consider a system of polynomials $\mathbf{h}$ with variety $\mathbf{V}(\mathbf{h})$. The definition of $\mathrm{im}(p;\, \mathbf{h})$, the intersection multiplicity of p on $\mathbf{V}(\mathbf{h})$, is tailored to satisfy

$$\sum_{p \in \mathbf{V}(\mathbf{h})} \mathrm{im}(p;\, \mathbf{h}) = \prod_{h \in \mathbf{h}} \deg(h).$$

This implies (in projective spaces with mild assumptions) that the cardinality of a finite algebraic variety $\mathbf{V}(\mathbf{h})$ is equal to the product of the total degrees among $\mathbf{h}$.

In this chapter we investigate the formal definition of the intersection multiplicity and Fulton's properties which enable an algorithm to calculate these values for planar curves. Finally we demonstrate how to extend Fulton's properties to ℓ-variate systems.

§3.1 Bivariate Intersection Multiplicity

To give a concrete example consider the intersection of a parabola (degree 2) and line (degree 1) in $\mathbb{A}^2(\mathbb{R})$:

$$\mathbf{V}\big(y - x^2, y - ax - b\big) : a, b \in \mathbb{R}.$$

Here we want the weighted sum over the points of intersection to be two. There are three possible cases:

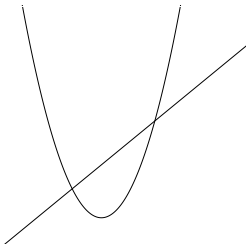
1. two points of intersection with IM one,
2. a single tangential intersection with IM two, or
3. two complex intersections with IM one.

In each case

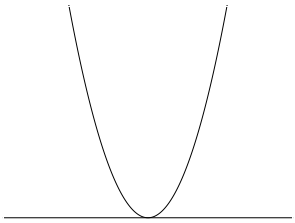
$$\sum_{p \in \mathbf{V}(y-x^2, y-ax-b)} \mathrm{im}\big(p;\, y-x^2,\, y-ax-b\big) = 2$$

is satisfied. These cases are illustrated in Figure 3.1.

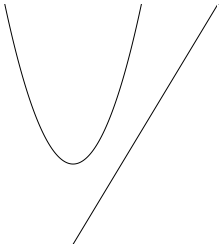
Regular points have intersection multiplicity one — in fact they can be defined by this property. Points at tangential intersections, crossovers, and singular points have IM greater than one. Everything else has IM zero.



(a) Both intersection points have IM 1.



(b) A tangent with IM 2.



(c) Two complex solutions with IM 1.

Figure 3.1: The various intersections of a line and parabola.

There are a myriad of ways to define the intersection multiplicity of two planar curves $h_0,\, h_1 \in \mathscr{F}[x, y]$. Its 'purest' form is Bézout's definition which simply states a point's intersection multiplicity is equal to the dimension of the *local ring* $\mathscr{O}_{\mathbb{A}^2(\mathscr{F}),\, p}$ at $\langle h_0,\, h_1 \rangle$.

Definition 3.1 (Bézout's IM for bivariates)**.** Let $\mathbf{h} \subseteq \mathscr{F}[x, y]$ and $p \in \mathbf{V}(\mathbf{h})$. The *intersection multiplicity* of p in $\mathbf{V}(\mathbf{h})$ is

$$\mathrm{im}(p;\, \mathbf{h}) := \dim_{\mathrm{vec}}(\mathscr{O}_{\mathbb{A}^2,\, p}/\langle \mathbf{h} \rangle),$$

where $\mathscr{O}_{\mathbb{A}^2,p} := \left\{ \frac{f}{g} : f, g \in \mathscr{F}[x,y],\ g(p) \neq 0 \right\}$.

As the intersection multiplicity is a local property it can safely be calculated using Taylor series instead of rational functions.

In order to different between ideal brackets and vector brackets we use $\langle\ \rangle$ for the former and $\langle\langle\ \rangle\rangle$ for the later. That is to say, when $\{f_0, \ldots, f_e\} \subseteq \mathscr{F}[\mathbf{x}]$ then

$$\langle\langle\, f_0, \ldots, f_e \,\rangle\rangle = \{c_0 f_0 + \cdots + c_e f_e : c_0, \ldots, c_e \in \mathscr{F}\}.$$

Example 3.1. Consider the parabola and line given by $\mathbf{h} = \{y - x^2, y - x\} \subseteq \mathscr{F}[x,y]$ is $x(x+1),\ y - x$. Near $\mathbf{0}$, a point in $\mathbf{h}$'s variety, we have

$$\begin{aligned}
\mathscr{F}[[x,\, y]]/\langle \mathbf{h} \rangle &= \mathscr{F}[[x,\, y]]/\langle x(x+1),\, y - x \rangle \\
&\qquad \text{(note } (x+1) \text{ is a unit near } \mathbf{0}.) \\
&= \mathscr{F}[[x,\, y]]/\langle x,\, y - x \rangle \\
&= \mathscr{F}[[x,\, y]]/\langle x,\, y \rangle \\
&= \langle\langle\, 1 \,\rangle\rangle.
\end{aligned}$$

This means $\dim_{\text{vec}}(\mathscr{O}_{\mathbb{A}^2,p}/\langle \mathbf{h} \rangle) = \text{im}(\mathbf{0};\, \mathbf{h}) = 1$.

Example 3.2 (Figure 3.1b)**.** Consider the parabola and tangent line given by $\mathbf{h} = \{y - x^2,\, y\} \subseteq \mathscr{F}[x,y]$ is $x^2,\, y$. Near $\mathbf{0}$ we have

$$\begin{aligned}
\mathscr{F}[[x,\, y]]/\langle \mathbf{h} \rangle &= \mathscr{F}[[x,\, y]]/\langle y,\, x^2 \rangle \\
&= \{a + bx : a, b \in \mathscr{F}\} \\
&= \langle\langle\, 1, x \,\rangle\rangle.
\end{aligned}$$

Thus $\text{im}(\mathbf{0};\, \mathbf{h}) = 2$.

§3.2 Fulton's Properties

Fulton's *constructive* characterization of the intersection multiplicity is an an algorithm for planar curves. Indeed this algorithm, and its proofs, form the basis of our generalization.

The *multiplicity* of $h \in \mathscr{F}[x, y]$ at p (denoted $m_p(h)$) is the tailing degree of h when viewed as a polynomial from $\mathscr{F}[\mathbf{x} - p]$.

Theorem 3.1 (Fulton's Properties)**.** Let two plane curves be given by $h_0,\, h_1 \in \mathscr{F}[x, y]$ and let $p \in \mathbb{A}^2(\mathscr{F}[x, y])$. The intersection multiplicity of $h_0,\, h_1$ at p satisfies *and is uniquely determined by* the following properties:

(2-1) $\operatorname{im}(p;\, h_0,\, h_1) = \begin{cases} \infty & \text{if } p \in \mathbf{V}(\gcd(h_0,\, h_1)) \\ n \in \mathbb{N} & \text{otherwise.} \end{cases}$,

(2-2) $\operatorname{im}(p;\, h_0,\, h_1) = 0 \iff p \notin \mathbf{V}(h_0) \cap \mathbf{V}(h_1)$,

(2-3) $\operatorname{im}(p;\, h_0,\, h_1)$ is invariant to affine change of coordinates on $\mathbb{A}^2(\mathscr{F})$,

(2-4) $\operatorname{im}(p;\, h_0,\, h_1) = \operatorname{im}(p;\, h_1,\, h_0)$,

(2-5) $\operatorname{im}(p;\, h_0,\, h_1) \geq m_p(h_0) \cdot m_p(h_1)$ with equality occurring if and only if $\pi_p(h_0) \pitchfork \pi_p(h_1)$. That is, if $\mathbf{V}(h_0)$ and $\mathbf{V}(h_1)$ have no tangent lines in common at p,

(2-6) $\forall\, g \in \mathscr{F}[\mathbf{x}];\, \operatorname{im}(p;\, h_0,\, h_1) = \operatorname{im}(p;\, h_0,\, h_1 g) - \operatorname{im}(p;\, h_0,\, g)$, and

(2-7) $\forall\, g \in \mathscr{F}[\mathbf{x}];\, \operatorname{im}(p;\, h_0,\, h_1) = \operatorname{im}(p;\, h_0,\, h_1 + h_0 g)$.

Notice Theorem 3.1 classifies *every* point of $\mathbb{A}^{\ell+1}\big(\overline{\mathscr{F}}\big)$.

Proof. See [14] for the full constructive proof yielding Algorithm 2. We note items (2-6) and (2-7) from Theorem 3.1 are the crucial properties for Algorithm 2 since they enable a recursive "division step" for lines 8–9 where the operands descend in degree until termination. Additionally, line 3 is justified by (2-2), line 5 by (2-4), and lines 11–12 by (2-7). □

1 **Function** $\mathrm{im}(p;\, h_0,\, h_1)$

Input:

1. $p = (p_x,\, p_y) \in \mathbb{A}^2(\mathscr{F})$, and
2. $h_0,\, h_1 \in \mathscr{F}[y \prec x] : \gcd(h_0, h_1) \in \mathscr{F}$.

Output: $\mathrm{im}(p;\, h_0,\, h_1) \in \mathbb{N}$ satisfying (2-1)–(2-7).

2 **if** $h_0(p),\, h_1(p) \neq 0$ **then**

3 **return** 0;

4 $r,\, s \leftarrow \deg(h_0(x, p_y)),\, \deg(h_1(x, p_y))$;

5 **if** $r > s$ **then**

6 **return** $\mathrm{im}(p;\, h_1,\, h_0)$;

7 **if** $r = -\infty$ **then** /* $(y - p_y) \,\big|\, h_0(x, y)$ */

8 write $h_1(x, p_y) = (x - p_x)^m (a_m + a_m(x - p_x) + \cdots)$;

9 **return** $m + \mathrm{im}(p;\, \mathrm{quo}(h_0,\, y - p_y;\, y),\, h_1)$;

10 **if** $r \leq s$ **then**

11 $h_1' \leftarrow h_1 - x^{s-r} \dfrac{\ell c(h_1(x, p_y))}{\ell c(h_0(x, p_y))}\, h_0$;

12 **return** $\mathrm{im}(p;\, h_1',\, h_0)$;

Algorithm 2: Fulton's Algorithm

Example 3.3. Find the intersection multiplicity of $\mathbf{h} = \{y, y - x^2\}$ at the origin using Fulton's algorithm. See Figure 3.1b for a geometric representation. Boxed values indicate the recursive calls and the remaining the algorithm's trace.

	LINE
$\boxed{\operatorname{im}\big(\mathbf{0};\, y,\, y - x^2\big)}$	
$(r,\, s) \leftarrow \deg\big(0,\, 0 - x^2\big)$	4
$= (-\infty,\, 2)$	
$h_1(x,\, 0) = x^2(-1) \implies m = 2$	8
$\boxed{2 + \operatorname{im}\big(\mathbf{0};\, \operatorname{quo}(y,\, y;\, y),\, y - x^2\big)}$	
$\operatorname{im}\big(\mathbf{0};\, 1,\, y - x^2\big) = 0$	2
$\boxed{2.}$	

Fulton's algorithm has not yet been generalized to more than two hypersurfaces.[1] Moreover, Algorithm 2 is limited to computing intersection multiplicities at rational coordinates from the base field. Thus, intersection multiplicities at complex points, irrational points, and more generally algebraic points cannot be calculated using this algorithm.

§3.3 Extending Fulton's Properties

Extending the *geometric* definition of intersection multiplicity to more variables is straightforward. We are still measuring the dimension of tangent spaces (albeit higher dimensional ones) about points in an affine space.

Definition 3.2 (Bézout's Intersection Multiplicity)**.** Let $\mathbf{h} \subseteq \mathscr{F}[\mathbf{x}]$ and $p \in \mathbf{V}(\mathbf{h}) \subseteq \mathbb{A}^{\ell+1}\big(\overline{\mathscr{F}}\big)$. The *intersection multiplicity* of p in $\mathbf{V}(\mathbf{h})$ is

$$\operatorname{im}(p;\, \mathbf{h}) := \dim_{\text{vec}}(\mathscr{O}_{\mathbb{A}^{\ell+1},\, p}\,/\langle \mathbf{h} \rangle).$$

[1] To our knowledge.

$$\mathscr{O}_{\mathbb{A}^{\ell+1},p} := \left\{ \frac{f}{g} : f, g \in \overline{\mathscr{F}}[\mathbf{x}],\ g(p) \neq 0 \right\}.$$

Note that by [11, Chapter 4. §2 Proposition 11] we can substitute the power series ring $\mathscr{F}[[\mathbf{x}-p]]$ for $\mathscr{O}_{\mathbb{A}^{\ell+1},p}/\langle \mathbf{h} \rangle$ below as they are isomorphic.

Example 3.4. Locally at the origin the system

$$\mathbf{h} = \left\{ x,\ x - y^2 - z^2,\ y - z^3 \right\} \subseteq \mathscr{F}[x,\ y,\ z]$$

is $x,\ y = z^3,\ z^2(z^4+1)$. Near $\mathbf{0}$ we have

$$\begin{aligned} \mathscr{F}[[\mathbf{x}]]/\langle \mathbf{h} \rangle &= \mathscr{F}[[\mathbf{x}]]/\left\langle x,\ y - z^3,\ z^2 \right\rangle \\ &= \mathscr{F}[[\mathbf{x}]]/\left\langle x,\ y,\ z^2 \right\rangle \\ &= \{a + bz : a,\ b \in \mathscr{F}\} \\ &= \langle\langle\ 1,\ z\ \rangle\rangle, \end{aligned}$$

where $\langle\langle\ 1,\ z\ \rangle\rangle$ is a $\mathscr{F}$-vector space. Thus $\operatorname{im}(\mathbf{0};\ \mathbf{h}) = 2$.

We propose, up to splitting, the following extension of Fulton's properties to correspond with Definition 3.2 for Regular Chains [24].

Theorem 3.2. Let $\mathbf{h} \in \mathbb{S}(\mathscr{F}[\mathbf{x}])$ be a sequence in $\mathscr{F}[\mathbf{x}]$ so that $\langle \mathbf{h} \rangle$ is zero dimensional, $p := (p_0,\ \ldots, p_\ell) \in \mathbb{A}^{\ell+1}\big(\overline{\mathscr{F}}\big)$, and let $\mathbf{h}^{\downarrow}$ denote the removal of the element $h_\ell \in \mathbf{h}$ (i.e., $\mathbf{h} = \{h_\ell\} \cup \mathbf{h}^{\downarrow}$) then

$$\operatorname{im}(p;\ \mathbf{h}) \text{ satisfies } (n\text{-}1) \text{ through } (n\text{-}7)$$

where

(n-1) $\operatorname{im}(p;\ \mathbf{h}) \in \mathbb{N}$,

(n-2) $\operatorname{im}(p;\ \mathbf{h}) = 0 \iff p \notin \mathbf{V}(\mathbf{h})$,

(n-3) $\operatorname{im}(p;\ \mathbf{h})$ is invariant to affine change of coordinates on $\mathbb{A}^{\ell+1}(\mathscr{F})$,

(n-4) $\operatorname{im}(p;\ \mathbf{h}) = \operatorname{im}(p;\ \sigma(\mathbf{h}))$ for any permutation $\sigma(\mathbf{h})$ of the elements of $\mathbf{h}$,

(n-5) $\operatorname{im}(p;\ (x_0 - p_0)^{m_0},\ \ldots,\ (x_\ell - p_\ell)^{m_\ell}) = m_0 \cdots m_\ell$,

(n-6) provided $\mathbf{h}^{\downarrow}$, gh is a regular sequence (and thus $\dim \langle \mathbf{h}^{\downarrow}, gh \rangle = 0$)

$$\operatorname{im}(p; \mathbf{h}^{\downarrow}, gh) = \operatorname{im}(p; \mathbf{h}^{\downarrow}, g) + \operatorname{im}(p; \mathbf{h}^{\downarrow}, h),$$

(n-7) $\forall\, g \in \langle \mathbf{h}^{\downarrow} \rangle$; $\operatorname{im}(p; \mathbf{h}^{\downarrow}, h) = \operatorname{im}(p; \mathbf{h}^{\downarrow}, h + g)$.

For these seven properties, we adapt the proofs of [14, 18] and note all but (n-6) are trivial and (n-4) and (n-7) in particular are obvious because the intersection multiplicity depends only on p and $\langle \mathbf{h} \rangle$.

Proof of (n-1). The sequence $\mathbf{h}$ is regular, so $\mathbf{V}(\mathbf{h})$ is proper intersection of varieties and $\langle \mathbf{h} \rangle$ forms a zero dimensional ideal. The result follows. □

Proof of (n-2). When $p \notin \mathbf{V}(\mathbf{h})$.

$$\begin{aligned} p \notin \mathbf{V}(\mathbf{h}) &\implies \exists\, f \in \mathbf{h} : p \notin \mathbf{V}(f) \\ &\implies f \notin \langle \mathbf{x} - p \rangle \\ &\implies \frac{1}{f} \in \mathscr{O}_{\mathbb{A}^{\ell+1},\, p} \\ &\implies \mathscr{O}_{\mathbb{A}^{\ell+1},\, p} / \langle \mathbf{h} \rangle = \mathbf{0} \\ &\implies \dim_{\text{vec}}(\mathscr{O}_{\mathbb{A}^{\ell+1},\, p} / \langle \mathbf{h} \rangle) = \dim_{\text{vec}}(\mathbf{0}) = 0. \end{aligned}$$

Conversely when $p \in \mathbf{V}(\mathbf{h})$.

$$\begin{aligned} p \in \mathbf{V}(\mathbf{h}) &\implies \forall\, f \in \mathbf{h};\, f(p) = 0 \\ &\implies \langle \mathbf{h} \rangle \subseteq \langle \mathbf{x} - p \rangle \\ &\implies \mathscr{O}_{\mathbb{A}^{\ell+1},\, p} / \langle \mathbf{x} - p \rangle \subseteq \mathscr{O}_{\mathbb{A}^{\ell+1},\, p} / \langle \mathbf{h} \rangle \\ &\implies \dim_{\text{vec}}(\mathscr{O}_{\mathbb{A}^{\ell+1},\, p} / \langle \mathbf{x} - p \rangle) \leq \dim_{\text{vec}}(\mathscr{O}_{\mathbb{A}^{\ell+1},\, p} / \langle \mathbf{h} \rangle). \end{aligned}$$

As $\mathscr{O}_{\mathbb{A}^{\ell+1},\, p} / \langle \mathbf{x} - p \rangle$ is a field

$$\dim_{\text{vec}}(\mathscr{O}_{\mathbb{A}^{\ell+1},\, p} / \langle \mathbf{x} - p \rangle) = 1$$

so it follows that

$$\forall\, p \in \mathbf{V}(\mathbf{h});\, \dim_{\text{vec}}(\mathscr{O}_{\mathbb{A}^{\ell+1},\, p} / \langle \mathbf{x} - p \rangle) \neq 0.$$

Thus $\operatorname{im}(p;\, \mathbf{h}) = 0 \iff p \notin \mathbf{V}(\mathbf{h})$. □

Proof of (n-3). Recall an affine change of coordinates induces an isomorphism on local rings:

$$\gamma : \mathbb{A}^{\ell+1}(\mathscr{F}) \to \mathbb{A}^{\ell+1}(\mathscr{F}).$$

We have $\mathscr{O}_{\mathbb{A}^{\ell+1},\, p} \cong \mathscr{O}_{\mathbb{A}^{\ell+1},\, \gamma(p)}$ and thus

$$\dim_{\text{vec}}(\mathscr{O}_{\mathbb{A}^{\ell+1},\, p}\,/\langle \mathbf{h} \rangle) = \dim_{\text{vec}}(\mathscr{O}_{\mathbb{A}^{\ell+1},\, \gamma(p)}\,/\langle \mathbf{h} \rangle),$$

from which the result follows immediately. □

Proof of (n-4). As $\langle \mathbf{h} \rangle = \langle \sigma(\mathbf{h}) \rangle$ by the definition of ideal.

$$\begin{aligned} \operatorname{im}(p;\, \mathbf{h}) &= \dim_{\text{vec}}(\mathscr{O}_{\mathbb{A}^{\ell+1},\, p}\,/\langle \mathbf{h} \rangle) \\ &= \dim_{\text{vec}}(\mathscr{O}_{\mathbb{A}^{\ell+1},\, p}\,/\langle \sigma(\mathbf{h}) \rangle) \\ &= \operatorname{im}(p;\, \sigma(\mathbf{h})). \end{aligned}$$

□

Proof of (n-5). Let $\mathbf{h} = (x_0 - p_0)^{m_0}, \ldots, (x_\ell - p_\ell)^{m_\ell}$ and notice $\mathbf{V}(\mathbf{h}) = \{p\}$. As $\langle \mathbf{h} \rangle$ is a Gröbner bases (for any monomial order) the monomials

$$\{x_0^{e_0} \cdots x_\ell^{e_\ell} : 0 \le e_i < m_\ell\}$$

form a vector space basis of $\mathscr{O}_{\mathbb{A}^{\ell+1},\, p}\,/\langle \mathbf{h} \rangle$. Thus $\operatorname{im}(p;\, \mathbf{h}) = m_0 \cdots m_\ell$ by definition. □

Alternate proof of (n-5). Let $\mathbf{h} = (x_0 - p_0)^{m_0}, \ldots, (x_\ell - p_\ell)^{m_\ell}$, assume (n-6) is valid, and notice

$$\forall\, m_0, \ldots, m_\ell \in \mathbb{N};\, \dim_{\text{vec}}(\langle (x_0 - p_0)^{m_0}, \ldots, (x_\ell - p_\ell)^{m_\ell} \rangle) = 0.$$

We can thus invoke (n-6) $m_0 \cdots m_\ell$ times to deduce

$$\operatorname{im}(p;\, (x_0 - p_0)^{m_0}, \ldots, (x_\ell - p_\ell)^{m_\ell})$$

$$
\begin{aligned}
&= \operatorname{im}(p;\, \mathbf{h}^{\downarrow},\, (x_\ell - p_\ell)^{m_\ell}) \\
&= \operatorname{im}(p;\, \mathbf{h}^{\downarrow},\, (x_\ell - p_\ell)^{m_\ell - 1}) + \operatorname{im}(p;\, \mathbf{h}^{\downarrow},\, (x_\ell - p_\ell)) \\
&\;\vdots \\
&= (m_\ell) \cdot \operatorname{im}(p;\, \mathbf{h}^{\downarrow},\, (x_\ell - p_\ell)) \\
&\;\vdots \\
&= (m_0 \cdots m_\ell) \cdot \operatorname{im}(p;\, (x_0 - p_0),\, \ldots, (x_\ell - p_\ell))
\end{aligned}
$$

where

$$\dim_{\text{vec}}(\mathscr{O}_{\mathbb{A}^{\ell+1},\,p}/\langle (x_0 - p_0),\, \ldots, (x_\ell - p_\ell)\rangle) = \dim_{\text{vec}}(\mathscr{F}) = 1.$$

It follows that

$$\operatorname{im}(p;\, (x_0 - p_0)^{m_0},\, \ldots,\, (x_\ell - p_\ell)^{m_\ell}) = m_0 \cdots m_\ell.$$

□

Proof of (n-6). Assume $\dim_{\text{vec}}(p;\, \mathbf{h}^{\downarrow},\, gh) = 0$, let $g, h \in \mathscr{F}[\mathbf{x}]$ be arbitrary, and set for notational convenience:

$$
\begin{aligned}
\mathscr{O}_{gh} &:= \mathscr{O}_{\mathbb{A}^{\ell+1},\,p}/\langle \mathbf{h}^{\downarrow}, gh\rangle, \\
\mathscr{O}_{h} &:= \mathscr{O}_{\mathbb{A}^{\ell+1},\,p}/\langle \mathbf{h}^{\downarrow}, h\rangle, \\
\mathscr{O}_{g} &:= \mathscr{O}_{\mathbb{A}^{\ell+1},\,p}/\langle \mathbf{h}^{\downarrow}, g\rangle.
\end{aligned}
$$

By Definition 3.2

$$
\begin{aligned}
&\operatorname{im}(p;\, \mathbf{h}^{\downarrow},\, gh) = \operatorname{im}(p;\, \mathbf{h}^{\downarrow},\, g) + \operatorname{im}(p;\, \mathbf{h}^{\downarrow},\, h) \\
&\quad\iff \dim_{\text{vec}}(\mathscr{O}_{gh}) = \dim_{\text{vec}}(\mathscr{O}_{g}) + \dim_{\text{vec}}(\mathscr{O}_{h}),
\end{aligned}
$$

so it suffices to show

$$\dim_{\text{vec}}(\mathscr{O}_{g}) - \dim_{\text{vec}}(\mathscr{O}_{gh}) + \dim_{\text{vec}}(\mathscr{O}_{h}) = 0, \tag{3.1}$$

which holds when there is injective ψ and surjective φ so that

$$0 \longrightarrow \mathscr{O}_h \xrightarrow{\psi} \mathscr{O}_{gh} \xrightarrow{\varphi} \mathscr{O}_g \longrightarrow 0$$

is a short exact sequence.

> The meaning behind the (standard) notation of $a = f + \langle \mathbf{h} \rangle$ is used to compactly express
>
> $$a = f + h : h \in \langle \mathbf{h} \rangle.$$
>
> That is, in prose, that a is f plus any element from $\langle \mathbf{h} \rangle$.

Lemma 3.1. There is an *injective* map $\psi : \mathscr{O}_h \to \mathscr{O}_{gh}$ and *surjective* map $\varphi : \mathscr{O}_{gh} \to \mathscr{O}_g$ such that $\operatorname{img}(\psi) = \ker(\varphi)$. That is, the image of ψ is the kernel of φ.

Proof of Lemma. Let

$$\begin{aligned} \psi : \mathscr{O}_h &\to \mathscr{O}_{gh}, & \varphi : \mathscr{O}_{gh} &\to \mathscr{O}_g, \\ f &\mapsto fg \bmod \langle \mathbf{h}^{\downarrow}, gh \rangle, & f &\mapsto f \bmod \langle \mathbf{h}^{\downarrow}, g \rangle. \end{aligned}$$

Since φ is onto by construction we need only show that $\operatorname{img}(\psi) = \ker(\varphi)$ and ψ is injective.

As $\varphi \circ \psi = 0$ we have $\operatorname{img}(\psi) \subseteq \ker(\varphi)$ immediately. For the reverse inclusion take an arbitrary element $u + \langle \mathbf{h}^{\downarrow}, gh \rangle \in \ker(\varphi)$. It follows

$$\varphi(u + \langle \mathbf{h}^{\downarrow}, gh \rangle) = u + \langle \mathbf{h}^{\downarrow}, g \rangle = \langle \mathbf{h}^{\downarrow}, g \rangle,$$

which implies $u \in \langle \mathbf{h}^{\downarrow}, g \rangle$. Thus there is $\{a_h : h \in \mathbf{h}^{\downarrow}\} \subseteq \mathscr{O}_{\mathbb{A}^{\ell+1}, p}$ and $b \in \mathscr{O}_{\mathbb{A}^{\ell+1}, p}$ such that

$$u = bg + \big(\sum_{h \in \mathbf{h}^{\downarrow}} a_h h \big).$$

Considering

$$\psi(b) = bg + \langle \mathbf{h}^{\downarrow}, gh \rangle$$

$$= bg + \big(\sum_{h\in\mathbf{h}^{\downarrow}} a_h h\big) + \langle \mathbf{h}^{\downarrow}, gh\rangle$$
$$= u + \langle \mathbf{h}^{\downarrow}, gh\rangle$$

we see $\psi(b + \langle \mathbf{h}^{\downarrow}, h\rangle) = u + \langle \mathbf{h}^{\downarrow}, h_\ell\rangle$ and thereby $\ker(\varphi) \subseteq \mathrm{img}(\psi)$.

Thus $\ker(\psi) = \mathrm{img}(\varphi)$.

To show ψ is injective, let $u + \langle \mathbf{h}^{\downarrow}, h\rangle \in \ker(\psi)$ be arbitrary. Since

$$\psi(u + \langle \mathbf{h}^{\downarrow}, h\rangle) = ug + \langle \mathbf{h}^{\downarrow}, gh\rangle = \langle \mathbf{h}^{\downarrow}, gh\rangle,$$

it follows that $gu \in \langle \mathbf{h}^{\downarrow}, gh\rangle$. Thus there is $\{a_{h'} : h' \in \mathbf{h}^{\downarrow}\} \subseteq \mathscr{O}_{\mathbb{A}^{\ell+1},\,p}$ so that $ug = bgh + \sum_{h'\in\mathbf{h}^{\downarrow}} a_{h'}h$. Recall g is regular modulo $\langle \mathbf{h}^{\downarrow}\rangle$ because otherwise $\mathbf{h}^{\downarrow}$, g and thus $\mathbf{h}^{\downarrow}$, gh are not regular sequences as assumed. By definition of regularity $u - bh \in \langle \mathbf{h}^{\downarrow}\rangle$ implying $u \in \langle \mathbf{h}^{\downarrow}, h\rangle$.

Thus ψ in injective. □ (n-6) follows from the lemma. □

Proof of (n-7). By definition of an ideal $\langle \mathbf{h}^{\downarrow}, g\rangle = \langle \mathbf{h}, g + h\rangle$ when $h \in \langle \mathbf{h}^{\downarrow}\rangle$ and thus

$$\begin{aligned}\mathrm{im}(p;\, \mathbf{h}^{\downarrow},\, g) &= \dim_{\mathrm{vec}}(\mathscr{O}_{\mathbb{A}^{\ell+1},\,p}/\langle \mathbf{h}^{\downarrow},\, g\rangle)\\ &= \dim_{\mathrm{vec}}(\mathscr{O}_{\mathbb{A}^{\ell+1},\,p}/\langle \mathbf{h}^{\downarrow},\, g+h\rangle)\\ &= \mathrm{im}(p;\, \mathbf{h}^{\downarrow},\, g+h).\end{aligned}$$

□

Because, in general, an arbitrary $\mathscr{F}[\mathbf{x}]$ is *not* a principal ideal domain we are not guaranteed (unlike in the bivariate case) a "Euclid like" step from (n-1) through (n-7). In order to descend to the bivariate case an additional criteria for reducing the $\ell+1$-variate case to the ℓ-variate one is required.

One generically sufficient condition is to test for transversality of the tangent plane h_ℓ with the tangent cone $\mathbf{h}^{\downarrow}$ at p. If the intersection is indeed transversal then h_ℓ can be replaced with a 1-form at p. Provided this 1-form is nonzero, which is assured when h_ℓ is nonsingular, then for

any $x \in \text{indets}(h_\ell)$ the pseudo-remainder $\text{prem}^*(\mathbf{h}^{\downarrow}, h_\ell; x)$ eliminates the variable x from $\mathbf{h}^{\downarrow}$ and

$$\text{im}(p; \mathbf{h}) = \text{im}(p; \text{prem}^*(\mathbf{h}^{\downarrow}, h_\ell; x)).$$

Another strategy is to try and 'cylindrify' the input system. That is, attempt to eliminate a variable via repeated pseudo-divisions among $\mathbf{h}$. Successful application of this procedure yields a cylinder which trivially satisfies transversality.

These concepts form the content of Chapter 6.

Chapter 4

Fulton's Algorithm for Regular Chains

We re-write Fulton's bivariate algorithm using reduction modulo $\langle x - p_0, y - p_1 \rangle$ instead of evaluation at p. We then extend that algorithm to work modulo bivariate regular chains (assuming no splitting) and finally to handle splitting as well.

§4.1 Descriptions

We wish to execute Fulton's algorithm using specialization and splitting instead of explicit evaluation. Namely, given $\mathbf{h} \subseteq \mathscr{F}[\mathbf{x}]$, this algorithm should calculate a 'description' of $\mathbf{h}$.

Definition 4.1 (Description)**.** Let $\mathbf{h}, \mathbf{f}_\triangle \subseteq \mathscr{F}[\mathbf{x}]$ give zero-dimensional ideals and write $\mathrm{im}(\mathbf{f}_\triangle; \mathbf{h}) = m$ if all points of $\mathbf{V}(\mathbf{f}_\triangle)$ have intersection multiplicity m:

$$\mathrm{im}(\mathbf{f}_\triangle; \mathbf{h}) = m \overset{\text{Defn.}}{\iff} \forall\, p \in \mathbf{V}(\mathbf{f}_\triangle);\ \mathrm{im}(p; \mathbf{h}) = m.$$

Let $\{\mathbf{f}_{\triangle,0}, \ldots, \mathbf{f}_{\triangle,e}\}$ be a Kalkbrenner decomposition of $\mathbf{h}$. A *description* of $\mathbf{h}$ is a set of tuples

$$\mathbf{D}(\mathbf{h}) = \{(m_0, \mathbf{f}_{\triangle,0}), \ldots, (m_e, \mathbf{f}_{\triangle,e})\}$$

where each $(m_i, \mathbf{f}_{\triangle,i})$ satisfies $\mathrm{im}(\mathbf{f}_{\triangle,i}; \mathbf{h}) = m_i$.

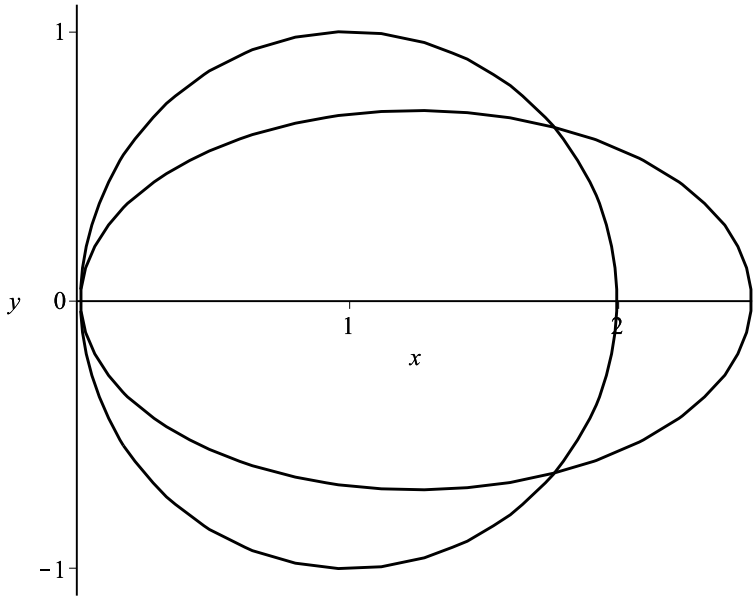


Figure 4.1: A circle and ellipse with IM two at **0** and IM one at the remaining two *irrational* intersection points.

Example 4.1 (Figure 4.1)**.** The circle and ellipse given by

$$\mathbf{h} = \left\{ (x-1)^2 + y^2 - 1,\ \left(\frac{4x}{5} - 1\right)^2 + 2y^2 - 1 \right\} \subseteq \mathscr{R}[x, y]$$

corresponding to the collection of regular chains

$$\mathbf{f}_{\triangle,1} = \begin{cases} x \\ y \end{cases}, \quad \mathbf{f}_{\triangle,2} = \begin{cases} 17x - 30 \\ 289y^2 - 120 \end{cases},$$

has description $\mathbf{D}(\mathbf{h}) = \{(2, \mathbf{f}_{\triangle,1}), (1, \mathbf{f}_{\triangle,2})\}$.

§4.2 Valuations

A good starting point is to devise a splitting algorithm for the *valuation* of a bivariate polynomial $h \in \mathscr{F}[x, y]$ at $p \in \mathbb{A}^{\ell+1}\big(\overline{\mathscr{F}}[\mathbf{x}]\big)$. These strategies will similarly apply to the broader intersection multiplicity the valuation is embedded into.

By valuation we essentially mean the tailing degree, or equivalently the *least* degree among the monomials of a (morally) univariate polynomial. For instance, the valuation of $h \in \mathscr{F}[x, y]$ at $(p_0, p_1) \in \mathbb{A}^2(\mathscr{F})$ is the tailing degree of $h(x, p_1)$ taken in $\mathscr{F}[x - p_0]$. That is to say, the valuation is the maximum m for which $h(x, p_1)$ writes

$$h(x, p_1) = (x - p_0)^m\big(a_m + a_{m+1}(x - p_0) + \cdots + a_d(x - p_0)^{d-m}\big)$$

where $d := \deg(h(x, p_1))$.

Example 4.2. Let

$$h := x^4y + 2x^4 - 4yx^3 - 8x^3 + 7x^2y + 14x^2 - 6xy - 12x + 2y + 4 \in \mathscr{F}[x, y]$$

and consider the valuation at (1, 2). Since $h(x, 2)$, taken as a polynomial from $\mathscr{F}[x - 1]$, has writing

$$h(x, 1) = 4(x - 1)^2\big(1 + (x - 1)^2\big)$$

the valuation of h is 2.

In fact, the valuation about a regular chain $\mathbf{f}_\triangle = \langle f_x, f_y \rangle \in \mathbb{T}(\mathscr{F}[x, y])$ is analogous to the valuation at a point. Here we want the tailing degree of $h \bmod \langle f_y \rangle$ taken as univariate in $\mathscr{F}[f_x]$. Thereby the valuation is the number of f_y factors which can be removed from $h \bmod \langle f_y \rangle$. Or, more precisely,

$$\max(m \in \mathbb{N} : h \bmod \langle f_y \rangle \not\equiv 0 \bmod \langle f_x^m \rangle). \tag{4.1}$$

There is a simple way to express Equation (4.1) recursively. Intuitively we are merely extracting the valuation from the writing of $h \bmod \langle f_y \rangle$ taken

as a univariate in f_x (i.e. from $\mathscr{F}[f_x]$) with as many f_x factors removed:

$$(f_x)^m\big(c_m + c_{m+1}(f_x) + \cdots + c_{m+d}(f_x)^d\big).$$

Recall $\mathbb{U}\langle \mathbf{f}_\triangle \rangle$ are the regular elements in $\mathscr{F}[x,y]/\langle \mathbf{f}_\triangle \rangle$ then

$$\text{Valuation}(\mathbf{f}_\triangle,\, h) = \begin{cases} 0 & \mathbf{f}_\triangle \in \mathbb{U}\langle \mathbf{f}_\triangle \rangle \\ 1 + \text{Valuation}(\mathbf{f}_\triangle,\, \text{quo}(h,\, f_x;\, x)) & \text{otherwise} \end{cases}.$$

However, as noted in §2.5.1, regularity testing modulo a regular chain may induce splitting. We address this by adjusting the output of valuation to return, as with our *descriptions*, a set of pairs encoding the valuations of the corresponding branches. See Algorithm 3 for the realization of this method.

```
1 Function Valuation
      Input:  Let x ≻ y.
        1. f_△ = ⟨ f_0, f_1 ⟩ ∈ T_reg(R[x, y]), and
        2. h ∈ R[x, y].
      Output: Let val(f'_△) = (max(m ∈ ℕ : h mod ⟨ f'_1 ⟩ ≢ 0 mod ⟨ f'_0 ⟩)) then the
              output is {(val(f'_△), f'_△) : f'_△ ∈ △(f_△)}.
2     if |Regularize(f_△; h)| > 1 then
3         return union( Valuation(f'_△; h) : f'_△ ∈ Regularize(f_△; h));
4     if h ∈ U⟨ f_△ ⟩ then
5         return {(0, f_△)};
6     else
7         h' ← quo(h, f_0; x);
8         return {(1 + m', f'_△) : (m', f'_△) ∈ Valuation(f_△; h')};
```

Algorithm 3: Valuation.

Example 4.3. The valuation of

$$(x^2 - x - 1)^3\big(\big(y^2 + 1\big) + (y)\big(x^2 - x - 1\big)\big) \in \mathscr{F}[x, y]$$

about the regular chain

$$\begin{cases} x^2 - x - 1 \\ y^3 \end{cases}$$

is three.

§4.3 Maximal Ideals

Let us rewrite Algorithm 2 using images modulo $\langle x - p_0,\, y - p_1 \rangle$ instead of evaluation. In particular, when h and p are (resp.) restricted to $\mathscr{F}[x, y]$ and $\mathbb{A}^2(\mathscr{F})$, we use

1. $h \bmod \langle x - p_0 \rangle = h(p_0,\, y)$ for $h(p_0,\, y)$,
2. $h \bmod \langle y - p_1 \rangle = h(x,\, p_1)$ for $h(x,\, p_1)$, and
3. $h \bmod \langle x - p_0,\, y - p_1 \rangle = h(p)$ for $h(p_0,\, p_1)$.

See Algorithm 4 for this rewrite.

Example 4.4. The intersection multiplicity of $\mathbf{h} = \{y - x^2,\, y^2 - x^3 - x^2\}$ at the origin calculated using Algorithm 4. Boxed values indicate recursive calls; the remaining is the algorithm's trace.

	LINE
$\boxed{\mathrm{im}_2\big(\,\mathbf{0};\, y - x^2,\, y^2 - x^3 - x^2\big)}$	
$(r,\, s) \leftarrow \deg\big(0 - x^2,\, 0 - x^3 - x^2\big)$	4
$= (2,\, 3)$	11
$h_1' \leftarrow \big(y^2 - x^3 - x^2\big) - x^{3-2}\dfrac{(-1)}{(-1)}(y - x^2)$	12
$= y^2 - x^2 - xy$	

$$\boxed{\operatorname{im}_2\big(\,\mathbf{0};\, y^2 - x^2 - xy,\, y - x^2\big)} \qquad 13$$

$$(r,\, s) \leftarrow \deg\big(0 - x^2 - 0,\, 0 - x^2\big) \qquad 4$$

$$= (2,\, 2) \qquad 11.$$

$$h_1' \leftarrow \big(y^2 - x^2\big) - x^{2-2}\frac{(-1)}{(-1)}(y^2 - x^2) \qquad 12$$

$$= y - y^2$$

$$\boxed{\operatorname{im}_2\big(\,\mathbf{0};\, y - y^2,\, y^2 - x^2 - xy\big)} \qquad 13$$

$$(r,\, s) \leftarrow \deg\big(0 - 0,\, 0 - x^2 - 0\big) \qquad 4$$

$$= (-\infty,\, 2)$$

$$h_1(x, 0) = x^2(-1)\operatorname{im}_2(\implies;\, m) = 2 \qquad 9$$

$$\boxed{2 + \operatorname{im}_2\big(\,\mathbf{0};\, \operatorname{quo}\big(y - y^2,\, y;\, ,\big)\, y^2 - x^2 - xy\big)} \qquad 10$$

$$\operatorname{im}_2\big(\,\mathbf{0};\, 1 - y,\, y^2 - x^2 - xy\big) = 0 \qquad 2$$

$$\boxed{2.} \qquad 3$$

§4.4 Non-Splitting Case

The next step is to lift the restriction on p and allow it to lie in the closure of $\mathscr{F}$. This means the encodings of p may (and will) have degrees greater than one; correspondingly evaluations at p will give polynomials of nonzero degree. Nevertheless, Fulton's algorithm operates as expected.

However there is a caveat: zero tests are required on Line 2 for h_0, $h_1 \not\equiv 0, 0 \bmod \langle \mathbf{f}_\triangle \rangle$ and an additional one on Line 9 to determine the valuation. We assume here that these zero tests will never induce splitting and address this in the next section.

See Algorithm 6 and Example 4.5.

Function $\mathrm{im}_2(\langle x-p_0,\, y-p_1\rangle;\, h_0,\, h_1)$

Input: Let $x \succ y$

1. $\langle x-p_0,\, y-p_1\rangle \in \mathbb{T}_{\mathrm{reg}}(\mathscr{F}[x,y])$, and
2. $h_0,\, h_1 \in \mathscr{F}[x,y] : \dim \langle h_0,\, h_1\rangle = 0$.

Output: $\mathrm{im}_2(\,(p_0,\, p_1);\, h_0,\, h_1) \in \mathbb{N}$.

if $h_0, h_1 \not\equiv 0, 0 \bmod \langle x-p_0,\, y-p_1\rangle$ **then**
  return 0;

$r \leftarrow \deg_x(h_0 \bmod \langle y-p_1\rangle)$;

$s \leftarrow \deg_x(h_1 \bmod \langle y-p_1\rangle)$;

if $r > s$ **then**
  return $\mathrm{im}_2(\langle x-p_0,\, y-p_1\rangle;\, h_1,\, h_0)$;

if $r = -\infty$ **then** /* $y-p_1 \,\big|\, h_0$ */

  $m \leftarrow \min\big(m \in \mathbb{N} : h_1 \not\equiv 0 \bmod \big\langle (x-p_0)^{m+1},\, y-p_1\big\rangle\big)$;

  return $m + \mathrm{im}_2(\langle x-p_0,\, y-p_1\rangle;\, \mathrm{quo}(h_0,\, y-p_1;\, y),\, h_1)$;

if $r \le s$ **then**

  $h' \leftarrow \ell c(h_0 \bmod \langle y-p_1\rangle)\cdot h_1 - x^{s-r}\,\ell c(h_1 \bmod \langle y-p_1\rangle)\cdot h_0$;

  return $\mathrm{im}_2(\langle x-p_0,\, y-p_1\rangle;\, h',\, h_0)$;

Algorithm 4: At the maximal ideal $\langle x-p_0,\, y-p_1\rangle$.

1 **Function** $\mathrm{im}_2(\,\mathbf{f}_{\triangle};\, h_0,\, h_1)$

Input: Let $x \succ y$, $f_0 \in \mathscr{F}[x,y]$, $f_1 \in \mathscr{F}[y]$,
1. $\mathbf{f}_{\triangle} = \langle f_0,\, f_1 \rangle \in \mathbb{T}_{\mathrm{reg}}(\mathscr{F}[x,y])$, and
2. $h_0,\, h_1 \in \mathscr{F}[x,y] : \dim \langle h_0,\, h_1 \rangle = 0$.

Output: $\mathrm{im}(\mathbf{f}_{\triangle};\, h_0,\, h_1) \in \mathbb{N}$.

2 **if** $h_0, h_1 \not\equiv 0, 0 \bmod \langle \mathbf{f}_{\triangle} \rangle$ **then**

3 **return** 0;

4 $r \leftarrow \deg(h_0 \bmod \langle f_1 \rangle)$;

5 $s \leftarrow \deg(h_1 \bmod \langle f_1 \rangle)$;

6 **if** $r > s$ **then**

7 **return** $\mathrm{im}_2(\,\mathbf{f}_{\triangle};\, h_1,\, h_0)$;

8 **if** $r = -\infty$ **then** /* $f_1 \,\big|\, h_0$ */

9 $m \leftarrow \min\big(m \in \mathbb{N} : h_1 \not\equiv 0 \bmod \langle f_0^{m+1},\, f_1 \rangle\big)$;

10 **return** $m + \mathrm{im}_2(\,\mathbf{f}_{\triangle};\, \mathrm{quo}(h_0,\, f_1;\, y),\, h_1)$;

11 **if** $r \leq s$ **then**

12 $h' \leftarrow \ell c(h_0 \bmod \langle f_1 \rangle) \cdot h_1 - (x)^{s-r}\, \ell c(h_1 \bmod \langle f_1 \rangle) \cdot h_0$;

13 **return** $\mathrm{im}_2(\,\mathbf{f}_{\triangle};\, h',\, h_0)$;

Algorithm 5: At a regular chain $\mathbf{f}_{\triangle}$ with no splitting assumed.

Example 4.5. The intersection multiplicity of $\mathbf{h} = \{x^2 - y,\, x^3 + x^2 - y^2\}$ at

$$\mathbf{f}_\triangle = \begin{cases} x - y + 1 \\ y^2 - 3y + 1 \end{cases}$$

calculated using Algorithm 4. Boxed values indicate the recursive calls; the remaining is the algorithm's trace.

	LINE
$\boxed{\mathrm{im}_2\big(\mathbf{f}_\triangle;\, y - x^2,\, y^2 - x^3 - x^2\big)}$	
$(r,\, s) \leftarrow \deg_x\big(x^2 - y,\, x^3 + x^2 - y^2 \bmod \langle y^2 - 3y + 1\rangle\big)$	4
$= \deg_x\big(y - x^2,\, x^3 + x^2 - 3y + 1\big)$	
$= (2,\, 3)$	11
$h_1' \leftarrow h_1 - \mathrm{pivot}(\mathbf{f}_\triangle;\, \mathbf{h})$	12
$= \big(y^2 - x^3 - x^2\big) - \big(-x^{3-2}\big)(y - x^2)$	
$= x^2 + xy - y^2$	
$\boxed{\mathrm{im}_2\big(\mathbf{f}_\triangle;\, x^2 + xy - y^2,\, x^2 - y\big)}$	13
$(r,\, s) \leftarrow \deg_x\big(x^2 + xy - y^2,\, x^2 - y \bmod \langle f_y\rangle\big)$	4
$= \deg_x\big(x^2 + xy - 3y + 1,\, x^2 - y\big)$	
$= (2,\, 2)$	11
$h_1' \leftarrow h_1 - \mathrm{pivot}(\mathbf{f}_\triangle;\, \mathbf{h})$	12
$= \big(x^2 - y\big) - \big(-x^{2-2}\big)(x^2 + xy - y^2)$	
$= y^2 - xy - y$	
$\boxed{\mathrm{im}_2\big(\mathbf{f}_\triangle;\, y^2 - xy - y,\, x^2 + xy - y^2\big)}$	12
$(r,\, s) \leftarrow \deg_x\big(y^2 - xy - y,\, x^2 + xy - y^2 \bmod \langle f_y\rangle\big)$	4
$= \deg_x\big(2y - xy - 1,\, x^2 + xy - 3y + 1\big)$	
$= (1,\, 2)$	11
$h_1' \leftarrow (x^2 + xy - y^2) - (-2 + y)\big(x^{2-1}\big)\big(y^2 - xy - y\big)$	12

$$= \big(y^2 - 3y + 1\big)x^2 + \big(-y^3 + 4y^2 - 2y\big)x - y^2$$

$$\boxed{\mathrm{im}_2\big(\mathbf{f}_\triangle;\, h_1',\, y^2 - xy - y\big)} \qquad 13$$

$$(r,\, s) \leftarrow \deg_x\big(h_0,\, y^2 - xy - y \bmod \langle f_y \rangle\big) \qquad 4$$

$$= \deg_x(2xy - x - 3y + 1,\, -xy + 2y - 1)$$

$$= (1,\, 1) \qquad 11$$

$$h_1' \leftarrow \big(y^2 - xy - y\big) - (2y + 5)\big(x^{1-1}\big)h_0 \qquad 12$$

$$= \big(2y^4 - 11y^3 + 17y^2 - 5y\big)x^2 + \big(-2y^5 + 13y^4 - 24y^3 + 10y^2 - y\big)x + \big(-2y^4 + 5y^3 + y^2 - y\big)$$

$$\boxed{\mathrm{im}_2(\,\mathbf{f}_\triangle;\, h_1',\, h_0)} \qquad 13$$

$$(r,\, s) \leftarrow \deg_x(h_0,\, h_1 \bmod \langle f_y \rangle) \qquad 4$$

$$= \deg_x(0,\, 2xy - x - 3y + 1)$$

$$= (-\infty,\, 1) \qquad 8$$

$$m \leftarrow \text{Tailing degree of } h_1 \text{ in } \mathscr{R}/\langle f_y \rangle\,[f_x]. \qquad 9$$

$$h_1 = \big(y^2 - 3y + 1\big)x^2 + \big(-y^3 + 4y^2 - 2y\big)x - y^2$$

$$= (f_y x + 2y - 1)f_x + f_y$$

$$\equiv (2y - 1)f_x + 0 \bmod \langle f_y \rangle$$

$$= 1$$

$$\boxed{1 + \mathrm{im}_2(\,\mathbf{f}_\triangle;\, \mathrm{quo}(h_0,\, \mathbf{f}_\triangle^{\downarrow};\, ,)\, h_1)} \qquad 10$$

$$h_0,\, h_1 \not\equiv \mathbf{0} \bmod \langle \mathbf{f}_\triangle \rangle \qquad 2$$

$$= 0 \qquad 3$$

$$\boxed{\mathrm{im}_2(\,\mathbf{f}_\triangle;\, h_0,\, h_1) = 1.}$$

Finally, let us provide justification for Algorithm 6 by demonstrating each calculation leaves the intersection multiplicity invariant and that the process eventually terminates.

Proposition 4.1. Each line of Algorithm 6 uses only the "allowed opera-

tions" from (2-1) through (2-7).

Proof. Lines 2 and 7 are justified by properties (2-2) and (2-4) respectively.

When $r = -\infty$ we have that h_0 writes $f_y\, h_0'$ and thereby

$$\mathrm{im}_2(\,\mathbf{f}_\triangle;\, f_y\, h_0',\, h_1) = \mathrm{im}_2(\,\mathbf{f}_\triangle;\, f_y,\, h_1) + \mathrm{im}_2(\,\mathbf{f}_\triangle;\, h_0',\, h_1)$$

by property (2-6).

Furthermore, as $h_1 \mathrm{mod} \langle\, f_y \,\rangle$ writes $(f_x)^m(a_m + a_{m+1}f_x + \cdots)$ we deduce

$$\begin{aligned}\mathrm{im}_2(\,\mathbf{f}_\triangle;\, f_y,\, h_1) &= \mathrm{im}(\mathbf{f}_\triangle;\, h_1 \bmod \langle\, f_y \,\rangle) \\ &= \mathrm{im}(\mathbf{f}_\triangle;\, (f_x)^m(a_m + a_{m+1}f_x + \cdots)\,) \\ &= m\end{aligned}$$

via property (2-5). Collectively this justifies line 10.

Finally, when $r \leq s$ the pivot requires only property (2-7).

□

Proposition 4.2. Algorithm 6 terminates.

Proof. The degree in x of $h_0 \bmod \langle\, y - p_1 \,\rangle$ is greater than zero only when $h_0(x,\, p_1) \in \mathscr{F}[\mathbf{x}]$; in this case line 2 triggers and zero returns. By line 7 $r > s$ is impossible. When $r = -\infty$ we remove one factor of $y - p_1$ and this cannot increase the degree in x. Finally, when $r \leq s$ the pivot on line 12 reduces the degree in x by design.

Thereby (forgetting line 7) the r strictly descends except when factors of $y - p_1$ are removed—however this can happen only finitely many times. □

§4.5 Splitting Case

In this case we simply invoke the D5 principle to justify the splitting step.

Proposition 4.3. Algorithm 6 is correct.

Proof. We (necessarily) gloss over the details here as they are beyond the scope of this work. We recall, as mentioned, that the D5 principle (loosely

speaking) enables an algorithm over a field (i.e. a non-splitting algorithm) to be imbued with splitting.

As the only splittings here are invoked in line 2 and 7 by regularization the computation is indeed decomposed, or 'split', into multiple computations over a *product of fields*. □

Proposition 4.4. Algorithm 6 terminates.

Proof. Regularizing can never produce infinite branches so each step with splitting reduces the calculation to that of new regular chains of strictly lower degree. □

Function $\mathrm{im}_2^*(\,\mathbf{f}_\triangle;\, h_0,\, h_1)$

Input: Let $x \succ y$, $f_0 \in \mathscr{F}[x,y]$, $f_1 \in \mathscr{F}[y]$,

1. $\mathbf{f}_\triangle = \langle f_0,\, f_1 \rangle \in \mathbb{T}_{\mathrm{reg}}(\mathscr{F}[x,y])$, and
2. $h_0,\, h_1 \in \mathscr{F}[x,y]$.

Output: $\mathbf{D}(\mathbf{f}_\triangle;\, h_0,\, h_1) \subseteq \mathbb{N} \times \mathbb{T}_{\mathrm{reg}}(\mathscr{F}[x,y])$.

if $h_0 \in \mathbb{U}\langle \mathbf{f}_\triangle \rangle$ or $h_1 \in \mathbb{U}\langle \mathbf{f}_\triangle \rangle$ **then**
  return $\{(0,\, \mathbf{f}_\triangle)\}$;
else if $|\mathrm{Regularize}(\mathbf{f}_\triangle;\, h_0,\, h_1)| > 1$ **then**
  return $\mathrm{union}(\,\mathrm{im}_2^*\big(\,\mathbf{f}'_\triangle;\, h_0,\, h_1\big) : \mathbf{f}'_\triangle \in \mathrm{Regularize}(\mathbf{f}_\triangle;\, h_0,\, h_1))$;

if $\mathrm{init}(h_0) \in \mathbb{U}\langle \mathbf{f}_\triangle \rangle$ and $\mathrm{init}(h_1) \in \mathbb{U}\langle \mathbf{f}_\triangle \rangle$ **then**
  $r,\, s \leftarrow \deg_x(h_0, h_1 \bmod \langle f_1 \rangle)$;
else if $|\mathrm{Regularize}(\mathbf{f}_\triangle;\, \mathrm{init}(h_0,\, h_1))| > 1$ **then**
  return $\mathrm{union}(\,\mathrm{im}_2^*\big(\,\mathbf{f}'_\triangle;\, h_0,\, h_1\big) : \mathbf{f}'_\triangle \in \mathrm{Regularize}(\mathbf{f}_\triangle;\, \mathrm{init}(h_0,\, h_1)))$;

if $r > s$ **then**
  return $\mathrm{im}_2^*(\,\mathbf{f}_\triangle;\, h_1,\, h_0)$;

if $r = -\infty$ **then** /* $h_0 \equiv 0 \bmod \langle f_1 \rangle$ */
  for $\big(m',\, \mathbf{f}'_\triangle\big) \in \mathrm{Valuation}(\mathbf{f}_\triangle;\, h_1)$ **do**
    return $\big\{\big(m' + m'',\, \mathbf{f}''_\triangle\big) : \big(m'', \mathbf{f}''_\triangle\big) \in \mathrm{im}_2^*\big(\,\mathbf{f}'_\triangle;\, \mathrm{quo}(h_0,\, f_0;\, y),\, h_1\big)\big\}$;

if $r \leq s$ **then**
  $h' \leftarrow \mathrm{pivot}(\mathbf{f}_\triangle;\, h_0,\, h_1)$;
  return $\mathrm{im}_2^*(\,\mathbf{f}_\triangle;\, h',\, h_0)$;

Algorithm 6: With splitting.

Chapter 5

Tangent Cones

Unlike a tangent hyperplane, computing a tangent cone of a one dimensional curve is *not* computationally easy. As our computation of intersection multiplicity in dimension greater than two has this as a bottleneck, we were motivated to create a practically efficient tangent cone algorithm. We realized such an algorithm by viewing each line of a tangent cone as the limit — along of curve — of some sequence of 'secant' lines.

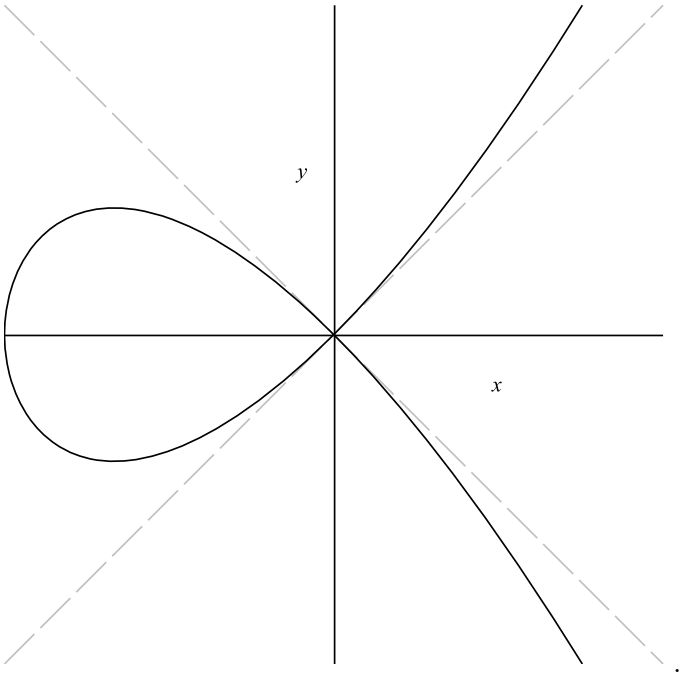
We present an efficient algorithm, based on triangular decomposition, for the computation of tangents cones on one-dimensional curves in dimension $\ell + 1$. Up to our knowledge (and up to this point) there was no alternative method which did not utilize Gröbner bases or standard bases in some way. And the use of either was causing our algorithms to bottleneck at transversality checking.

§5.1 Singularities

Sometimes it is useful to investigate the local behaviour of a variety near a point. When this point is 'nice' (which in our case means non-singular) tangent planes provide adequate linear descriptions of the variety around that point. However further consideration is required when the point is singular.

In the planar case, singular points are those places on the curve where the gradient vanishes. Geometrically, these are points like crossovers or cusps which cannot be approximated by single lines.

For example, consider the typical 'fish' system, a planar curve given by $h = y^2 - x^2(x+1) \in \mathscr{F}[x, y]$:



Notice there are two tangent lines through the origin. Correspondingly, we see in Figure 5.1 by looking locally about the origin that a single tangent line is insufficient to approximate h at the origing. In this case *two* lines are required.

In general, when $\mathbf{h} \subseteq \mathscr{F}[\mathbf{x}]$ and $p \in \mathbf{V}(\mathbf{h})$ is singular then the tangent space of $\mathbf{V}(\mathbf{h})$ at p is *not* a single tangent line. This is because the dimension of the tangent space is different than that of the variety at p. In fact singular points can be defined by this property.

Definition 5.1 (Dimension of a variety)**.** Let V be a variety and $p \in V$. The dimension of V at p is the maximum dimension of an irreducible component of V containing p. Denote this value by $\dim_p(V)$.

Definition 5.2 (Tangent Space)**.** Let $\mathbf{h} \subseteq \mathscr{F}[\mathbf{x}]$, $p \in \mathbf{V}(\mathbf{h})$, $f \in \mathscr{F}[\mathbf{x}]$.

The *tangent space* of $\mathbf{V}(\mathbf{h})$ at p is the variety

$$T_p(\mathbf{h}) := \mathbf{V}(\pi_p(f) : f \in \langle \mathbf{h} \rangle)$$

where $\pi_p(f)$ is the (equation for) the *linear part*

$$\frac{\partial f}{\partial x_0}(p)(x_0 - p_0) + \cdots + \frac{\partial f}{\partial x_\ell}(p)(x_\ell - p_\ell).$$

or (equivalently) the tangent plane of f at p.

Definition 5.3 (Singular)**.** Let $\mathbf{h} \subseteq \mathscr{F}[\mathbf{x}]$ and $p \in \mathbf{V}(\mathbf{h})$. Then p is *non-singular* (or *smooth*) when

$$\dim_{\text{vec}}(T_p(\mathbf{h})) = \dim_p(V)$$

and *singular* otherwise. Moreover define the *singular locus* of $\mathbf{h}$ as

$$\text{sing}(\mathbf{h}) := \{p \in \mathbf{V}(\mathbf{h}) : p \text{ is singular}\}.$$

§5.2 Homogeneous Components

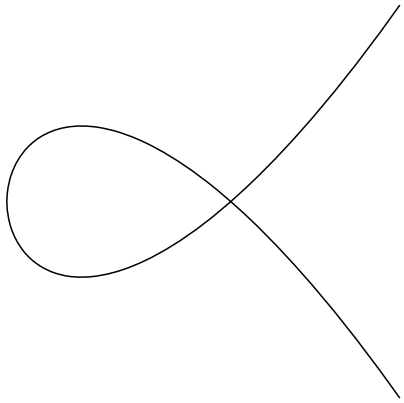
Formally, the tangent cone of a *curve* $\mathbf{h}$ *at the origin* is given by the homogeneous components of least degree among $\langle \mathbf{h} \rangle$. Homogeneous polynomials have the property that all terms have equivalent degree. For example $x^5 + 2x^2y^3 + xy^4$ is a homogeneous polynomial.

Arbitrary polynomials can then be written as a sum of homogeneous polynomials like

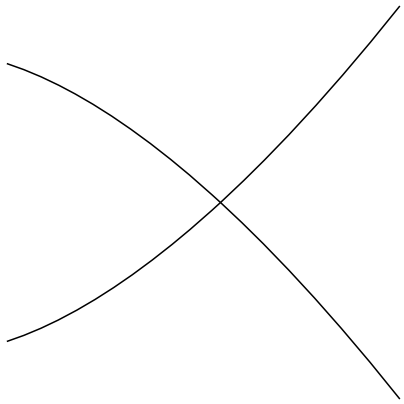
$$\left(53y^2x - 75yz^2 + 5z^3\right) + \left(27x^2 - 15xy + 16xz + 3yz\right) + (68x - 10y + 31z)$$

but more generally as

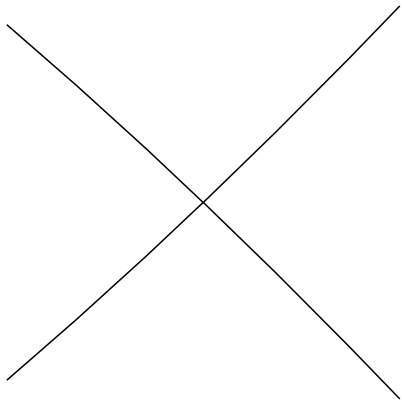
$$h = \sum_{d=0}^{\deg(h)} \sum (t \in \text{terms}(h) : \deg(t) = d). \tag{5.1}$$



(a) The fish.



(b) Closer to origin.



(c) Very close to the origin.

Figure 5.1: Investigating the local behaviour of $y^2 - x^2(x+1)$. Notice a single line is insufficient to approximate the curve at the origin.

The groupings of terms of equivalent degree in (5.1) are called the *homogeneous components* of h.

Definition 5.4 (Homogeneous Component)**.** Let $h \in \mathscr{F}[\mathbf{x}]$. The degree d homogeneous component of h is

$$\sum(t : t \in \text{terms}(h) \text{ and } \deg(t) = d).$$

The degree d homogeneous component of $h \in \mathscr{F}[\mathbf{x} - p]$ is

$$\text{HC}_p(h;\, d) := \sum\big(t \in \text{terms}(h) : \deg_{(\mathbf{x}-p)}(t) = d\big).$$

Moreover let the *homogeneous component of least degree* (corresponding to the smallest d for which $\{t \in \text{terms}(h) : \deg(t) = d\}$ is non-empty) be denoted $\text{HC}_p(h;\, \min)$

$$\text{HC}_p(h;\, \min) := \text{HC}_p(h;\, d),$$

where $d = \min(d \in \mathbb{N} : \text{HC}_p(h;\, d) \neq 0)$.

§Classical Tangent Cone Definition

The tangent cone of $\mathbf{h}$ is the ideal generated by the homogeneous components of least degree among $\langle \mathbf{h} \rangle$.

Definition 5.5 (Tangent Cone)**.** Let $\mathbf{h} \subseteq \mathscr{F}[\mathbf{x}]$ and $p \in \mathbf{V}(\mathbf{h})$. The *tangent cone* of $\mathbf{h}$ at p is the ideal generated by the homogeneous components in $\mathbf{x} - p$ of least degree among $\langle \mathbf{h} \rangle$

$$\kappa_p(\mathbf{h}) := \langle\, \text{HC}_p(h;\, \min) : h \in \langle \mathbf{h} \rangle\, \rangle.$$

For principally generated ideals this is easy as we need only find the homogeneous component of least degree of among the single generator. In other words, we require no ideal manipulation to calculate $\langle\, \text{HC}_p(h;\, \min)\, \rangle$.

Example 5.1. Let $\mathbf{h} = \{y^2 - x^2(x+1)\} \subseteq \mathscr{F}[x, y]$ and note $\mathbf{h}$ is a basis of $\langle \mathbf{h} \rangle$. Accordingly, the tangent cone at the origin is the homogeneous

component of least degree from $y^2 - x^3 - x^2$:

$$\kappa_{\mathbf{0}}\big(y^2 - x^2(x+1)\big) = \big\{y^2 - x^2\big\} = \{(x+y)(x-y)\}.$$

Which are the expected two lines through the origin.

For ideals with more generators however it need *not* follow that

$$\langle\, \mathrm{HC}_p(h;\, \mathrm{min}) : h \in \langle \mathbf{h} \rangle \,\rangle \stackrel{?}{=} \langle\, \mathrm{HC}_p(h;\, \mathrm{min}) : h \in \mathbf{h} \,\rangle. \tag{5.2}$$

Example 5.2. Let $\mathbf{h} = \{h_0,\, h_1\} = \{xz + z(y^2 - z^2),\, xy\} \subseteq \mathscr{F}[x,\, y,\, z]$. Notice $y \cdot h_1 - xy \cdot h_0 = yz(y^2 - z^2) \in \langle \mathbf{h} \rangle$ and therefore

$$\mathrm{HC}_{\mathbf{0}}(y\, h_0 - z\, h_1;\, \mathrm{min}) = yz(y^2 - z^2)$$

implying $yz(y^2 - z^2) \in \langle\, \mathrm{HC}_{\mathbf{0}}(h;\, \mathrm{min}) : h \in \langle \mathbf{h} \rangle \,\rangle$. However

$$\langle\, \mathrm{HC}_{\mathbf{0}}(h;\, \mathrm{min}) : h \in \big\{xz + z(y^2 - z^2),\, xy\big\} \,\rangle = \langle xz,\, xy \rangle$$

and clearly $yz(y^2 - z^2) \notin \langle xz,\, xy \rangle$ and thus $yz(y^2 - z^2) \notin \langle\, \mathrm{HC}_{\mathbf{0}}(h;\, \mathrm{min}) : h \in \mathbf{h} \,\rangle$.

One can compute $\langle\, \mathrm{HC}_p(h;\, \mathrm{min}) : h \in \langle \mathbf{h} \rangle \,\rangle$ by finding a graded Gröbner basis (say $\mathbf{G}$) of the *homogenization* of $\mathbf{h}$ (a process where an additional name $x_{\ell+1}$ is used to make every $h \in \mathbf{h}$ a homogeneous polynomial in $\mathscr{F}[\mathbf{x}][x_{\ell+1}]$). *Dehomogenizing* $\mathbf{G}$ (that is, removing $x_{\ell+1}$ by setting it to one) produces the tangent cone of $\mathbf{h}$ [10, Chapter 9 §7 Proposition 4]. (This way of computing tangent cones was investigated by Mora et al. in [27].)

Example 5.3. Continuing Example 5.2 the homogenization of $\mathbf{h}$ in t is $\{txz + y^2z - z^3,\, xy\}$ which has a graded Gröbner basis (with t largest) given by $\mathbf{G} = \{xy,\, tx + y^2 - z^2,\, y^3 - yz^2\}$. Dehomogenizing $\mathbf{G}$ leaves $\{xy,\, y^2 - z^2 + x,\, y^3 - yz^2\}$ and therefore the tangent cone of $\mathbf{h}$ is $\kappa_{\mathbf{0}}(\mathbf{h}) = \langle xy,\, x,\, y^3 - yz^2 \rangle$.

Since Gröbner basis computation can be expensive let us explore calculating these tangent lines as limits of secants instead.

§Secants

There is an alternate definition for tangent cones which enables the construction of lines in the tangent cone using limits of *secants*.

Theorem 5.1. Let $\mathbf{h} \subseteq \mathscr{F}[\mathbf{x}]$. A line L through $p \in \mathbf{V}(\mathbf{h})$ lies in the tangent cone $\kappa_p(\mathbf{h})$ *if and only if* there is a sequence of points from $\mathbf{V}(\mathbf{h}) - \{p\}$ converging to p where the secant lines L_k containing p and q_k become L in the limit.

Equivalently,

$$L \in \kappa_p(\mathbf{h}) \iff$$
$$\exists \{q_k : k \in \mathbb{N}\} \subseteq \mathbf{V}(\mathbf{h}) - \{p\} : \lim_{k\to\infty} q_k = p \text{ and } \lim_{k\to\infty} L_k = L.$$

Proof. See [10, Chapter 9 §7 Theorem 6]. □

§5.3 Tangent Cone Algorithm

As the following is mainly a geometric presentation we use the geometric analogue of the tangent cone and let $TC_q(\mathbf{V}(\mathbf{h}))$ denote the tangent cone of $\mathbf{V}(\mathbf{h})$ at q. Namely,

$$TC_q(\mathbf{h}) := \mathbf{V}(\kappa_q(f) : f \in \langle \mathbf{h} \rangle).$$

This is much like using a tangent *space* rather than a tangent *plane*.

Let $\mathscr{F}$ be a field, $\mathbf{h} = \{h_0, \ldots, h_{\ell-1}\} \subseteq \mathscr{F}[\mathbf{x}]$ a collection of polynomials, and $p \in \mathbf{V}(\mathbf{h})$. For this section (and without loss of generality) assume

1. $\overline{\mathscr{F}} = \mathbb{C}$ (the complex numbers) and that
2. $\mathbf{V}(h)$ is non-singular at p for any $h \in \mathbf{h}$.

For each branch of a connected component $\mathscr{D}$ through p of $\mathscr{C} = \mathbf{V}(\mathbf{h})$ there is a neighbourhood B about p in the analytic topology where $\mathbf{V}(h_0)$

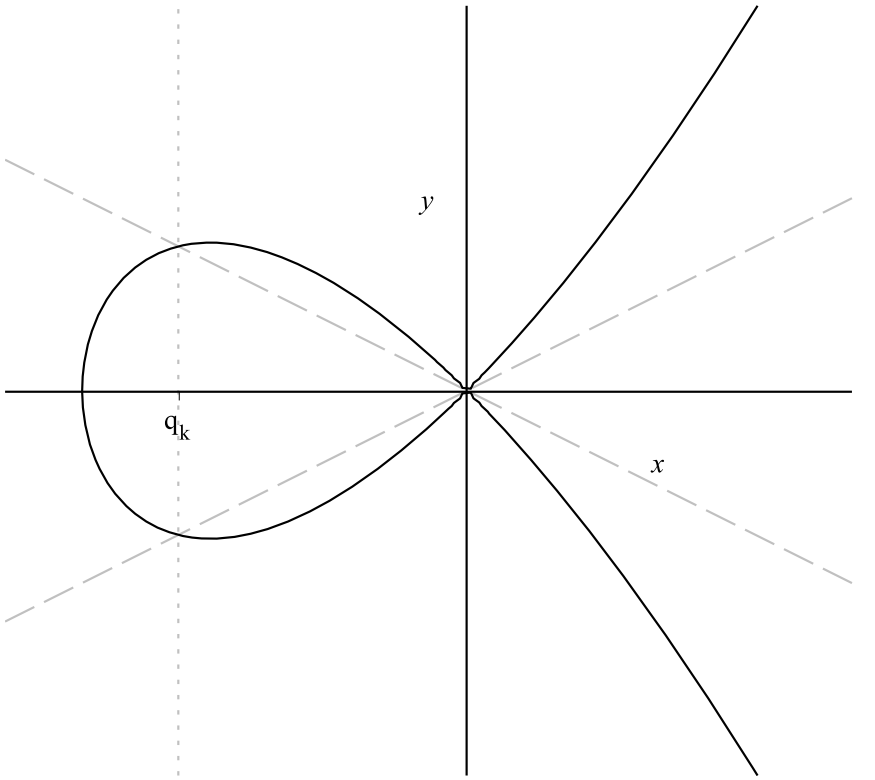


Figure 5.2: Secant lines on the fish.

through $\mathbf{V}(h_{\ell-1})$ are non-singular for each $q \in (B \cap \mathscr{D}) - \{p\}$. Moreover, the singular locus $\text{sing}(\mathscr{D})$ contains a *finite* number of points.

Take B small enough so that $B \cap \text{sing}(\mathscr{D})$ is either empty or $\{p\}$ and recall $\mathbf{V}(\pi_q(h_0))$ is the tangent hyperplane of $\mathbf{V}(h_i)$ at q. Regard $\mathbf{V}(\pi_q(h_0), \ldots, \pi_q(h_{\ell-1}))$ as the zero set of a parametric polynomial system, with coordinates of q as parameters and let

$$v(q) := T_q(h_0) \cap \cdots \cap T_q(h_{\ell-1}).$$

We obtain $TC_p(\mathscr{C})$ by taking the limit of $v(q)$ as q approaches p. Since $TC_p(\mathscr{C})$ is the union of all the $TC_p(\mathscr{D})$ we are done. Crucially, this process can be simulated through variable elimination.

Lemma 5.1. The collection of limits of lines $v(q)$ in $TC_p(\mathscr{D})$ as q approaches p along the branches of $\mathscr{D}$ gives the tangent cone of $\mathscr{D}$ at q. That is to say

$$TC_p(\mathscr{D}) = \lim_{q \to p} v(q) = \lim_{q \to p} T_q(h_0) \cap \cdots \cap T_q(h_{\ell-1}).$$

Proof. There are two cases, either

1. $\mathscr{D}$ is *smooth* at p and $B \cap \text{sing}(\mathscr{D}) = \varnothing$, or
2. $\mathscr{D}$ is *singular* at p and $B \cap \text{sing}(\mathscr{D}) = \{p\}$.

Case 1. Assume $q \in B \cap \mathscr{D}$ is arbitrary and observe $\mathscr{D}$ is smooth within B and thereby the tangent cone of $\mathscr{D}$ is simply the tangent space (i.e. $TC_q(\mathscr{D}) = T_q(\mathscr{D})$).

Notice $T_q(\mathscr{D})$ is a sub-vector space of $v(q)$. Indeed, let $w \in T_q(\mathscr{D})$ be any tangent vector to $\mathscr{D}$ at q. As $\mathscr{D}$ is a curve in each $\mathbf{V}(h)$ for $h \in \mathbf{h}$ it follows w is a vector tangent to each $\mathbf{V}(h)$ as well. Correspondingly $w \in T_q(h)$ for any $h \in \mathbf{h}$ and thus $w \in v(q)$.

Finally, since $h_0, \ldots, h_{\ell-1}$ form a local complete intersection in B, we know $v(q)$ is a one-dimensional subspace of each $T_q(h_0)$. Since $w \in T_q(h)$ for each $h \in \mathbf{h}$, the vector w must span this subspace. Thus, for each

$q \in B \cap \mathscr{D}$, we have

$$T_q(\mathscr{D}) = T_q(h_0) \cap \cdots \cap T_q(h_{\ell-1}).$$

Taking the limit of each side of the above equality, when q approaches p and using again the fact that $\mathscr{D}$ is smooth at $q = p$, we obtain the desired result, that is, $TC_p(\mathscr{D}) = \lim_{q \to p} v(q)$.
Case 2. Assume $\mathscr{D} \cap B - \{p\}$ is a finite union of smooth curves $\mathscr{D}_0, \ldots, \mathscr{D}_j$. These are the smooth branches of $\mathscr{D} \cap B$ meeting at the singular point p. Each j corresponds to a unique line

$$L_j = \lim_{q \to p} v(q) \subseteq T_p(\mathscr{D})$$

as q approaches p *along* $\mathscr{D}_j$.

By Theorem 5.1 the tangent cone $TC_p(\mathscr{D})$ is the collection of limits to p of secant lines through p in $\mathscr{D}$. Such lines given by secants along $\mathscr{D}_j$ must coincide with L_j. More precisely

$$L_0 \cup \cdots \cup L_j \subseteq TC_p(\mathscr{D}).$$

Because each $\mathscr{D}_j$ is smooth there is only one secant line for each j and thereby

$$L_0 \cup \cdots \cup L_j = TC_p(\mathscr{D})$$

as desired. □

Lemma 5.1 states a principle. Let us now give a precise algorithm implementing this principle.

Let q be a point on the curve $\mathscr{C} = \mathbf{V}(\mathbf{h})$ with co-ordinates $\mathbf{x}$. Further let $\widehat{pq}$ be a unit vector in the direction of $\overline{pq}$ (i.e. the line through p and q). To exploit Theorem 5.1 we must calculate

$$\left\{ \lim_{\substack{q \to p \\ q \neq p}} \widehat{pq} \right\},$$

which is indeed a set because there can be many branches of $\mathscr{C}$ through p.

Let $\mathbf{f}_\triangle \in \mathbb{T}(\mathscr{F}[\mathbf{y}])$ be a zero-dimensional regular chain encoding the point p. This renaming of $\mathbf{x}$ to $\mathbf{y}$ is necessary since the "moving point" q is already using $\mathbf{x}$ for its coordinates. Consider the polynomial set

$$\mathbf{s} = \mathbf{f}_\triangle \cup \{h_0, \ldots, h_{\ell-1}\}.$$

and observe that the ideal $\langle \mathbf{s} \rangle$ is one-dimensional in $\mathscr{F}[x_{\ell-1} \succ \cdots \succ x_0 \succ y_{\ell-1} \succ \cdots \succ y_0]$. Let $\{\mathbf{f}_{\triangle,0}, \ldots, \mathbf{f}_{\triangle,e}\} \subseteq \mathscr{F}[\mathbf{y}][\mathbf{x}]$ be regular chains forming a Kalkbrenner decomposition of $\mathbf{s}$. Thus we have

$$\mathbf{V}(\mathbf{s}) = \overline{\mathbf{W}(\mathbf{f}_{\triangle,0})} \cup \cdots \cup \overline{\mathbf{W}(\mathbf{f}_{\triangle,e})}$$

where each $\langle \mathbf{f}_{\triangle,0} \rangle$ through $\langle \mathbf{f}_{\triangle,e} \rangle$ is one-dimensional.

Computing with the normal vector $\widehat{pq}$ is unnecessary so we instead divide the entries of $\overline{pq}$ by $x_\ell - y_\ell$ (making the last position one). This enables a limit computation only when $x_\ell - y_\ell$ vanishes finitely many times in $\mathbf{V}(\mathbf{s})$. When this is the case, the lines of the tangent cone not contained in the hyperplane $y_\ell = x_\ell$ can be obtained via limits of meromorphic functions (namely Puiseux series expansions) by letting $x_\ell \to y_\ell$ [2]. Moreover we are ensured there is an ordering of $\mathbf{x}$ for which $x_\ell - y_\ell$ is regular, as we shall prove below.

Since the tangent cone may have lines contained in the hyperplane $y_\ell - x_\ell$, additional computations are needed to capture them. There are essentially three options.

1. A randomized approach where a random linear change of the coordinates is performed so as to avoid those particular lines, generically.

2. A reduction of the problem to lower dimension by adding the constraint $y_\ell - x_\ell$ so as to capture those particular lines.

3. Compute in turn the lines not contained in the hyperplane $y_i = x_i$ for $i = 0, \ldots, \ell$ and remove the duplicates.

In our implementation, we have experimented with the first and third approaches. Although the third one seems gross, it avoids the expression

swell of the first one and is practically more efficient. The second approach should not have the limitations of the other two and is currently work in progress.

From now on, we focus on computing the lines of the tangent cone *not* contained in the hyperplane $y_\ell - x_\ell$. Or, equivalently, we assume the tangent cone transversally intersects the hyperplane $y_\ell - x_\ell$.

> A *meromorphic function*, loosely speaking, is one that is holomorphic everywhere but at its poles.
>
> For our purposes, holomorphic functions can be regarded as complex valued functions of one or more complex variables.

Fortunately, deciding whether $x_\ell - y_\ell$ vanishes finitely many times in $\mathbf{V}(\mathbf{s})$ *can* be done algorithmically by testing whether $x_\ell - y_\ell$ is regular modulo the saturated ideal of a regular chain. Let $\mathbf{f}_{\triangle,j} \in \{\mathbf{f}_{\triangle,0}, \ldots, \mathbf{f}_{\triangle,e}\}$ be arbitrary and assume $x_\ell - y_\ell$ is regular modulo $\mathrm{sat}(\mathbf{f}_{\triangle,j})$. Because

$$\mathbf{V}(x_\ell - y_\ell) \cap \overline{\mathbf{W}(\mathbf{f}_{\triangle,j})}$$

is zero-dimensional, each component of $\overline{pq}$ is divisible by $x_\ell - y_\ell$, when q is close enough to p, with $q \neq p$.

If $x_\ell - y_\ell \equiv 0 \bmod \mathrm{sat}(\mathbf{f}_{\triangle,j})$ then $\overline{\mathbf{W}(\mathbf{f}_{\triangle,j})} \subseteq \mathbf{V}(x_\ell - y_\ell)$ permitting us to attempt to divide each component of $\overline{pq}$ by $x_{\ell-1} - y_{\ell-1}$ instead of $x_\ell - y_\ell$. A key observation is

$$\exists\, d \in \{0, \ldots, \ell\} : x_d - y_d \not\equiv 0 \bmod \mathrm{sat}(\mathbf{f}_{\triangle,j}).$$

Indeed, if (conversely)

$$\begin{aligned} x_\ell - y_\ell &\equiv 0 \bmod \mathrm{sat}(\mathbf{f}_{\triangle,j}) \\ &\vdots \\ x_0 - y_0 &\equiv 0 \bmod \mathrm{sat}(\mathbf{f}_{\triangle,j}) \end{aligned}$$

then $\overline{\mathbf{W}(\mathbf{f}_{\triangle,j})} \subseteq \mathbf{V}(x_0 - y_0) \cap \cdots \cap \mathbf{V}(x_\ell - y_\ell)$. Since the $\mathbf{y}$ are fixed by $\mathbf{f}_\triangle$ we have $\overline{\mathbf{W}(\mathbf{f}_{\triangle,j})}$ is zero-dimensional — a contradiction.

Assume then, that $x_\ell - y_\ell$ is regular modulo $\mathrm{sat}(\mathbf{f}_{\triangle,j})$. If follows $x_\ell \neq y_\ell$ when q is close enough to (but not equal to) p. Define

$$m_0 = \frac{x_0 - y_0}{x_\ell - y_\ell}, \ldots, m_\ell = \frac{x_\ell - y_\ell}{x_\ell - y_\ell}.$$

and regard $\mathbf{m} = \{m_0, \ldots, m_\ell\}$ as new variables. We have $\widehat{pq} = \langle\langle\, m_0, \ \ldots, \ m_{\ell-1}, \ 1\,\rangle\rangle$ and our goal is to "solve for" $\mathbf{m}$ when $x_\ell \to y_\ell$.

We use [2] to turn this question into one computing the limit points of a one-dimensional regular chain. To this end, extend the regular chain $\mathbf{f}_{\triangle,j}$ to the regular chain $\mathcal{M}_\triangle \in \mathbb{T}(\mathscr{F}[\mathbf{y}][\mathbf{x}])$ given by

$$\mathcal{M}_{\triangle,j} = \mathbf{f}_{\triangle,j} \cup \begin{cases} m_0(x_0 - y_0) - (x_\ell - y_\ell) \\ \ \vdots \\ m_\ell(x_\ell - y_\ell) - (x_\ell - y_\ell) \end{cases}.$$

Note $\mathcal{M}_{\triangle,j}$ is one-dimensional in this extended space.

Finally $\{\lim_{q \to p, q \neq p} \widehat{pq}\}$ are the limit points of the quasi-component of $\mathcal{M}_{\triangle,0}$ through $\mathcal{M}_{\triangle,\ell}$. That is, the sets

$$\overline{\mathbf{W}(\mathcal{M}_{\triangle,0})} - \mathbf{W}(\mathcal{M}_{\triangle,0}),$$

for which one can use the algorithm of [2].

This process determines $m_0, \ldots, m_\ell$ as roots of the top ℓ polynomials of zero-dimensional regular chains in

$$m_\ell \succ \cdots \succ m_0 \succ x_\ell \succ \cdots \succ x_0 \succ y_\ell \cdots \succ y_0.$$

Performing a change of variable ordering to $\mathbf{x} \succ \mathbf{m} \succ \mathbf{y}$ expresses $m_0, \ldots, m_{\ell-1}$ as functions of the coordinates of the point p only. We consider this a more desirable output.

§Equations of Tangent Cones

One may prefer to return lines of the tangent cone as equations instead of as encoded by a slope.

Let S be an arbitrary point with coordinates $(X_0, \ldots, X_\ell)$. This point belongs to one of the lines of the tangent cone [corresponding to the branches of the curve defined by $\overline{\mathbf{W}(\mathbf{f}_{\triangle,j})}$] if and only if the vectors

$$\widehat{pq} \begin{pmatrix} 1 \\ m_{\ell-1} \\ \vdots \\ m_0 \end{pmatrix} \quad \text{and} \quad \overline{p\,S} \begin{pmatrix} X_\ell - y_\ell \\ X_{\ell-1} - y_{\ell-1} \\ \vdots \\ X_0 - y_0 \end{pmatrix}$$

are collinear. That is, if and only if

$$\begin{cases} X_\ell = m_\ell(x_\ell - y_\ell) + y_\ell \\ \quad \vdots \\ X_0 = m_0(x_\ell - y_\ell) + y_0 \end{cases}.$$

Consider a regular chain (obtained at the end of the process described in the previous section) expressing the slopes $m_0, \ldots, m_{\ell-1}$ as functions of $y_0, \ldots, y_\ell$ and, let us extend this regular chain with the above equations, so as to obtain a one-dimensional regular chain in the variables

$$X_\ell \succ \cdots \succ X_0 \succ m_{\ell-1} \succ \cdots \succ m_0 \succ y_\ell \cdots \succ y_0.$$

We eliminate the variables $m_0, \ldots, m_{\ell-1}$, with the above equations. Indeed, the only point of a line of the tangent cone (corresponding to the branches of the curve defined by $\overline{\mathbf{W}(\mathbf{f}_{\triangle,j})}$) where the equation $x_\ell = y_\ell$ holds is p itself. Finally, this elimination process consists simply of substituting $\frac{X_i - y_i}{x_\ell - y_\ell}$ for m_i into the equations defining $m_2, \ldots, m_n$.

§Examples

See Algorithm 7 for the realization of the Tangent Cone algorithm and the following examples. We write tangent cones using unions to save vertical space and to separate slope from point.

Example 5.4. Consider calculating the tangent cone of the fish $h = y^2 - x^2(x+1)$ at the origin. The Puiseux expansions of h at $x = 0$ in T are given by

$$\begin{cases} y = -T - \frac{1}{2}T^2 + O(T^3) \\ x = T \end{cases} \quad \text{and} \quad \begin{cases} y = T + \frac{1}{2}T^2 + O(T^3) \\ x = T \end{cases}$$

and substituting these values into $ym - x$ produces

$$\big(-\tfrac{1}{2}T^2 - T\big)m - T \quad \text{and} \quad \big(\tfrac{1}{2}T^2 + T\big)m - T.$$

Call these expressions M_0 and M_1 resp.

To find the value of m at $T = 0$ we find the Puiseux series expansions for M_0 and M_1 at $T = 0$ in U; these are (resp.)

$$\begin{cases} m = -1 + \frac{1}{2}U - \frac{1}{4}U^2 + O(U^3) \\ T = U \end{cases} \quad \text{and} \quad \begin{cases} m = 1 - \frac{1}{2}U + \frac{1}{4}U^2 + O(U^3) \\ T = U \end{cases}.$$

Taking $U \to 0$ in the above produces the (expected) slopes of 1 and -1.

Example 5.5. Consider Figure 5.3, i.e. secants along the the curve $\mathbf{h} = \{x^2 + y^2 + z^2 - 1,\, x^2 - y^2 - z\} \subseteq \mathscr{F}[x,\, y,\, z]$ limiting to a point given by a zero dimensional regular chain $\mathbf{f}_\triangle = \langle x + y,\, 2y^2 - 1,\, z \rangle$.

$$\kappa_{\mathbf{f}_\triangle}(\mathbf{h}) = \begin{cases} m_1 - 1 \\ m_2 \\ m_3 \end{cases} \cup \begin{cases} 2x^2 - 1 \\ 2y^2 - 1 \\ z \end{cases}$$

Figure 5.3: Limiting secants along $\mathbf{V}\big(x^2 + y^2 + z^2 - 1,\, x^2 - y^2 - z\big)$.

or alternatively (using equations of lines instead)

$$\kappa_{\mathbf{f}_\triangle}(\mathbf{h}) = \left\{ z \pm \frac{4x}{\sqrt{2}} + 2,\, y - x \pm \frac{2}{\sqrt{2}} \right\}.$$

Notice the slope for *four* points are encoded here. In particular the points

$$\left\{ \left(\frac{1}{\pm\sqrt{2}}, \frac{1}{\pm\sqrt{2}}, 0 \right), \left(-\frac{1}{\pm\sqrt{2}}, \frac{1}{\mp\sqrt{2}}, 0 \right) \right\}$$

have slope $\langle\langle\, 1,\, 0,\, 0\,\rangle\rangle$.

Example 5.6. Consider Figure 5.4, i.e. secants along the curve $\mathbf{h} = \{x^2 + y^2 + z^2 - 1,\, x^2 - y^2 - z(z-1)\} \subseteq \mathscr{F}[x,\, y,\, z]$ limiting to (0, 0, 1)

$$\kappa_{(0,0,1)}(\mathbf{h}) = \begin{cases} m_1 + m_2 \\ 2m_2^2 - 6m_2 + 3 \\ m_3 \end{cases} \cup \begin{cases} x \\ y \\ z - 1 \end{cases}$$

or alternatively (using equations of lines instead)

$$\kappa_{(0,0,1)}(\mathbf{h}) = \left\{ z - 1,\, y^2 - 3x^2 \right\}.$$

Notice the values of the slopes here are in the algebraic closure of the coefficient ring. In particular, they are

$$\left\{ \left(\tfrac{3}{2} + \sqrt{6},\, \tfrac{3}{2} + \sqrt{6},\, 0 \right), \left(\tfrac{3}{2} - \sqrt{6},\, \tfrac{3}{2} - \sqrt{6},\, 0 \right) \right\}.$$

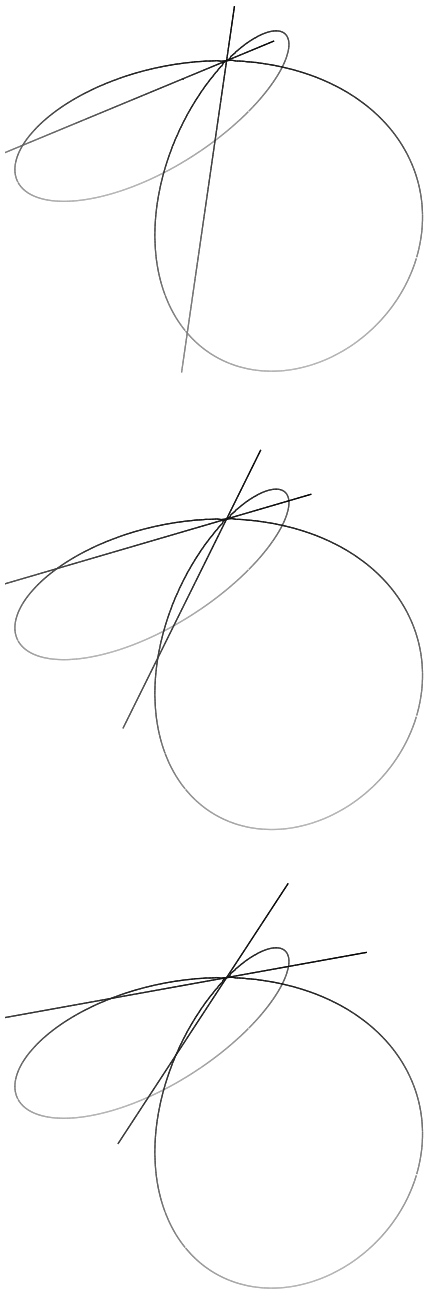


Figure 5.4: Secants along $\mathbf{V}\big(x^2+y^2+z^2-1\big)\cap\mathbf{V}\big(x^2-y^2-z(z-1)\big)$ limiting to (0, 0, 1).

Function $\kappa_{\mathbf{f}_\triangle}(h_0, \ldots, h_{\ell-1})$

Input: Recall $\mathbf{x} = x_0, \ldots, x_\ell$ and $\mathbf{f}_\triangle|_{\mathbf{x}=\mathbf{y}}$ is the renaming of the x-variables to y-variables in $\mathbf{f}_\triangle$.

1. $\mathbf{f}_\triangle \in \mathbb{T}_{\text{reg}}(\mathscr{F}[\mathbf{x}])$ a zero-dimensional regular chain and
2. $\mathbf{h} = \{h_0, \ldots, h_{\ell-1}\} \subseteq \mathscr{F}[\mathbf{x}] : \dim \langle \mathbf{h} \rangle = 1$.

Output: A description (as in Definition 4.1) of the tangent cone at $\mathbf{f}_\triangle$.

$\mathbf{g} \leftarrow \mathbf{f}_\triangle|_{\mathbf{x}=\mathbf{y}} \cup \{h_0, \ldots, h_{\ell-1}\}$;

if $|\text{Regularize}(x_\ell - y_\ell; \mathbf{g})| > 1$ **then**

  return union($\kappa_{\mathbf{f}'_\triangle}(\mathbf{h}) : \mathbf{f}'_\triangle \in \text{Regularize}(x_\ell - y_\ell; \mathbf{g})$);

else if $x_\ell - y_\ell \equiv 0 \bmod \langle \mathbf{g} \rangle$ **then**

  return $\kappa_{\mathbf{f}_\triangle}(h_0, \ldots, h_{\ell-1})$ using a different variable ordering on $\mathbf{x}$;

$M \leftarrow \mathbf{g} \cup \{m_0(x_\ell - y_\ell) - (x_0 - y_0), \ldots, m_\ell(x_\ell - y_\ell) - (x_\ell - y_\ell)\}$;

return $\{\overline{\mathbf{W}(M)} - \mathbf{W}(M)\}$; // Using limits of quasi-components.

Algorithm 7: Tangent cone about a regular chain.

Chapter 6

Extended Fulton's Algorithm

We present sufficient conditions for recursing the calculation of the intersection multipclity in $\mathscr{F}[x_0, \ldots, x_\ell]$ to $\mathscr{F}[x_0, \ldots, x_{\ell-1}]$.

It is important to note the subsequent presentation presumes that pseudo-remainder sequences can be performed on $\mathbf{h}$ modulo $\mathbf{f}_\triangle$ without incident. More precisely, it is assumed there is always an $h_\ell \in \mathbf{h}$ with a regular leading coefficient. Thereby the Algorithms in this chapter work only when they do not fail (though failure is detectable). However, at least practically speaking, these highly degenerate cases very rarely occur naturally.

§6.1 Transversality

In our setting, transversally intersecting curves are those curves that only intersect at a single point. That is to say, two surfaces cannot have transverse intersection if their common component has nonzero dimension.

Definition 6.1 (Transverse)**.** Let $h_0, h_1 \in \mathscr{F}[\mathbf{x}]$. Two varieties $\mathbf{V}(h_0)$ and $\mathbf{V}(h_1)$ in $\mathbb{A}^{\ell+1}\big(\overline{\mathscr{F}}[\mathbf{x}]\big)$ *transversally intersect* at $p \in \mathbf{V}(h_0, h_1)$ when their tangent cones intersect at $\{p\}$ *only* or not at all.

$$\mathbf{V}(h_0) \pitchfork \mathbf{V}(h_1) \overset{\text{Defn.}}{\iff} \kappa_p(h_0) \cap \kappa_p(h_1) \in \{\varnothing, \{p\}\}.$$

(Note at non-singular points the tangent cone is simply the tangent plane.)

Proposition 6.1. Let $h_0, \ldots, h_{\ell-1}, h_\ell \in \mathscr{F}[\mathbf{x}]$ such that $p \in \mathbb{A}^{\ell+1}(\mathscr{F})$ is an isolated point of $\mathbf{V}(\mathbf{h})$ and let $\mathbf{h}^{\downarrow} := \{h_0, \ldots, h_{\ell-1}\}$. Suppose h_ℓ at p is non-singular and transverse to the tangent cone of $\mathbf{V}(\mathbf{h}^{\downarrow})$. Finally, let π be the tangent hyperplane to $\mathbf{V}(h_\ell)$ at p. In this setting, the intersection multiplicities of $\{\mathbf{h}^{\downarrow}, h_\ell\}$ and $\{h_0, \ldots, h_{\ell-1}, \pi\}$ at p coincide:

$$\pi \pitchfork \kappa_p(\mathbf{h}^{\downarrow}) \implies \mathrm{im}_{\ell+1}(p; \mathbf{h}^{\downarrow}, h_\ell) = \mathrm{im}_{\ell+1}(p; \mathbf{h}^{\downarrow}, \pi).$$

Proof. The proposition follows directly from results of [30, Chapter IV]; we reuse the same notation as that reference when feasible. For instance (contrary to our own notation) we let $\mathscr{O}$ be the local ring at p, and $\overline{\mathscr{O}} := \mathscr{O}/\langle \mathbf{h}^{\downarrow} \rangle$.

Since p is an isolated point of $\mathbf{V}(\mathbf{h})$, any irreducible component of $\mathbf{V}(\mathbf{h}^{\downarrow})$ through p must have dimension one. By Lemma 2 in [30, Chapter IV.1.3] it follows $\overline{\mathscr{O}}$ is a one-dimensional local ring.

Let $\mathscr{C}_0, \ldots, \mathscr{C}_r$ be the irreducible components of $\mathbf{V}(\mathbf{h}^{\downarrow})$ passing through p and let $\mathfrak{p}_0, \ldots, \mathfrak{p}_r$ be their respective defining ideals in $\mathscr{O}$. Our transversality assumption ensures h_ℓ and π are both nonzero divisors in $\overline{\mathscr{O}}$ and consequently, since $\overline{\mathscr{O}}$ is a one-dimensional local ring, we use Equation 6 from [30, Chapter IV.1.3] to deduce

$$\mathrm{im}_{\ell+1}(p; \mathbf{h}^{\downarrow}, h_\ell) = \sum_{i=0}^{r} m_i \dim_{\mathrm{vec}}\big(\overline{\mathscr{O}}/\langle \mathfrak{p}_i, h_\ell \rangle\big) \tag{6.1}$$

and

$$\mathrm{im}_{\ell+1}(p; \mathbf{h}^{\downarrow}, \pi) = \sum_{i=0}^{r} m_i \dim_{\mathrm{vec}}\big(\overline{\mathscr{O}}/\langle \mathfrak{p}_i, \pi \rangle\big) \tag{6.2}$$

for some constants $m_1, \ldots, m_r$ that we need not define more precisely.

> In the original reference the above dimensions are written as lengths but [13, Example A.1.1] permits us to use the vector space dimension instead. This holds for all the dimensions written below as well.

Because $\langle \mathbf{h}^{\downarrow} \rangle \subseteq \mathfrak{p}_i$ for all i, we can rewrite (6.1) and (6.2) as (resp.) $\dim_{\text{vec}}(\mathscr{O}/\langle \mathfrak{p}_i, h_\ell \rangle)$ and $\dim_{\text{vec}}(\mathscr{O}/\langle \mathfrak{p}_i, \pi \rangle)$. Hence it is enough to prove that

$$\dim_{\text{vec}}(\mathscr{O}/\langle \mathfrak{p}_i, h_\ell \rangle) = \dim_{\text{vec}}(\mathscr{O}/\langle \mathfrak{p}_i, \pi \rangle)$$

for all $i = 1, \ldots, r$ to conclude. (Note we have replaced $\langle \mathbf{h}^{\downarrow} \rangle$ by a dimension one prime ideal.)

Fix i for the remainder of this proof and write $\mathfrak{p}$ instead of $\mathfrak{p}_i$. This prime ideal defines a curve $\mathscr{C} \subseteq \overline{\mathscr{F}}^{\ell+1}$. Let $\mathscr{C}' \subseteq \overline{\mathscr{F}}^{\ell'+1}$ be a normalization of $\mathscr{C}$ given by $\nu : \mathscr{C}' \to \mathscr{C}$; thus $\mathscr{C}'$ is nonsingular. Also, it follows from [30, Chapter IV.1.3.(9)] that

$$\dim_{\text{vec}}(\mathscr{O}/\langle \mathfrak{p}, h_\ell \rangle) = \sum_{\nu(p')=p} \dim_{\text{vec}}(\mathscr{O}_{\mathscr{C}',p'}/h_\ell^*),$$

when $\mathscr{O}_{\mathscr{C}',p'}$ is the local ring of $\mathscr{C}'$ at p' and h_ℓ^* is the *pull-back* of h_ℓ by ν. A similar expression holds for π.

Now fix p' in the fiber $\nu^{-1}(p)$. We prove

$$\dim_{\text{vec}}(\mathscr{O}_{\mathscr{C}',p'}/h_\ell^*) = \dim_{\text{vec}}(\mathscr{O}_{\mathscr{C}',p'}/\pi^*).$$

Without loss of generality shift to the origin, that is, assume $p = 0 \in \overline{\mathscr{F}}^{\ell+1}$ and $p' = 0 \in \overline{\mathscr{F}}^{\ell'+1}$ and also let t be a *uniformizer* for $\mathscr{C}'$ at p' (remember that $\mathscr{C}'$ is nonsingular). Finally, write $\nu = (\nu_0, \ldots, \nu_\ell)$, with all ν_i in $\overline{\mathscr{F}}[\mathscr{C}']$.

Expanding $\nu = (\nu_0, \ldots, \nu_\ell)$ in power series at the origin permits us view them as in $\overline{\mathscr{F}}[[t]]^{\ell+1}$. With this in mind, and without loss of generality, assume ν_0 has the smallest valuation among $\nu_0, \ldots, \nu_\ell$ (otherwise, do a change of coordinates in $\overline{\mathscr{F}}^{\ell+1}$). Call this valuation r, so that we can write, for all i:

$$\nu_i(t) = \nu_{i,\,r}\, t^r + \nu_{i,\,r+1}\, t^{r+1} + \cdots$$

It follows the component of the $\kappa_{\mathbf{0}}(\mathscr{C})$ corresponding to the image $\nu(\mathscr{C}')$

around p' is the limit of secants having directions

$$\left(\frac{\nu_0(t)}{\nu_0(t)}, \frac{\nu_1(t)}{\nu_0(t)}, \ldots, \frac{\nu_\ell(t)}{\nu_0(t)}\right).$$

This limit is a line with direction

$$\left(1, \frac{\nu_{1,\,r}}{\nu_{0,r}} \ldots, \frac{\nu_{\ell,\,r}}{\nu_{\ell,\,r}}\right),$$

or equivalently $(\nu_{1,\,r}, \ldots, \nu_{n,\,r})$. Because we assumed p is the origin, h_ℓ has a writing

$$h_\ell(x_0,\, \ldots,\, x_\ell) = \pi + \text{higher order terms}$$

with $\pi = h_{\ell,0}\, x_0 + \cdots + h_{\ell,\ell}\, x_\ell$; the transversality assumption implies

$$h_{\ell,0}\, \nu_{0,r} + \cdots + h_{\ell,\ell}\, \nu_{\ell,r} \neq 0.$$

Using the local parameter t, the multiplicities $\dim_{\text{vec}}(\mathscr{O}_{\mathscr{C}',p'}/h_\ell^*)$ and $\dim_{\text{vec}}(\mathscr{O}_{\mathscr{C}',p'}/\pi^*)$ can be rewritten as the respective valuations in t of h_ℓ^* and π^*, that is, of

$$h_\ell(\nu_0(t), \ldots, \nu_\ell(t)) \quad \text{and} \quad \pi(\nu_0(t), \ldots, \nu_\ell(t)).$$

The latter is easy; it reads

$$\begin{aligned}&\pi(\nu_0(t), \ldots, \nu_\ell(t)) = \\ &\quad (h_{\ell,0}\, \nu_{0,r} + \cdots + h_{\ell,\ell}\, \nu_{\ell,r})t^r + (h_{\ell,0}\, \nu_{0,r+1} + \cdots + h_{\ell,\ell}\, \nu_{\ell,r+1})t^{r+1} + \cdots .\end{aligned}$$

Due to the shape of h_ℓ, the former expression is

$$h_\ell(\nu_0(t), \ldots, \nu_\ell(t)) = (h_{\ell,0}\, \nu_{0,r} + \cdots + h_{\ell,\ell}\, \nu_{\ell,r})t^r + \text{higher order terms}.$$

Since we know $h_{\ell,0}\, \nu_{0,r} + \cdots + h_{\ell,\ell}\, \nu_{\ell,r} \neq 0$, both expressions must have the same valuation r, so we are done. □

§6.2 Cylindrification

In practice, the conditions for reduction from ℓ to $\ell-1$ do not always apply. For instance, it is simple to devise a 'degenerate' system which does not satisfy transversality. Take, for instance,

$$\left\{x^2+y+z-1,\, x+y^2+z-1,\, x+y+z^2-1\right\} \subseteq \mathscr{F}[x,\, y,\, z]$$

at any of the coordinates $(1,0,0)$, $(0,1,0)$, or $(0,0,1)$. (See Figure 6.1.)

Notice though, that if one uses $x^2+y+z-1$ to eliminate z in the remaining polynomials (using pseudoremainders), we obtain two bivariate polynomials

$$h_0' = x+y^2-x^2-y \quad \text{and} \quad h_1' = x-y+x^4+2x^2y-2x^2+y^2$$

independent of z. Consequently, the curve given by $\mathbf{V}(h_0',\, h_1')$ does not depend on z as well — in other words, it is a cylinder with base $\mathbf{V}(h_0',\, h_1')$. (See Figure 6.2.)

Cylinders are vertical along (in this case) the x_ℓ axis and so their tangent cones must also be vertical. More precisely if $\mathbf{h}$ is independent of x_ℓ so must $\kappa_p(\mathbf{h})$.

Conversely, the tangent *plane* of $\mathbf{V}(h_1)$ at p with $h_2 = x^2+y+z-1$ necessarily depends on z (by our assumptions). It follows that the tangent plane and the tangent cone of $\mathbf{V}(h_0', h_1')$ at p intersect only at p. That is to say, they automatically have transverse intersection.

More generally, if one polynomial among $\mathbf{h}$ (say h_ℓ) has degree one in x_ℓ and $\operatorname{init}(h_\ell)$ is invertible in the local ring at p then one can replace $h_0,\, \ldots,\, h_{\ell-1}$ by $\operatorname{prem}(\{h_0,\, \ldots,\, h_{\ell-1}\},\, h_\ell;\, x_\ell)$.

Proposition 6.2. Assume $\mathbf{h} \subseteq \mathscr{F}[\mathbf{x}]$ generates a zero-dimensional idea, h_ℓ has nonzero coefficient on x_ℓ, and further that this coefficient is invertible in the local ring $\mathscr{O}_{\mathbb{A}^{\ell+1},\, p}$, then

$$\operatorname{im}_{\ell+1}(p;\, \mathbf{h}) = \operatorname{im}_\ell(p;\, \operatorname{prem}(\{h_0,\, \ldots,\, h_{\ell-1}\},\, h_\ell;\, x_\ell)).$$

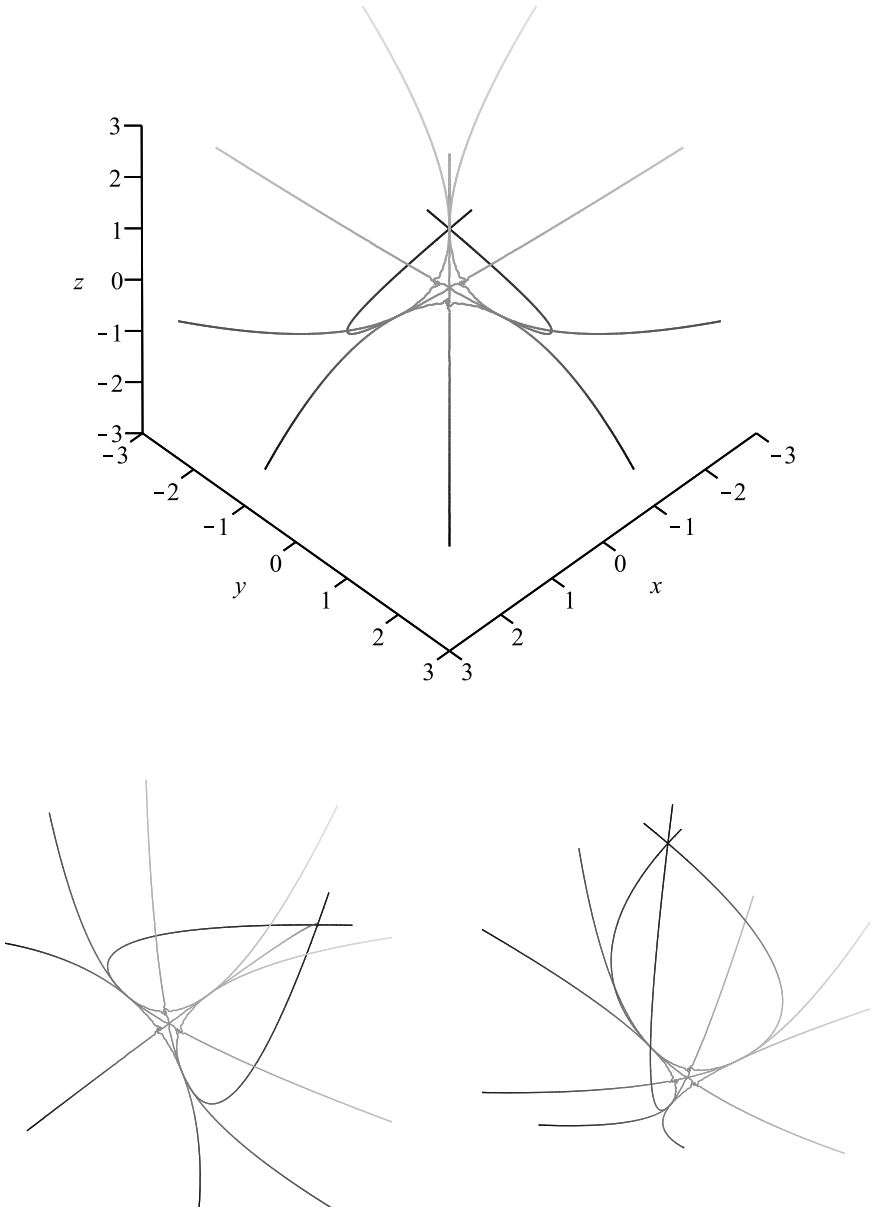


Figure 6.1: Let $h_0, h_1, h_2 = x^2 + y + z - 1, x + y^2 + z - 1, x + y + z^2 - 1$. The above graphs are plots of $\mathbf{V}(h_0, h_1) \cup \mathbf{V}(h_0, h_2) \cup \mathbf{V}(h_1, h_2)$ from various viewpoints.

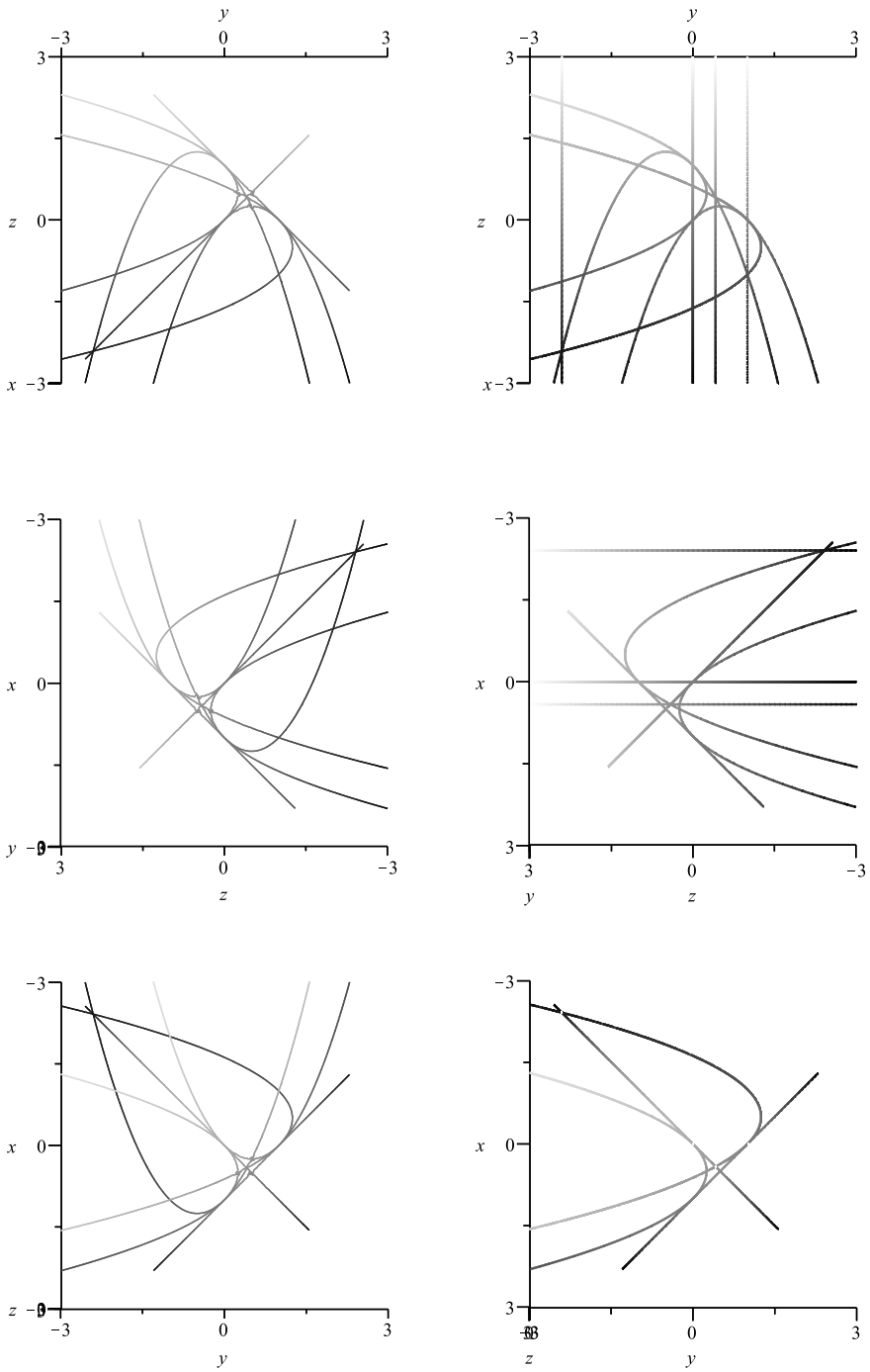


Figure 6.2: Before cylindrification (left). After cylindrification (right).

Assume the pseudo-remainder never fails to find an h_ℓ with regular initial.

Proof. A pseudo-remainder is (obviously) a pseudo-remainder sequence which generally only requires subtraction and products of $h \in \mathbf{h}$ by elements from $\mathscr{F}[\mathbf{x}]$. The properties (n-6) and (n-7) give (resp.) that the intersection multiplicity is invariant to adding $g \in \mathscr{F}[\mathbf{x}]$ to h_ℓ or multiplying $g \in \mathscr{F}[\mathbf{x}]$ by h_ℓ. Thereby we have the pseudo-remainder must leave the intersection multiplicity invariant. □

If no h among $\mathbf{h}$ has degree one in x_ℓ, but (say) h_ℓ has a degree two term with an initial that is invertible in the local ring, then similarly one can replace $\mathbf{h}^{\downarrow}$ by $\mathrm{prem}(\mathbf{h}^{\downarrow}, h_\ell; x_\ell)$ while leaving the intersection multiplicity at p invariant. At this stage, either the degree one case applies or every h in $\mathrm{prem}(\mathbf{h}^{\downarrow}, h_\ell; x_\ell)$ has degree zero in x_ℓ (i.e. it is a cylinder).

This process can be iterated to 'solve' the case where the least degree in x_ℓ among $\mathbf{h}$ is (say) $d \in \mathbb{N}$. Repeating pseudoremainders by some h_ℓ at each stage will force the degree in x_ℓ to strictly descend to one (in no more than d steps). Naturally, we call this process *cylindrification* and it is given by Algorithm 9. We note when cylindrification succeeds that conditions for Proposition 6.2 are satisfied.

Proposition 6.3. Algorithm 9 (cylindrification) is correct.

Proof. The invariance of the intersection multiplicity (and subsequently correctness) is ensured by Proposition 6.2. If $h_0, \ldots, h_{\ell-1}$ are already in $\mathscr{F}[x_0, \ldots, x_{\ell-1}]$ then line 5 returns and we are done. Else line 6 is called and the pseudo-remainder ensures every $\deg_{x_\ell}(h_0), \ldots, \deg_{x_\ell}(h_{\ell-1})$ has degree in x_ℓ less than h_ℓ. Thus we must have termination because line 2 forms a strictly descending sequence until $\deg_{x_\ell}(h_\ell) = 0$ (the first case). □

§6.3 Algorithms

Here we provide the Algorithm (along with arguments for their correctness) required to calculate the intersection multiplicity of $\ell + 1$ hypersurfaces

Function Transversalize$^*(\mathbf{f}_\triangle;\ \mathbf{h})$

Input:

1. $\mathbf{f}_\triangle \in \mathbb{T}_{\text{reg}}(\mathscr{F}[\mathbf{x}])$ a zero dimensional regular chain, and
2. $\mathbf{h} = \{h_0, \ldots, h_\ell\} \subseteq \mathscr{F}[\mathbf{x}] : \dim \langle \mathbf{h} \rangle = 0$.

Output: A list of

$$(B,\ \mathbf{f}'_\triangle,\ \mathbf{h}', h'_\ell) \in \{0,\ 1\} \times \mathbb{T}_{\text{reg}}(\mathscr{F}[\mathbf{x}]) \times \mathscr{F}[\mathbf{x}]^\ell \times \mathscr{F}[\mathbf{x}]$$

such that $B \implies \pi_{\mathbf{f}'_\triangle}(h'_\ell) \Cap \kappa_{\mathbf{f}'_\triangle}(\mathbf{h})$ and $\mathbf{h}' \cup \{h'_\ell\} = \mathbf{h}$; where the $\mathbf{f}'_\triangle$s form a triangular decomposition of $\mathbf{h}$ at $\mathbf{f}_\triangle$.

Choose $h \in \mathbf{h}$;

$\mathbf{h}^\downarrow \leftarrow \mathbf{h} - \{h\}$;

$\boldsymbol{\kappa} \leftarrow \kappa_{\mathbf{f}_\triangle}(\mathbf{h}^\downarrow)$;

$t \leftarrow \varnothing$;

for $(\mathbf{f}'_\triangle,\ \kappa) \in \boldsymbol{\kappa}$ **do**

Check if the normal of the tangent plane of h is perpendicular to the slope of $\mathbf{h}^\downarrow$ at $\mathbf{f}_\triangle$ via dot product.

$s \leftarrow \nabla(h) \bmod \langle \mathbf{f}'_\triangle \rangle \cdot \langle\langle\, m_0, \ldots, m_{\ell+1} \,\rangle\rangle$;

if $\left|\text{Regularize}\big(\langle\, \mathbf{f}'_\triangle,\ \boldsymbol{\kappa} \,\rangle;\ s\big)\right| = 1$ **then**

if $s \in \mathbb{U}\big\langle \mathbf{f}'_\triangle,\ \kappa \big\rangle$ **then**

$t \leftarrow t \cup \big\{(1,\ \mathbf{f}'_\triangle,\ \mathbf{h}^\downarrow,\ h)\big\}$;

else

$t \leftarrow t \cup \big\{(0,\ \mathbf{f}'_\triangle,\ \mathbf{h}^\downarrow,\ h)\big\}$;

else

return union(Transversalize$^*\big(\mathbf{f}''_\triangle;\ \mathbf{h}\big) : \mathbf{f}''_\triangle \in \text{Regularize}\big(\langle\, \mathbf{f}'_\triangle,\ \boldsymbol{\kappa} \,\rangle;\ s\big)$);

return t;

Algorithm 8: Try to find transversal intersections along the various branches of $\mathbf{h}$ towards $\mathbf{f}'_\triangle$.

from $\mathscr{F}[\mathbf{x}]$ at a point p encoded by a zero dimensional regular chain $\mathbf{f}_{\triangle} \in \mathbb{T}_{\mathrm{reg}}(\mathscr{F}[\mathbf{x}])$.

Proposition 6.4. Algorithm 10 (multivariate intersection multiplicity) is correct and terminates.

Proof. Lines 6–8 and Line 10 are simple applications of (resp.) Proposition 6.1 and Proposition 6.2.

Notice in either case the computation is reduced to that of one in a polynomial ring of one less variable. Accordingly the process must eventually call Algorithm 6 (the algorithm for the intersection multiplicity in two variables) which terminates. □

1 **Function** Cylindrify($\mathbf{f}_\triangle$; $\mathbf{h}$)

Input: Let $x_\ell \succ \cdots \succ x_0$.

1. $\mathbf{f}_\triangle \in \mathbb{T}_{\mathrm{reg}}(\mathscr{F}[x_0, \ldots, x_\ell])$ a zero dimensional regular chain, and
2. $\mathbf{h} = \{h_0, \ldots, h_\ell\} \subseteq \mathscr{F}[x_0, \ldots, x_\ell]$.

Output: $\{h'_0, \ldots, h'_{\ell-1}\} \subseteq \mathscr{F}[x_0, \ldots, x_{\ell-1}]$ such that
$\mathrm{im}_{\ell-1}(\mathbf{f}_\triangle; \{h'_0, \ldots, h'_{\ell-1}\}) = \mathrm{im}_\ell(\mathbf{f}_\triangle; \mathbf{h})$.

2 Suppose $\deg_{x_\ell}(h_\ell) = \min(\deg(h) : h \in \mathbf{h})$;

3 Assume $\mathrm{init}(h_\ell) \in \mathbb{U}\langle \mathbf{f}_\triangle \rangle$;

4 **if** $\{h_0, \ldots, h_{\ell-1}\} \subseteq \mathscr{F}[x_0, \ldots, x_{\ell-1}]$ **then**

5 **return** $\{h_0, \ldots, h_{\ell-1}\}$;

6 **return** $\mathrm{prem}(\{h_0, \ldots, h_{\ell-1}\}, h_\ell; x_\ell)$;

Algorithm 9: Cylindrification at $\mathbf{f}_\triangle$.

Function $\mathrm{im}^*_{\ell+1}(\,\mathbf{f}_\triangle;\,\mathbf{h})$

Input:

1. $\mathbf{f}_\triangle \in \mathbb{T}_{\mathrm{reg}}(\mathscr{F}[\mathbf{x}])$ a zero dimensional regular chain, and
2. $\mathbf{h} = \{h_0,\,\ldots,\,h_\ell\} \subseteq \mathscr{F}[\mathbf{x}] : \dim\langle\mathbf{h}\rangle = 0.$

Output: $\mathbf{D}(\mathbf{f}_\triangle;\,\mathbf{h}) \subseteq \mathbb{N} \times \mathbb{T}_{\mathrm{reg}}(\mathscr{R}[\mathbf{x}])$.

```
if ℓ + 1 = 2 then
    return im_2(f_△; h);
t ← ∅;
for (B, f'_△, h', h'_ℓ) ∈ Transversalize*(f_△; h) do
    if B then
        π ← π_{f'_△}(h'_ℓ);
        t ← t ∪ im*_ℓ( f'_△; prem(h', π; x_ℓ) );
    else
        t ← t ∪ im*_ℓ( f_△; Cylindrify(f_△; h) );
return t;
```

Algorithm 10: $\ell + 1$-variate intersection multiplicity about a zero dimensional regular chain $\mathbf{f}_\triangle$.

Chapter 7

Experiments

We present experimental results for the Maple implementation of the algorithms outlined in this work.

The relevant hardware details are as follows.

```
os          : Ubuntu 12.04.4 LTS
processors  : 2
vendor_id   : GenuineIntel
model name  : Intel(R) Core(TM)2 Duo CPU     E8500  @ 3.16GHz
cpu MHz     : 3163.000
cache size  : 6144 KB
ram         : 2 x 4GB DDR2
```

All timings are given in seconds and the coefficient field has characteristic 101, 962 592 769, or 0 as indicated. It should be noted that 962 592 769 is a so-called FFT-prime which allows some sub-packages to run faster by exploiting techniques for FFT based calculations.[20]

The experimentation is done in three parts:

First we study systems taken from [12] (a paper on intersection multiplicity) and from [5] (a test suite for benchmarking homotopy solvers). Next we investigate random homogeneous bivariate polynomials from $\mathscr{R}[x, y]$ of the form

$$c_0 x^{a_0} y^{b_0} + c_1 x^{a_1} y^{b_1} + c_2 x^{a_2} y^{b_2} + c_3 x^{a_3} y^{b_3} + c_4 x^{a_4} y^{b_4}$$

where $a_0 + b_0, \ldots, a_4 + b_4 = d$ for varying $d \in \mathbb{N}^{>1}$ and $c_0, \ldots, c_4 \in \mathscr{R}$ for both the optimized (testing for trivial intersection multiplicity using the Jacobian) and unoptimized versions.

Note the density, or number of terms relative to the degree, of the starting polynomials are irrelevant as they inevitably become dense during the algorithm's operation.

System	$\lvert\mathbf{x}\rvert$	$\deg(\mathbf{h})$	$\deg_x(\mathbf{h}) : x \in \mathbf{x}$
Ojika2	3	(2, 2, 2)	(2, 1, 1)
			(1, 2, 1)
			(1, 1, 2)
Ojika3	3	(1, 2, 2)	(1, 1, 1)
			(1, 2, 1)
			(1, 1, 2)
Arnborg-Lazard-rev	3	(4, 5, 6)	(2, 2, 2)
			(2, 2, 2)
			(2, 2, 2)
Barry	3	(5, 4, 1)	(5, 0, 1)
			(5, 4, 1)
			(0, 0, 1)
GonzalezGonzalez	3	(3, 3, 2)	(3, 2, 2)
			(5, 4, 1)
			(0, 0, 1)
Eco5	5	(3, 3, 3, 2, 1)	(1, 1, 1, 0, 1)
			(1, 1, 0, 0, 1)
			(1, 1, 1, 0, 1)
			(1, 1, 1, 1, 1)
			(1, 1, 1, 1, 0)
Cyclohexane	3	(4, 4, 4)	(0, 2, 2)
			(2, 0, 2)
			(2, 2, 0)
ℓ-3	4	(3, 3, 3, 3)	(3, 1, 1, 1)
			(3, 1, 1, 1)
			(1, 3, 1, 1)
			(1, 1, 3, 1)
			(1, 1, 1, 3)

Table 7.1: Systems taken from [12] and [5].

§7.1 Examples from literature

§Characteristic 101

$\mathbf{h}$ = ojika2 $p = 101$.

$\mathrm{im}(\mathbf{f}_\triangle; \mathbf{h})$	$\lvert\mathbf{f}_\triangle\rvert$	Bézout Weight	Cones	Total	Optimized
1	2	2	0.368	0.436	0.020
2	1	2	0.780	1.280	1.244
2	1	2	0.728	1.140	1.144
2	1	2	0.764	1.130	1.128
		8	2.640	3.984	3.536

$\mathbf{h}$ = ojika3 $p = 101$.

$\mathrm{im}(\mathbf{f}_\triangle; \mathbf{h})$	$\lvert\mathbf{f}_\triangle\rvert$	Bézout Weight	Cones	Total	Optimized
1	1	1	0.204	0.236	0.012
1	1	1	0.232	0.268	0.012
1	1	1	0.236	0.268	0.008
1	1	1	0.192	0.224	0.012
		4	0.864	0.996	0.044

$\mathbf{h}$ = Arnborg-Lazard-rev $p = 101$.

$\mathrm{im}(\mathbf{f}_\triangle; \mathbf{h})$	$\lvert\mathbf{f}_\triangle\rvert$	Bézout Weight	Cones	Total	Optimized
1	6	6	10.505	10.900	0.096
1	6	6	8.784	9.130	0.172
1	3	3	6.117	6.360	0.136
1	3	3	6.024	6.260	0.132
1	1	1	2.448	2.560	0.088
1	1	1	2.448	2.610	0.120
		20	36.326	37.814	0.744

$\mathbf{h}$ = Barry $p = 101$.

$\mathrm{im}(\mathbf{f}_\triangle; \mathbf{h})$	$\lvert\mathbf{f}_\triangle\rvert$	Bézout Weight	Cones	Total	Optimized
1	20	20	9.052	9.290	0.040
		20	9.052	9.292	0.040

$\mathbf{h}$ = GonzalezGonzalez $p = 101$.

$\text{im}(\mathbf{f}_\triangle; \mathbf{h})$	$\lvert\mathbf{f}_\triangle\rvert$	Bézout Weight	Cones	Total	Optimized
1	3	3	1.972	2.140	0.024
1	1	1	0.828	0.868	0.012
		4	2.800	3.004	0.036

$\mathbf{h}$ = eco5 $p = 101$.

$\text{im}(\mathbf{f}_\triangle; \mathbf{h})$	$\lvert\mathbf{f}_\triangle\rvert$	Bézout Weight	Cones	Total	Optimized
1	2	2	3.072	3.610	0.092
1	2	2	3.008	3.600	0.096
1	1	1	1.692	1.930	0.032
1	1	1	1.712	1.950	0.040
1	1	1	1.680	1.910	0.036
1	1	1	1.712	2.000	0.040
		8	12.876	15.001	0.336

$\mathbf{h}$ = Cyclohexane $p = 101$.

$\text{im}(\mathbf{f}_\triangle; \mathbf{h})$	$\lvert\mathbf{f}_\triangle\rvert$	Bézout Weight	Cones	Total	Optimized
1	2	2	4.837	5.200	0.036
1	2	2	3.516	3.690	0.048
1	2	2	4.896	5.190	0.080
1	2	2	4.500	4.780	0.040
1	2	2	8.225	8.580	0.040
1	2	2	8.097	8.560	0.048
		16	34.071	36.015	0.292

$\mathbf{h} = \ell\text{-}3 \;\; p = 101.$

$\mathrm{im}(\mathbf{f}_\triangle; \mathbf{h})$	$\lvert\mathbf{f}_\triangle\rvert$	Bézout Weight	Cones	Total	Optimized
1	6	6	7.684	7.972	0.064
1	6	6	2.220	2.432	0.072
1	6	6	2.268	2.472	0.068
1	4	4	7.361	7.585	0.064
1	4	4	2.352	2.772	0.140
1	4	4	7.300	7.652	0.060
1	4	4	7.477	7.773	0.056
1	2	2	2.352	2.508	0.052
1	2	2	2.344	2.504	0.048
1	2	2	2.276	2.536	0.056
1	2	2	1.353	1.509	0.056
1	4	4	2.516	2.796	0.068
1	2	2	1.328	1.556	0.056
1	2	2	1.436	1.624	0.048
1	2	2	0.848	1.004	0.048
1	1	1	1.384	1.460	0.132
1	1	1	1.380	1.456	0.064
1	1	1	1.372	1.452	0.048
1	1	1	2.924	3.084	0.044
1	1	1	2.789	2.861	0.040
1	1	1	5.148	5.276	0.040
1	1	1	2.040	2.140	0.040
1	1	1	2.756	2.840	0.048
1	1	1	3.556	3.636	0.040
1	1	1	1.361	1.437	0.044
1	1	1	2.768	2.864	0.044
1	1	1	2.912	3.004	0.048
1	1	1	0.768	0.844	0.048
1	1	1	0.776	0.852	0.120
1	1	1	0.784	0.860	0.044
1	1	1	3.168	3.300	0.064
1	1	1	0.748	0.820	0.040
1	1	1	4.285	4.465	0.048
1	1	1	0.772	0.848	0.040
1	1	1	0.756	0.912	0.044

1	1	1	0.772	0.844	0.040
1	1	1	2.100	2.196	0.044
1	1	1	0.748	0.816	0.060
1	1	1	2.976	3.088	0.044
1	1	1	0.532	0.608	0.040
1	1	1	0.544	0.620	0.132
1	1	1	0.456	0.612	0.044
1	1	1	0.728	0.808	0.040
1	1	1	0.440	0.508	0.060
	81	81	102.858	109.206	2.540

§Characteristic 962 592 769

$\mathbf{h} =$ ojika2 $p = 962\,592\,769$.

$\mathrm{im}(\mathbf{f}_\triangle; \mathbf{h})$	$\lvert\mathbf{f}_\triangle\rvert$	Bézout Weight	Cones	Total	Optimized
2	1	2	0.796	1.460	1.360
2	1	2	0.408	0.636	1.300
1	1	1	0.208	0.264	0.024
1	1	1	0.212	0.348	0.028
2	1	2	0.792	1.180	1.264
		8	2.416	3.888	3.976

$\mathbf{h} =$ ojika3 $p = 962\,592\,769$.

$\mathrm{im}(\mathbf{f}_\triangle; \mathbf{h})$	$\lvert\mathbf{f}_\triangle\rvert$	Bézout Weight	Cones	Total	Optimized
1	1	1	0.208	0.268	0.028
1	1	1	0.200	0.260	0.024
1	1	1	0.280	0.340	0.024
1	1	1	0.200	0.252	0.024
		4	0.888	1.120	0.100

$\mathbf{h}$ = Arnborg-Lazard-rev $p = 962\,592\,769$.

$\mathrm{im}(\mathbf{f}_\triangle; \mathbf{h})$	$\lvert\mathbf{f}_\triangle\rvert$	Bézout Weight	Cones	Total	Optimized
1	6	6	25.310	26.000	0.296
1	6	6	27.302	28.100	0.372
1	6	6	16.861	17.700	0.332
1	2	2	7.876	8.480	0.308
		20	77.349	80.321	1.308

$\mathbf{h}$ = Barry $p = 962\,592\,769$.

$\mathrm{im}(\mathbf{f}_\triangle; \mathbf{h})$	$\lvert\mathbf{f}_\triangle\rvert$	Bézout Weight	Cones	Total	Optimized
1	2	2	0.192	0.380	0.048
1	2	2	0.188	0.296	0.052
1	2	2	0.188	0.292	0.132
1	2	2	0.188	0.288	0.048
1	2	2	0.188	0.284	0.044
1	2	2	0.188	0.368	0.040
1	2	2	0.188	0.277	0.036
1	2	2	0.272	0.360	0.040
1	1	1	0.152	0.228	0.040
1	1	1	0.152	0.224	0.040
1	1	1	0.148	0.304	0.032
1	1	1	0.148	0.212	0.032
		20	2.192	3.513	0.584

$\mathbf{h}$ = GonzalezGonzalez $p = 962\,592\,769$.

$\mathrm{im}(\mathbf{f}_\triangle; \mathbf{h})$	$\lvert\mathbf{f}_\triangle\rvert$	Bézout Weight	Cones	Total	Optimized
1	4	4	2.288	2.630	0.048
		4	2.288	2.628	0.048

$\mathbf{h} = \text{eco5} \quad p = 962\,592\,769.$

$\text{im}(\mathbf{f}_\triangle; \mathbf{h})$	$\lvert\mathbf{f}_\triangle\rvert$	Bézout Weight	Cones	Total	Optimized
1	3	3	5.728	8.730	0.928
1	3	3	5.929	8.910	0.956
1	1	1	1.464	2.710	0.352
1	1	1	1.996	2.970	0.352
		8	15.117	23.321	2.588

$\mathbf{h} = \text{Cyclohexane} \quad p = 962\,592\,769.$

$\text{im}(\mathbf{f}_\triangle; \mathbf{h})$	$\lvert\mathbf{f}_\triangle\rvert$	Bézout Weight	Cones	Total	Optimized
1	2	2	6.937	7.590	0.088
1	2	2	8.248	8.940	0.200
1	2	2			
1	2	2	11.248	12.300	0.100
1	1	1	2.056	2.300	0.100
1	1	1	2.073	2.370	0.152
1	1	1	2.052	2.250	0.176
1	1	1	1.996	2.410	0.080
1	1	1	2.504	2.700	0.104
1	1	1	4.480	4.700	0.068
1	1	1	4.765	4.920	0.184
1	1	1	2.476	2.620	0.180
		16	48.835	53.092	1.432

$\mathbf{h} = \ell\text{-}3 \quad p = 962\,592\,769.$

$\text{im}(\mathbf{f}_\triangle; \mathbf{h})$	$\lvert\mathbf{f}_\triangle\rvert$	Bézout Weight	Cones	Total	Optimized
1	4	4	0.000	0.372	0.316
1	4	4	0.000	0.212	0.260
1	4	4	0.000	0.364	0.248
1	4	4	0.000	0.312	0.340
1	3	3	0.000	0.280	0.204
1	2	2	0.000	0.176	0.328
1	2	2			
1	2	2	0.000	0.228	0.344
1	2	2	0.000	0.268	0.196
1	2	2	0.000	0.160	0.276

1	2	2	0.000	0.252	0.328
1	1	1	0.000	0.164	0.160
1	1	1	0.000	0.224	0.172
1	1	1	0.000	0.356	0.148
1	1	1	0.000	0.164	0.132
1	1	1	0.000	0.224	0.132
1	1	1	0.000	0.176	0.216
1	1	1	0.000	0.260	0.136
1	1	1	0.000	0.240	0.132
1	1	1	0.000	0.176	0.208
1	1	1	0.000	0.132	0.196
1	1	1	0.000	0.132	0.216
1	1	1	0.000	0.168	0.128
1	1	1	0.000	0.312	0.124
1	1	1	0.000	0.184	0.308
1	1	1	0.000	0.185	0.232
1	1	1	0.000	0.148	0.148
1	1	1	0.000	0.136	0.220
1	1	1	0.000	0.160	0.344
1	1	1	0.000	0.196	0.136
1	1	1	0.000	0.224	0.188
1	1	1	0.000	0.340	0.264
1	1	1	0.000	0.152	0.272
1	1	1	0.000	0.184	0.148
1	1	1	0.000	0.232	0.132
1	1	1	0.000	0.224	0.220
1	1	1	0.000	0.148	0.304
1	1	1	0.000	0.268	0.148
1	1	1	0.000	0.236	0.200
1	1	1	0.000	0.152	0.264
1	1	1	0.000	0.176	0.428
1	1	1	0.000	0.148	0.240
1	1	1	0.000	0.160	0.124
1	1	1	0.000	0.160	0.156
1	1	1	0.000	0.132	0.144
1	1	1	0.000	0.252	0.184
1	1	1	0.000	0.136	0.208

1	1	1	0.000	0.132	0.136
1	1	1	0.000	0.188	0.224
1	1	1	0.000	0.260	0.152
1	1	1	0.000	0.220	0.172
1	1	1	0.000	0.184	0.208
1	1	1	0.000	0.160	0.148
1	1	1	0.000	0.252	0.132
1	1	1	0.000	0.140	0.128
1	1	1	0.000	0.212	0.164
1	1	1	0.000	0.132	0.132
1	1	1	0.000	0.228	0.132
1	1	1	0.000	0.148	0.136
1	1	1	0.000	0.212	0.212
1	1	1	0.000	0.148	0.204
		81	0.000	12.301	12.232

§Characteristic 0

$\mathbf{h} = \text{ojika2} \quad p = 0.$

$\text{im}(\mathbf{f}_\triangle; \mathbf{h})$	$\lvert\mathbf{f}_\triangle\rvert$	Bézout Weight	Cones	Total	Optimized
1	2	2	0.192	0.228	0.012
2	1	2	0.564	0.816	0.800
2	1	2	0.560	0.748	0.744
2	1	2	0.560	0.740	0.736
		8	1.876	2.532	2.292

$\mathbf{h} = \text{ojika3} \quad p = 0.$

$\text{im}(\mathbf{f}_\triangle; \mathbf{h})$	$\lvert\mathbf{f}_\triangle\rvert$	Bézout Weight	Cones	Total	Optimized
1	1	1	0.136	0.156	0.008
1	1	1	0.136	0.152	0.004
1	1	1	0.132	0.152	0.008
1	1	1	0.132	0.236	0.008
		4	0.536	0.696	0.028

$\mathbf{h}$ = Arnborg-Lazard-rev $p = 0$.

$\mathrm{im}(\mathbf{f}_\triangle; \mathbf{h})$	$\lvert\mathbf{f}_\triangle\rvert$	Bézout Weight	Cones	Total	Optimized
1	6	6	29.274	29.400	0.016
1	2	2	1.772	1.820	0.016
		20	8203.865	8204.165	0.060

$\mathbf{h}$ = Barry $p = 0$.

$\mathrm{im}(\mathbf{f}_\triangle; \mathbf{h})$	$\lvert\mathbf{f}_\triangle\rvert$	Bézout Weight	Cones	Total	Optimized
1	20	20	9.052	9.290	0.040
		20	9.052	9.292	0.040

$\mathbf{h}$ = GonzalezGonzalez $p = 0$.

$\mathrm{im}(\mathbf{f}_\triangle; \mathbf{h})$	$\lvert\mathbf{f}_\triangle\rvert$	Bézout Weight	Cones	Total	Optimized
1	4	4	2.288	2.630	0.048
		4	2.288	2.628	0.048

$\mathbf{h}$ = eco5 $p = 0$.

$\mathrm{im}(\mathbf{f}_\triangle; \mathbf{h})$	$\lvert\mathbf{f}_\triangle\rvert$	Bézout Weight	Cones	Total	Optimized
1	3	3	5.728	8.730	0.928
1	3	3	5.929	8.910	0.956
1	1	1	1.464	2.710	0.352
1	1	1	1.996	2.970	0.352
		8	15.117	23.321	2.588

$\mathbf{h}$ = Cyclohexane $p = 0$.

$\mathrm{im}(\mathbf{f}_\triangle; \mathbf{h})$	$\lvert\mathbf{f}_\triangle\rvert$	Bézout Weight	Cones	Total	Optimized
1	2	2	6.937	7.590	0.088
1	2	2	8.248	8.940	0.200
1	2	2			
1	2	2	11.248	12.300	0.100
1	1	1	2.056	2.300	0.100
1	1	1	2.073	2.370	0.152
1	1	1	2.052	2.250	0.176
1	1	1	1.996	2.410	0.080
1	1	1	2.504	2.700	0.104
1	1	1	4.480	4.700	0.068
1	1	1	4.765	4.920	0.184
1	1	1	2.476	2.620	0.180
		16	48.835	53.092	1.432

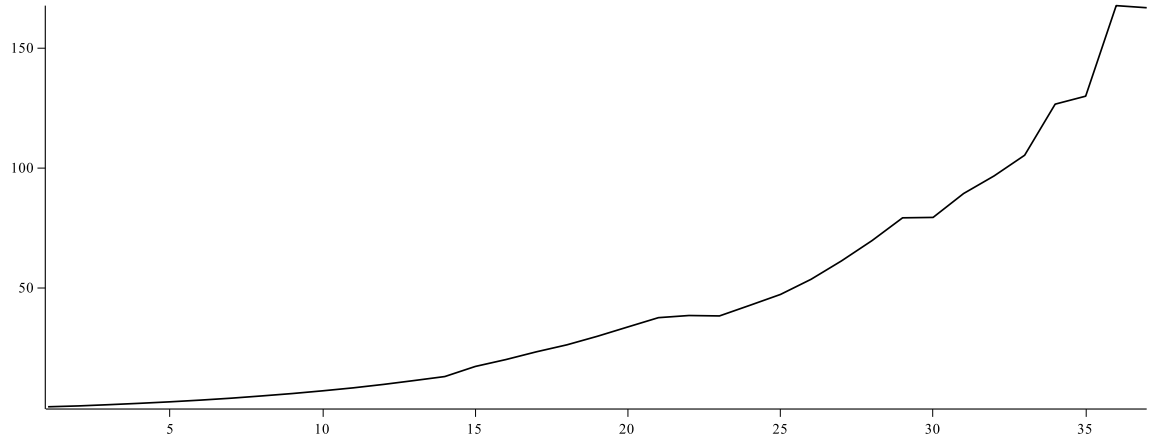
$\mathbf{h} = \ell$-3 $p = 0$.

$\mathrm{im}(\mathbf{f}_\triangle; \mathbf{h})$	$\lvert\mathbf{f}_\triangle\rvert$	Bézout Weight	Cones	Total	Optimized
1	6	6	5.972	6.130	0.020
1	6	6	2.548	2.760	0.020
1	6	6	2.596	2.720	0.020
1	5	5	5.149	5.290	0.020
1	5	5	2.356	2.470	0.020
1	5	5	2.384	2.490	0.100
1	5	5	1.764	1.890	0.016
1	8	8	24.398	24.600	0.024
1	4	4	4.396	4.530	0.020
1	3	3	2.168	2.270	0.016
1	4	4	5.888	6.020	0.020
1	4	4	2.849	3.010	0.020
1	4	4	0.628	0.776	0.020
1	1	1	3.236	3.300	0.008
1	1	1	3.000	3.080	0.012
1	1	1	6.605	6.840	0.008
1	1	1	5.064	5.180	0.012
1	1	1	3.012	3.090	0.012
1	1	1	3.936	4.020	0.012

1	1	1	1.480	1.550	0.012
1	1	1	3.077	3.140	0.008
1	1	1	3.152	3.220	0.008
1	1	1	4.288	4.420	0.008
1	1	1	0.772	0.832	0.008
1	1	1	5.765	5.870	0.012
1	1	1	3.076	3.160	0.012
1	1	1	0.872	0.924	0.008
1	1	1	4.132	4.230	0.008
1	1	1	0.616	0.668	0.008
		81	115.179	118.491	0.492

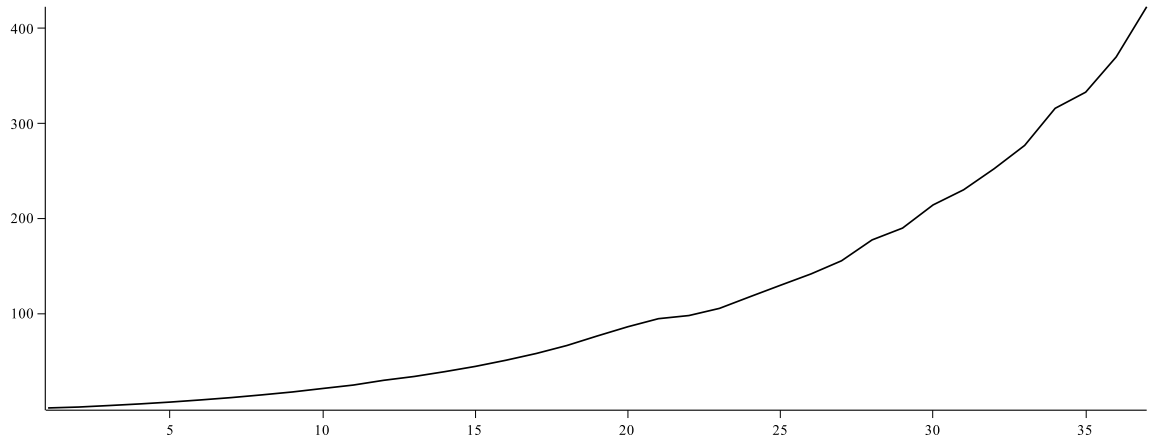
§7.2 Random Case Testing (Bivariate)

d	Max Time	Min Time	Average
2	0.228	0.144	0.194
3	0.680	0.276	0.556
4	1.272	0.608	1.078
5	1.820	1.189	1.644
6	2.544	1.773	2.270
7	3.341	2.529	2.986
8	4.188	2.617	3.787
9	5.229	3.884	4.727
10	6.221	4.617	5.723
11	7.545	5.944	6.864
12	9.045	6.817	8.104
13	11.757	7.812	9.551
14	12.313	9.677	11.161
15	18.837	10.413	12.822
16	22.214	14.564	17.040
17	24.873	15.697	19.910
18	36.078	18.013	23.149
19	29.410	18.302	26.064
20	40.286	20.85	29.641
21	64.965	24.322	33.543
22	55.515	26.59	37.414
23	51.627	29.018	38.311
24	76.033	29.610	38.135
25	61.647	31.618	42.584
26	57.024	34.670	47.113
27	151.378	38.418	53.425
28	244.291	42.279	61.130
29	206.889	45.330	69.598
30	320.312	51.640	79.104
31	227.870	54.475	79.275
32	146.541	66.548	89.253
33	187.979	64.240	96.613
34	177.071	65.748	105.240
35	835.312	73.605	126.576
36	214.282	86.766	129.909
37	1734.821	101.394	167.719
38	471.741	101.519	166.836



Let h_0 and h_1 be two homogeneous polynomials of degree d (horizontal access). Plotted above is the average time in seconds (vertical access) over 100 trials required to calculate a description of $\{h_0, h_1\}$ in $\mathbb{Z}_{101}[x, y]$.

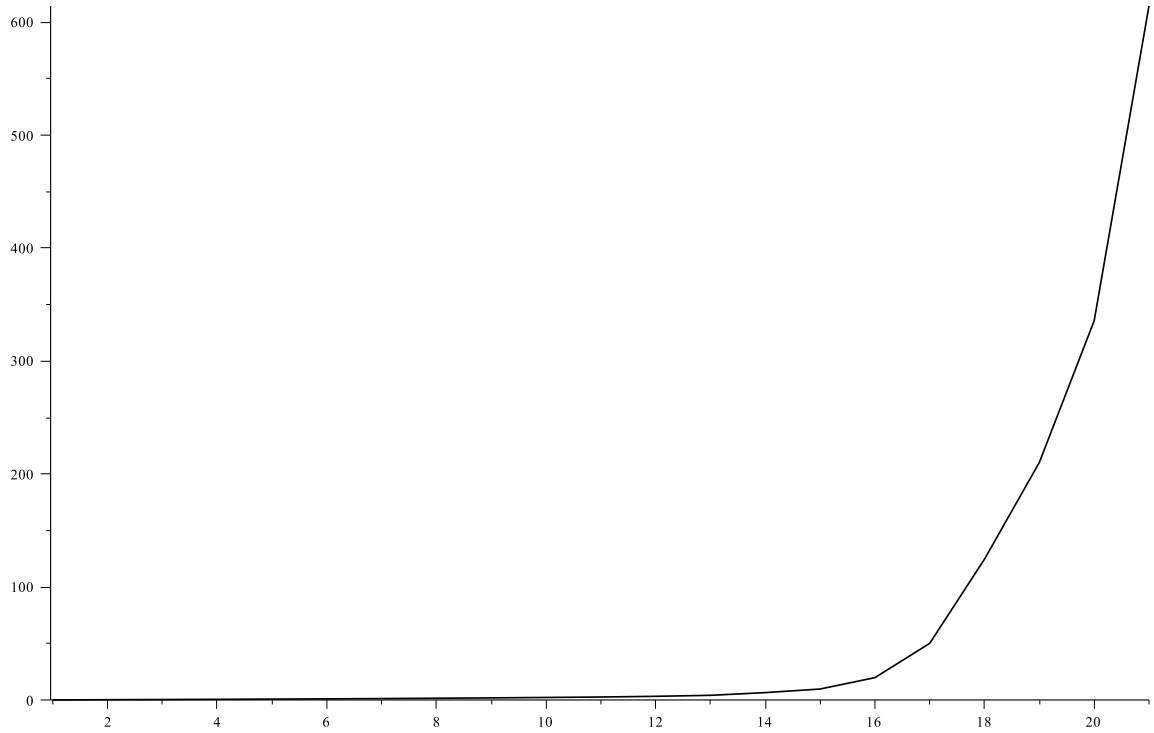
d	Max Time	Min Time	Average
2	0.260	0.160	0.222
3	1.712	0.404	1.174
4	3.545	2.048	2.771
5	5.416	3.376	4.456
6	7.457	5.113	6.412
7	10.216	6.768	8.684
8	12.833	8.825	11.130
9	15.901	9.021	13.988
10	19.145	14.009	17.049
11	24.062	15.457	20.742
12	28.190	19.201	24.342
13	33.414	22.477	29.372
14	38.819	24.730	33.396
15	45.106	28.570	38.475
16	55.375	33.738	44.004
17	58.612	33.298	50.474
18	65.812	41.927	57.648
19	81.237	51.727	66.026
20	89.282	53.596	76.124
21	100.21	64.956	85.827
22	109.747	68.308	94.293
23	66.256	115.347	97.612
24	71.076	124.512	105.164
25	74.785	162.347	117.440
26	93.97	159.774	129.5348
27	91.518	177.483	141.4713
28	100.778	195.884	155.323
29	119.419	217.074	177.308
30	122.8	245.335	189.783
31	127.944	420.554	214.194
32	140.753	302.039	230.133
33	137.685	422.694	252.320
34	167.982	594.469	276.888
35	182.779	396.033	316.008
36	190.636	574.968	333.008
37	217.377	864.262	370.141
38	224.418	818.135	423.000



Let h_0 and h_1 be two homogeneous polynomials of degree d (horizontal access). Plotted above is the average time in seconds (vertical access) over 100 trials required to calculate a description of $\{h_0, h_1\}$ in $\mathbb{Z}_{962\,592\,769}[x, y]$.

h = randpoly([x,y], homogeneous, deg=d) mod 0.

d	Max Time	Min Time	Average
2	0.068	0.144	0.111
3	0.200	0.264	0.237
4	0.340	0.464	0.390
5	0.480	0.616	0.569
6	0.632	0.804	0.763
7	0.892	1.084	0.984
8	1.128	1.424	1.243
9	1.324	1.704	1.536
10	1.565	2.036	1.834
11	1.861	2.568	2.223
12	2.132	3.088	2.621
13	2.516	4.612	3.236
14	2.784	7.512	4.106
15	3.248	32.07	6.517
16	3.536	40.134	9.682
17	3.80	123.464	19.760
18	4.836	479.066	50.156
19	1163.633	4.849	124.730
20	137.957	33.638	9.068
21	319.104	2240.668	132.613
22	8.525	1086.528	151.689



Let h_0 and h_1 be two homogeneous polynomials of degree d (horizontal access). Plotted above is the average time in seconds (vertical access) over 100 trials required to calculate a description of $\{h_0, h_1\}$ in $\mathbb{Q}[x, y]$.

§7.3 Comparison to other systems

§Magma

Since MAGMA is a commercial product these experiments were done on a different machine. The relevant hardware details are as follows.

```
os          : Ubuntu 10.10
processor   : 4
vendor_id   : GenuineIntel
model name  : Intel(R) Xeon(R) CPU           E5620  @ 2.40GHz
cpu MHz     : 1596.000
cache size  : 12288 KB
```

We timed MAGMA's `IntersectionMultiplicty` [22, Example H84E6] command which can only accept rational points; thereby we are only able to provide timings for rational zeros. As is the case we report the partial Bézout bound (that is, the sum of the intersection multiplicities) and the total time required to calculate them. (Times are reported in seconds.)

Note some systems are entirely disqualified as all their zeros reside in the algebraic closure.

CHARACTERISTIC 0

System	Partial Weight	Bézout Weight	Time
Ojika2	6	8	0.05
Ojika3	4	4	0.00
Eco5	2	8	0.08
ℓ-3	15	81	2.67

CHARACTERISTIC 101

System	Partial Weight	Bézout Weight	Time
Ojika2	6	8	0.05
Ojika3	4	4	0.001
Eco5	2	8	0.240
ℓ-3	15	81	2.680

CHARACTERISTIC 962 592 769

System	Partial Weight	Bézout Weight	Time
Ojika2	8	8	0.010
Ojika3	4	4	0.010
Eco5	2	8	0.020
Barry	4	20	0
Cyclohexane	8	16	0.240
ℓ-3	49	81	8.15

Bibliography

[1] Maria Emilia Alonso, Teo Mora, and Mario Raimondo. Computing with algebraic series. In *Proceedings of the ACM-SIGSAM 1989 International Symposium on Symbolic and Algebraic Computation, ISSAC '89, Portland, Oregon, USA, July 17-19, 1989*, pages 101–111, 1989.

[2] Parisa Alvandi, Changbo Chen, and Marc Moreno Maza. Computing the limit points of the quasi-component of a regular chain in dimension one. In *CASC*, pages 30–45, 2013.

[3] P. Aubry, D. Lazard, and M. Moreno Maza. On the theories of triangular sets. *J. Symb. Comp.*, 28(1-2):105–124, 1999.

[4] P. Aubry and M. Moreno Maza. Triangular sets for solving polynomial systems: a comparison of four methods. Technical Report LIP6/009, LIP6, Université Paris 6, Paris, 1997.

[5] D. Bini and B. Mourrain. Polynomial test suite. `http://www-sop.inria.fr/saga/POL/`. Accessed: April 1, 2012.

[6] F. Boulier, F. Lemaire, and M. Moreno Maza. Well known theorems on triangular systems and the D5 principle. In *Proc. of* Transgressive Computing 2006, Granada, Spain, 2006.

[7] François Boulier, François Lemaire, and Marc Moreno Maza. Well known theorems on triangular systems. Technical Report LIFL 2001–09, Université Lille I, LIFL, 2001.

[8] C. Chen and M. Moreno Maza. Algorithms for computing triangular decompositions of polynomial systems. In *Proc. ISSAC'11*, pages 83–90. ACM, 2011.

[9] Jin-San Cheng and Xiao-Shan Gao. Multiplicity-preserving triangular set decomposition of two polynomials. *Journal of Systems Science and Complexity*, pages 1–25, 2011.

[10] D. Cox, J. Little, and D. O'Shea. *Ideals, Varieties, and Algorithms*. Spinger-Verlag, 1st edition, 1992.

[11] D. Cox, J. Little, and D. O'Shea. *Using Algebraic Geometry*. Graduate Text in Mathematics, 185. Springer-Verlag, New-York, 1998.

[12] B. H. Dayton and Z. Zeng. Computing the multiplicity structure in solving polynomial systems. In *Proceedings of ISSAC '05*, pages 116–123. ACM, 2005.

[13] W. Fulton. *Introduction to intersection theory in algebraic geometry*, volume 54 of *CBMS Regional Conference Series in Mathematics*. Published for the Conference Board of the Mathematical Sciences, Washington, DC, 1984.

[14] W. Fulton. *Algebraic curves*. Advanced Book Classics. Addison-Wesley, 1989.

[15] Patrizia Gianni, Barry Trager, and Gail Zacharias. Gröbner bases and primary decomposition of polynomial ideals. *Journal of Symbolic Computation*, 6(2):149–167, 1988.

[16] Robin Hartshorne. *Algebraic geometry*. Springer, 1977.

[17] M. Kalkbrener. A generalized euclidean algorithm for computing triangular representations of algebraic varieties. *J. Symb. Comp.*, 15:143–167, 1993.

[18] Anthony W. Knapp. *Advanced algebra*. Cornerstones. Birkhäuser Boston Inc., Boston, MA, 2007. Along with a companion volume ıt Basic algebra.

[19] D. Lazard. A new method for solving algebraic systems of positive dimension. *Discr. App. Math*, 33:147–160, 1991.

[20] X. Li, M. Moreno Maza, R. Rasheed, and É. Schost. The modpn library: Bringing fast polynomial arithmetic into maple. In *MICA'08*, pages 73–80, 2008.

[21] Y. L. Li, B. Xia, and Z. Zhang. Zero decomposition with multiplicity of zero-dimensional polynomial systems. *CoRR*, abs/1011.1634, 2010.

[22] Magma. Local geometry. `http://www.itcs.umich.edu/scs/magma/text1029.htm`. [Online; accessed 04-July-2014].

[23] Maplesoft. Regularchains[triangularize]. `http://www.maplesoft.com/support/help/Maple/view.aspx?path=RegularChains/`. [Online; accessed 26-May-2014].

[24] Steffen Marcus, Marc Moreno Maza, and Paul Vrbik. On Fulton's algorithm for computing intersection multiplicities. In *Computer Algebra in Scientific Computing*, pages 198–211. Springer Berlin Heidelberg, 2012.

[25] M. G. Marinari, H. M. Mller, and T. Mora. On multiplicities in polynomial system solving. *TRANS. AMER. MATH. SOC*, 348:3283–3321, 1996.

[26] Ferdinando Mora. An algorithm to compute the equations of tangent cones. In Jacques Calmet, editor, *Computer Algebra*, volume 144 of *Lecture Notes in Computer Science*, pages 158–165. Springer Berlin Heidelberg, 1982.

[27] T Mora and G Pfister C Traverso. An introduction to the tangent cone algorithm issues in robotics and non-linear geometry. *Advances in Computing Research*, 6:199–270, 1992.

[28] M. Moreno Maza. A new algorithm for computing triangular decompositions of algebraic varieties. Technical Report TR 4/98, NAG Ltd, Oxford, UK, 1998.

[29] Bernard Mourrain. Isolated points, duality and residues. *Journal of Pure and Applied Algebra*, 117:469–493, 1997.

[30] I. R. Shafarevich. *Basic algebraic geometry. 1.* Springer-Verlag, Berlin, second edition, 1994.

[31] Singular. Online manual - imult. `http://www.singular.uni-kl.de/Manual/latest/sing_1150.htm#SEC1225`. [Online; accessed 04-July-2014].

[32] D. M. Wang. *Elimination Methods.* Springer, 2000.

[33] Wikipedia. Algebraic Variety — Wikipedia, the free encyclopedia. `http://en.wikipedia.org/wiki/Algebraic_variety`. [Online; accessed 5-May-2014].

[34] Wikipedia. Intersection number — Wikipedia, the free encyclopedia. `http://en.wikipedia.org/wiki/Intersection_number`. [Online; accessed 28-July-2014].

[35] Wikipedia. Regular chain — Wikipedia, the free encyclopedia. `http://en.wikipedia.org/w/index.php?title=Regular_chain`. [Online; accessed 18-June-2014].

[36] W. T. Wu. On zeros of algebraic equations – an application of Ritt principle. *Kexue Tongbao*, 31(1):1–5, 1986.

[37] W. T. Wu. A zero structure theorem for polynomial equations solving. *MM Research Preprints*, 1:2–12, 1987.

Index

affine space, 14
affine spaces, 14

back substitution, 23
base fields, 14

coefficient, 9
cylindrification, 87

Dehomogenizing, 66
description, 48
descriptions, 50

Fulton's algorithm, 1
function notation, 15

generic points, 29
graded, 20

Hilbert Polynomial, 20
homogeneous component of least degree, 65

ideal, 17
ideal brackets, 17
indeterminates, 12
intersection multiplicity, 34, 36, 39
iterated pseudo-quotient, 25
Iterated Pseudo-remainder, 24
iterated pseudo-remainder, 24

kernel, 15

leading coefficient, 12
leading monomial, 12
leading term, 12
linear part, 63
local ring, 35

main variable, 10, 23
maximal, 19
maximal ideals, 19
meromorphic function, 72
monomial, 8
monomial ordering, 10
monomials, 8, 12
multiplicity, 37

non-singular, 63
nullspace, 15

polynomial, 9
polynomial map, 15
polynomial mappings, 14
powerset, 16
prime, 19
prime ideals, 19
pseudo-quotient, 14
pseudo-remainder, 14
pull-back, 82

quasi component, 26
quasi-component, 26
quotient, 13

radical, 18
radical of $\langle \mathbf{f} \rangle$, 18
regular chain, 27
regular elements, 27
Regular points, 35
remainder, 13
Ritt characteristic set, 25

saturation, 27
saturation ideal, 26
secants, 67
singular, 63
singular locus, 63
smooth, 63
Solving, 15
square triangular set, 24
Strong Nullstellensatz, 18

tangent cone, 65
tangent space, 63
term, 9
terms, 9, 11
the ideal defined by V, 17
total degree, 11
total ordering, 10
transversally intersect, 80
triangular sets, 23
triangularization, 29

uniformizer, 82
univariate, 9

variety, 16

Wu characteristic sets, 25

Zariski closure, 27
zero-divisor, 27

Paul Vrbik · The University of Western Ontario · London Ontario Canada

Education

1. Ph.D. Computer Science, University of Western Ontario, 2014.
2. M.Sc. Pure Mathematics, Simon Fraser University, 2008.
3. B.Sc. Pure Mathematics, McMaster University, 2006.

Contributions to research and development

i. Books

1. Jan Vrbik and **Paul Vrbik**. (2012) *Informal Introduction to Stochastic Processes with Maple*. ISBN-10: 1461440564. ISBN-13: 978-1461440567. Springer

ii. Articles published or accepted in refereed journals

1. Michael Coons, **Paul Vrbik**. (2012) An Irrationality Measure for Regular Paperfolding Numbers. Journal of Integer Sequences. Volume 14. Issue 2.
2. Braden Coles, **Paul Vrbik**, Robert D. Giacometti, and Stuart M. Rothstein. (2008) Gamma Distribution Model To Provide a Direct Assessment of the Overall Quality of Quantum Monte Carlo-Generated Electron Distributions. J. Phys. Chem. A, 2008, 112 (10), pp 2012-2017.

iii. Refereed conference proceedings

1. Parisa Alvandi, Changbo Chen, Steffen Marcus, Marc Moreno Maza, Éric Schost, **Paul Vrbik**. (2014) Doing Algebraic Geometry with the RegularChains Library. Mathematical Software (ICMS 2014). Lecture Notes in Computer Science. Springer Berlin Heidelberg.
2. Marc Moreno Maza, Éric Schost, **Paul Vrbik***. (2012) Inversion Modulo Zero-dimensional Regular Chains. Proceedings of the 14th International Workshop on Computer Algebra in Scientific Computing (CASC 2012. Maribor, Slovenia). 198-210. Springer Verlag.
3. Steffen Marcus, Marc Moreno Maza, **Paul Vrbik**. (2012) On Fulton's Algorithm for Computing Intersection Multiplicities. Proceedings of the 14th International Workshop on Computer Algebra in Scientific Computing (CASC 2012. Maribor, Slovenia). 224-235. Springer Verlag.
4. Michael Monagan, **Paul Vrbik***. (2009) Lazy and Forgetful Polynomial Arithmetic and Applications. Proceedings of the 11th International Workshop on Computer Algebra in Scientific Computing (CASC 2009. Kobe, Japan). 226-239. Springer Verlag. (MSc work).
5. B. Coles, I. Bosa, **P. Vrbik**, and R. M. Rothstein*. (2005) Analysis of diffusion Monte Carlo distributions. (Pacifichem 2005. USA, Honolulu). Invited paper. American Institute of Physics.

iv. Non-refereed contributions

1. Marc Moreno Maza, **Paul Vrbik***. (2012) On Fulton's Algorithm for Computing Intersection Multiplicities. Poster presented at East Coast Computer Algebra Day (ECCAD 2012. Rochester, MI).
2. Marc Moreno Maza, **Paul Vrbik***. (2011) Inverting Matrices Modulo Regular Chains. Poster presented at ISSAC 2011 (San Jose, CA).
3. Greg Reid, **Paul Vrbik***. (2009) Visualization of Homotopy's and their Properties. Poster presented at East Coast Computer Algebra Day 2009 (Kingston, RI).

4. Michael Coons*, **Paul Vrbik**. (2007) On the density of integers bi-representable as the sum of two cubes. Poster presented at CMS-MITACS Joint Conference (Winnepeg, MB).
5. **P. Vrbik**, S. Jahed. (2006) Verifying Baklava. Undergraduate Thesis (McMaster University).
6. **Paul Vrbik***, Stuart M. Rothstein. (2005) Determining α-polarizability of hydrogen molecule using Quantum Monte Carlo. Poster presented at Mercury conference on computational chemistry (Clinton, NY).

v. Technology Transfers

1. **Paul Vrbik***. (2012) Algebraic Geometry Tools (regular chains sub-library). Software written for Maplesoft.
2. **Paul Vrbik***. (2006) A generalized algorithm for Quantum Monte Carlo on arbitrary molecules. Software written for the Theoretical Chemistry Lab at Brock University.

Honours and Awards

i. Scholarships

1. Alexander Graham Bell Canada Graduate Scholarships, Doctorate. $105,000. (2010).
2. Graduate Fellowship. Simon Fraser University. $6,250. (2008).
3. MITACS Industrial Scholarship. $15,000. (2008).
4. McMaster Entrance Scholarship. $4,000. (2002).

ii. Distinctions

1. University Students Council, Teaching Honour Roll. (2012).
2. UWORCS, best talk in session. (2011).
3. UWORCS, best talk in session. (2009).
4. CECM Days, second place poster prize. (2008).

iii. Nominations

1. For USC Teaching Award by students. CS3331A Foundations of Computer Science (2013). *This award is given for execellence in instruction.*
2. For best TA by Dr. Charles Ling at UWO, CS1011 Applied Logic. (2011).
3. For best TA by Dr. Marc Moreno Maza at UWO, CS1026 Introduction to Programming. (2010).
4. For McMaster President's Award by the department of Mathematics at McMaster University. (2006). *This award is considered the schools highest honour in student leadership.*

Relevant activities

i. Teaching

1. Instructor, CS 3331 "Foundations of Computer Science", Fall 2012.
2. Teaching Assistant, Computer Science, University of Western Ontario, 2009-present.
3. Teaching Assistant, Mathematics, Simon Fraser Univerity, 2006-2007.
4. Teaching Assistant, Computer Science, McMaster University, 2004-2006. *In addition to my regular TA duties I wrote lab handouts and courseware that are still being used.*

5. Student Director of High School Outreach, McMaster University, 2004-2005. *I ran an outreach program to teach "gifted" high school students mathematics.*

ii. Committees

1. Math representative to the Graduate Issues Committee, Simon Fraser University, 2007.
2. Mathematics and Statistics representative to the Ad Hoc Science Curriculum Review Committee (SCRC), McMaster University, 2006. *The mandate of the SCRC was to examine the nature and delivery of the undergraduate curriculum in Science, and to make recommendations to the Dean and to the departments and programs of the Faculty of Science.*

iii. Peer Review

1. ISSAC 2013 (1), 2012 (1), 2010 (2).
2. CASC 2011 (2).

iv. Elected Positions

1. Members Services Officer, Math Grad Student Union, Simon Fraser University, 2007.
2. President, Math Student Union, Simon Fraser University, 2006.
3. President, Math and Stats Society, McMaster University, 2003, 2004, 2005.