

ULTRAMETRIC FEWNOMIAL THEORY

A Dissertation

by

ASHRAF IBRAHIM ABDELHALIM

Submitted to the Office of Graduate Studies of
Texas A&M University
in partial fulfillment of the requirements for the degree of

DOCTOR OF PHILOSOPHY

December 2009

Major Subject: Mathematics

ULTRAMETRIC FEYNOMIAL THEORY

A Dissertation

by

ASHRAF IBRAHIM ABDELHALIM

Submitted to the Office of Graduate Studies of
Texas A&M University
in partial fulfillment of the requirements for the degree of

DOCTOR OF PHILOSOPHY

Approved by:

Chair of Committee,	J. Maurice Rojas
Committee Members,	Andreas Klappenecker
	Frank Sottile
	Matthew Young
Head of Department,	Albert Boggess

December 2009

Major Subject: Mathematics

ABSTRACT

Ultrametric Fewnomial Theory. (December 2009)

Ashraf Ibrahim Abdelhalim, B.S., University of Khartoum, Sudan;

M.S., Southern Illinois University

Chair of Advisory Committee: Dr. J. Maurice Rojas

An ultrametric field is a field that is locally compact as a metric space with respect to a non-archimedean absolute value. The main topic of this dissertation is to study roots of polynomials over such fields.

If we have a univariate polynomial with coefficients in an ultrametric field and non-vanishing discriminant, then there is a bijection between the set of roots of the polynomial and classes of roots of the same polynomial in a finite ring. As a consequence, there is a ball in the polynomial space where all polynomials in it have the same number of roots.

If a univariate polynomial satisfies certain generic conditions, then we can efficiently compute the exact number of roots in the field. We do that by using Hensel's lemma and some properties of Newton's polygon.

In the multivariate case, if we have a square system of polynomials, we consider the tropical set which is the intersection of the tropical varieties of its polynomials. The tropical set contains the set of valuations of the roots, and for every point in the tropical set, there is a corresponding system of lower polynomials. If the system satisfies some generic conditions, then for each point w in the tropical set the number of roots of valuation w equals the number roots of valuation w of the lower system.

The last result enables us to compute the exact number of roots of a polynomial system where the tropical set is finite and the lower system consists of binomials. This algorithmic method can be performed in polynomial-time if we fix the number

of variables.

We conclude the dissertation with a discussion of the feasibility problem. We consider the problem of the p -adic feasibility of polynomials with integral coefficients with the prime number p as a part of the input. We prove this problem can be solved in nondeterministic polynomial-time. Furthermore, we show that any problem, which can be solved in nondeterministic polynomial-time, can be reduced to this feasibility problem in randomized polynomial-time.

To the memory of my mother

ACKNOWLEDGMENTS

I would like to express my sincere gratitude to my advisor Dr. J. Maurice Rojas, for his guidance, support and patience during my slow progress while doing my research throughout my doctoral study.

I also would like to thank my committee members, Dr. Andreas Klappenecker, Dr. Frank Sottile and Dr. Matthew Young, for reviewing my work and for their helpful remarks regarding this dissertation. I am also very grateful to my friend Dr. Martin Avendaño for our fruitful collaboration.

I thank Dr. Al Boggess, Dr. Thomas Schlumprecht, Dr. Paulo Lima-Filho, Ms. Monique Stewart, and all other staff in the Department of Mathematics for their appropriate support.

Finally, I would like to thank all of my friends in the Mathematics Department at Texas A&M.

TABLE OF CONTENTS

CHAPTER		Page
I	INTRODUCTION	1
	A. p -adic Root Counting	1
	B. p -adic Descartes' Bounds	2
	C. p -adic Feasibility	3
	D. Dissertation Overview	3
II	BACKGROUND	6
	A. Non-archimedean Fields	6
	B. p -adic Numbers	8
	1. What Are the p -adic Numbers?	8
	2. Finite Extensions of \mathbb{Q}_p	10
	3. Universal p -adic Fields	11
	C. Polyhedral Geometry	13
	D. Newton Polygon and Regular Polynomials	15
III	ROOT COUNTING	19
	A. Roots of the Reduced Polynomials	19
	B. Counting Roots of Regular Polynomials	22
	C. Tropical Varieties	25
	D. Multivariate Root Counting	32
	1. Semiregular Polynomial Systems	32
	2. Regular Polynomial Systems	38
IV	DESCARTES' BOUNDS	44
	A. Univariate Bounds	44
	B. Multivariate Bounds	48
	C. Semiregular Polynomials Bounds	52
V	COMPLEXITY THEORY	56
	A. Complexity and Feasibility	56
	1. Overview of Some Complexity Classes	56
	2. The Feasibility Problem	57
	B. p -adic Feasibility	60

CHAPTER	Page
VI CONCLUSIONS AND FUTURE WORK	65
REFERENCES	66
VITA	68

LIST OF FIGURES

FIGURE		Page
1	The Newton polygon of $X^4 - \frac{2}{3}X^3 - \frac{28}{3}X^2 + 6X + 3$	16
2	The tropical variety of $X^2Y^2 + 9XY^2 + 5X + 3$	27

CHAPTER I

INTRODUCTION

A. p -adic Root Counting

One of the fundamental problems in computational algebraic geometry is counting roots of polynomials over different fields. Over the reals, Sturm's theorem is the most famous algorithmic result for counting the number of real roots of univariate polynomials with real coefficients in a given interval. Sylvester and Habicht gave generalizations of Sturm's theorem, see [2, Section 8.3]. Those results are the basis for most algorithmic methods over the real numbers and many of the algorithms have been implemented in many computer algebra systems.

On the other hand, the field of p -adic numbers \mathbb{Q}_p is also, like the reals, the completion of the rational number, \mathbb{Q} with respect to some norm. Therefore \mathbb{Q}_p shares many properties with \mathbb{R} and they have the same cardinality. But the results on root counting over the p -adics remain theoretical for the most part. T. Sturm and V. Weispfenning [20] gave an algorithm to compute the exact number of roots of a univariate polynomial in a prescribed p -adic ball. Here we are trying to answer a slightly different question, that is given a polynomial $f \in K[X]$, where K is an ultrametric field, under what conditions would we be able to count the exact number of roots in K and not just in a particular ball? We show that if the polynomial, say f , is a regular polynomial (see definition D.12), then we can count the exact number of roots in K .

This dissertation follows the style of *Advances in Computational Mathematics*.

Another interesting result over the reals is: if two polynomials $f, g \in \mathbb{R}[X]$ are in the same discriminant chamber, then they have the same number of real roots. Since \mathbb{Q}_p is totally disconnected, we can't translate the techniques to the p -adic case. We have made some progress in answering the question of when two polynomials in \mathbb{Q}_p have the same number of roots and that is Corollary A.8.

B. p -adic Descartes' Bounds

Descartes' Rule of Signs implies that any real univariate polynomial with exactly t non-zero terms has at most $2t - 1$ real roots (counted with multiplicities except for the possible root 0 which is counted only once). A lot of progress has been made in the direction of generalizing Descartes' Rule of Signs to multivariate polynomials. A. Khovanskii [8] has generalized Descartes' Bound to a certain systems of sparse polynomials. Khovanskii's results imply that a square system of n real polynomial equations in n variables with total t terms has at most $(n + 1)^t 2^{t(t-1)/2}$ non-degenerate roots in the positive orthant. Khovanskii's bound was improved by the work of F. Bihan and F. Sottile [3].

On the ultrametric side, Denef and van den Dries [5] gave a bound of sparse systems of polynomials over \mathbb{Q}_p . Later, their bound was improved by L. Lipshitz [10]. In 1994, Gelfand, Kapranov and Zelvinsky [7] derived the archimedean amoeba theorem which describe complex zero sets of polynomial on "log paper". H.W. Lenstra [9] gave an analogue of Descartes' bound over the p -adic numbers. He showed that if $f \in K[X]$ is an univariate polynomial with coefficients in K , a finite extension of the p -adic rationals \mathbb{Q}_p , with at most $t \geq 1$ monomial terms, then the number of roots of f in K is $O(t^2(q - 1) \log(t))$ where q is the cardinality of the residue field of K . As a consequence of our result of root counting, we can improve Lenstra's bound to

$O(t(q - 1))$ for regular polynomials.

C. p -adic Feasibility

The feasibility problem over a field K is deciding whether a K -algebraic set, i.e. the zero set of a collection of multivariate polynomials, is empty or not. It has been known that feasibility over the complex numbers is **NP**-hard which means any problem in **NP** can be reduced in polynomial-time to the feasibility problem over the complex numbers.

Over finite fields of prime cardinalities, the feasibility problem is known to be **NP**-complete, i.e. it is in **NP** and it is **NP**-hard as well. But the feasibility over the rationals is an open problem.

On the ultrametric side, we show that deciding whether or not a univariate binomial with integral coefficients has a root can be done in polynomial-time. In addition to that, feasibility of polynomials with integral coefficients over the p -adics is in **NP** if the prime p is part of the input.

D. Dissertation Overview

The main topic of this dissertation is counting and estimating the number of roots of polynomials over non-archimedean fields with discrete valuation. This dissertation consists of the following four chapters (in addition to the Introduction and the Conclusion):

Chapter II- Background. This chapter is a brief overview of the material used in this dissertation and it contains four sections:

1. *Non-archimedean Fields:* This section is a short introduction to non-archimedean fields and their main algebraic and topological properties.

2. *p-adic Numbers*: The section discusses the p -adic numbers as our main example of non-archimedean fields with discrete valuation.
3. *Polyhedral Geometry*: This is a brief introduction to the theory of polytopes and it contains the results used later in the dissertation.
4. *Newton Polygon and Regular Polynomials*: We define Newton's polygon of univariate polynomials and regularity. In addition, we define the lower polynomials and prove a key property of regular polynomials.

Chapter III- Root Counting. In this chapter we discuss some algorithmic methods to count the exact number of roots of univariate polynomials, as well as square systems of multivariate polynomials. It consists of the following sections:

1. *Roots of the Reduced Polynomials*: In this section we obtain a reformulation of Hensel's lifting and show a condition for two polynomials to have the same number of roots.
2. *Counting Roots of Regular Polynomials*: For univariate regular polynomials, we can count the exact number of roots and the method is discussed in this section.
3. *Tropical Varieties*: This section presents algebraic definitions of tropical variety and lower polynomials and discusses some of their properties.
4. *Multivariate Root Counting*: This section introduces the semiregular and regular systems of polynomials. A method of computing the exact number of roots of a regular system of polynomials is also presented.

Chapter IV- Descartes' Bounds. In this chapter, we study estimations of the number of roots of polynomials over non-archimedean fields with discrete valuation. The chapter divides into the following three sections:

1. *Univariate Bounds*: It discusses the work of Lenstra over the p -adic numbers and the improved bound of the number of roots for regular polynomials.
2. *Multivariate Bounds*: In this section we prove Rojas' bound for the number of isolated roots of a system of polynomials in more than one variable over the p -adic numbers.
3. *Semiregular Polynomials Bounds*: In this section we show that Rojas' bound can be improved for semiregular square systems of polynomials.

Chapter V- Complexity Theory. The last chapter discusses the connection between p -adic numbers and complexity theory. It contains only the following two sections:

1. *Complexity and Feasibility*: It is a short introduction to complexity classes and feasibility problems and present some recent work.
2. *p -adic Feasibility*: This section dicusses some results about the feasibility problem over the p -adic numbers.

CHAPTER II

BACKGROUND

A. Non-archimedean Fields

Definition A.1. Let K be a field and K^\times be the set of non-zero elements of the field K . A non-archimedean valuation on K is a function

$$v : K \rightarrow \mathbb{R} \cup \{\infty\}$$

satisfies the following three conditions:

- 1- $v(a) = \infty \Leftrightarrow a = 0$.
- 2- $v(ab) = v(a) + v(b)$.
- 3- $v(a + b) \geq \min\{v(a), v(b)\} \quad \forall a, b \in K^\times$.

The following two lemmas are key properties of non-archimedean valuations.

Lemma A.2. If $v(a) \neq v(b)$ for $a, b \in K$ then $v(a + b) = \min\{v(a), v(b)\}$.

Lemma A.3. If $a_1 + a_2 + \dots + a_k = 0$ then there are $i \neq j$ such that

$$v(a_i) = v(a_j) = \min\{v(a_1), v(a_2), \dots, v(a_k)\}$$

.

The valuation v on K induces an *absolute value* $|\cdot| : K^\times \rightarrow \mathbb{R}_{>0}$, extended by $|0| = 0$, as follows

$$|a|_v = \alpha^{v(a)}$$

for $0 < \alpha < 1$, $a \in K^\times$. This absolute value satisfies a stronger triangle inequality namely

$$|a + b| \leq \max(|a|, |b|)$$

which is known as *the non-archimedean property* and we call $|\cdot|$ a *non-archimedean absolute value*. Any field K with a non-archimedean absolute value is called a *non-archimedean field*.

Example:

Let $\mathbb{C}((T))$ be the field of Laurent series in T , then field of *Puiseux series*, $\mathbb{C}\{\{T\}\}$ is defined as follows

$$\mathbb{C}\{\{T\}\} := \bigcup_{n \geq 1} \mathbb{C}((T^{\frac{1}{n}})).$$

A typical element $c(T) \in \mathbb{C}\{\{T\}\}$ is written as follows

$$c(T) = c_1 T^{a_1} + c_2 T^{a_2} + c_3 T^{a_3} + \dots$$

where $c_i \in \mathbb{C} \forall i$ and $a_1 < a_2 < \dots$ are rational numbers that have a common denominator. The valuation $v : \mathbb{C}\{\{T\}\} \rightarrow \mathbb{R}$ is given by $v(c(T)) = a_1$. The field of Puiseux series is algebraically closed.

Theorem A.4. *Let K be a non-archimedean field with non-trivial absolute value. Then K is locally compact if and only if the following three conditions are satisfied:*

- 1- K is a complete metric space.
- 2- The residue field is finite.
- 3- $|K^\times|$ is a discrete subgroup of $\mathbb{R}_{>0}$.

Definition A.5. *Any non-archimedean field has the above properties is called an ultrametric field.*

Theorem A.6 (Hensel). *Let K a complete non-archimedean field with maximal subring A and $f \in A[X]$. If $x \in A$ satisfies $v(f(x)/f'(x)^2) > 0$ then there exists a root $\xi \in A$ of f such that $v(\xi - x) = v(f(x)/f'(x))$.*

Proof. See [15, Sec. 1.5, Ch. 2]. □

B. p -adic Numbers

In this exposition, we are going to give a short introduction to p -adic numbers and then state some preliminary results in p -adic analysis. For more details see [12], [15], [17] and [21].

1. What Are the p -adic Numbers?

Let \mathbb{Q} denote the set of rational numbers, we can construct a norm on \mathbb{Q} in the following way:

Let p be a prime number, and for any integer $a \in \mathbb{Z}$, define the p -adic valuation of a , denoted $v_p(a)$, to be the highest power of p which divides a . We can extend the definition of the p -adic valuation of $x \in \mathbb{Q}$ by $v_p(x) = v_p(a) - v_p(b)$ where $x = a/b$ for $a, b \in \mathbb{Z}, b \neq 0$.

So, now we can define the p -adic norm, $|\cdot|_p$, as follows

$$|x|_p = \begin{cases} p^{-v_p(x)} & \text{if } x \neq 0 \\ 0 & \text{if } x = 0. \end{cases}$$

The p -adic norm on \mathbb{Q} is in fact a norm and it satisfies the non-Archimedean property, namely,

$$|x + y|_p \leq \max(|x|_p, |y|_p) \quad \forall x, y \in \mathbb{Q}.$$

which implies that if $|x|_p > |y|_p$, then $|x + y|_p = |x|_p$.

In 1918, Ostrowski showed that any norm defined on \mathbb{Q} is equivalent to $|\cdot|_p$ for some prime p or the usual absolute value.

Definition B.1. *The field of p -adic numbers, \mathbb{Q}_p , is defined to be the completion of \mathbb{Q} with respect to the norm $|\cdot|_p$.*

Therefore, by the above definition, \mathbb{Q} is dense in the complete field \mathbb{Q}_p .

Definition B.2. *The subring*

$$\mathbb{Z}_p = \{x \in \mathbb{Q}_p : |x|_p \leq 1\}$$

is called the ring of p -adic integers, and the subset

$$\mathfrak{m} = \{x \in \mathbb{Q}_p : |x|_p < 1\}$$

is a maximal ideal of \mathbb{Z}_p which is equal to $p\mathbb{Z}_p$.

It can be shown that \mathbb{Z}_p is a local ring and \mathbb{Z} is dense in \mathbb{Z}_p . In addition to that, the ring of p -adic integers, \mathbb{Z}_p , is an integral domain and a principal ideal domain with \mathbb{Q}_p as its field of fractions. If we look at \mathbb{Z}_p as subspace of \mathbb{Q}_p , it is compact and totally disconnected.

Given any $x \in \mathbb{Q}_p$, we can write it as a formal power series

$$x = \sum_{n \leq m}^{\infty} a_n p^n, \quad 0 \leq a_n \leq p - 1.$$

If $m \geq 0$, then $x \in \mathbb{Z}_p$.

The following result is Hensel's lemma, which plays an important role in computing zeros of polynomials over the p -adic numbers.

Theorem B.3. *Let $f(X) \in \mathbb{Z}_p$ be a polynomial in $\mathbb{Z}_p[X]$ and $f'(X)$ its formal derivative. If $f(X) \equiv 0 \pmod{p}$ has a_1 satisfying $f'(a_1) \not\equiv 0 \pmod{p}$ then there is a unique p -adic integer a such that $f(a) = 0$ and $a \equiv a_1 \pmod{p}$.*

So if we have, for example, $\alpha\mathbb{Z}_p \setminus p\mathbb{Z}_p$, $\alpha \neq 0$, then we consider the polynomial $f(X) = \alpha X - 1$. Since for some β , $f(\beta) \equiv 0 \pmod{p}$ and $f'(\beta) = \alpha \not\equiv 0 \pmod{p}$, so by Hensel's lemma, there is a p -adic integer x such that $f(x) = 0$, hence α is invertible in \mathbb{Z}_p .

2. Finite Extensions of \mathbb{Q}_p

If K is any finite extension of \mathbb{Q}_p , the p -adic norm $|\cdot|_p$ can be extended uniquely to the field K by

$$|\alpha|_p = |N_{K/\mathbb{Q}_p}(\alpha)|_p^{1/d} \quad \forall \alpha \in K$$

where

$$N_{K/\mathbb{Q}_p}(\alpha) = \prod_{\sigma \in G} \sigma \alpha \in \mathbb{Q}_p,$$

$G = \text{Gal}(K/\mathbb{Q}_p)$ is Galois group and $d = |G| = [K : \mathbb{Q}_p]$. The norm defined over K is also non-Archimedean and K is complete with respect to it. In fact, the field K is locally compact and the set $|K^\times|_p$ is a discrete subgroup of $\mathbb{R}_{>0}$. Hence there is an element $\pi \in K^\times$ such that

$$|\pi|_p = \max |K^\times|_p \cap (0, 1) = \theta.$$

Let's define the maximal subring of the field K to be

$$A_K = \{x \in K : |x|_p \leq 1\}$$

and the maximal ideal of A_K to be

$$M_K = \{x \in K : |x|_p < 1\}.$$

We have now, $M_K = \pi A_K$ and the field $k = A_K/M_K$ is a finite extension of $\mathbb{Z}_p/p\mathbb{Z}_p = \mathbb{F}_p$. The field k is called *the residue field* and the degree of the extension k/\mathbb{F}_p , denoted f , is called *the residue degree*. Since $p \in M_K$, we have $|p|_p = 1/p = \theta^e$, i.e. $|\pi|_p = |p|_p^{1/e}$ for some integer $e \geq 1$. The integer e is called *the ramification index* of K over \mathbb{Q}_p and

$$e = [|K^\times|_p : |\mathbb{Q}_p^\times|_p] = [p^{\frac{1}{e}\mathbb{Z}} : p^{\mathbb{Z}}].$$

In addition, any $x \in K$ can be written in the following form

$$x = \sum_{i \geq m} a_i \pi^i$$

where $m \in \mathbb{Z}$ and $a_i \in A_K/M_K$. The following result states a very interesting relation between the residue degree and the ramification index.

Theorem B.4. *For each finite extension K of \mathbb{Q}_p , we have*

$$ef = [K : \mathbb{Q}_p] = d.$$

A finite extension K of \mathbb{Q}_p is said to be

- 1- *unramified* if $e = 1$.
- 2- *totally ramified* if $f = 1$.
- 3- *tamely ramified* if p does not divide e .
- 4- *widely ramified* if e is a power of p .

Eisenstein criterion for irreducibility holds over \mathbb{Z}_p as well as \mathbb{Z} .

Theorem B.5. *let $f(X) \in \mathbb{Z}$ be a monic polynomial of degree $n \geq 1$ with $f(X) \equiv X^n \pmod{p}$ and $f(0) \not\equiv 0 \pmod{p^2}$, then f is irreducible over $\mathbb{Z}_p[X]$ and $\mathbb{Q}_p[X]$.*

A polynomial satisfies the conditions of the above result is called an *Eisenstein polynomial*. If K is totally ramified over \mathbb{Q}_p , so it is generated by a root of an Eisenstein polynomial.

3. Universal p -adic Fields

The norm extension can be defined over the algebraic extension, \mathbb{Q}_p^a , of \mathbb{Q}_p in a very similar manner

$$|\alpha|_p = |N_{\mathbb{Q}_p(\alpha)/\mathbb{Q}_p}(\alpha)|_p^{1/[\mathbb{Q}_p(\alpha):\mathbb{Q}_p]} \quad \forall \alpha \in \mathbb{Q}_p^a.$$

Here the valuation ring defined in the usual manner

$$A^a = \{x \in \mathbb{Q}_p^a : |x|_p \leq 1\}$$

and the maximal ideal

$$M^a = \{x \in \mathbb{Q}_p^a : |x|_p < 1\}.$$

The residue field $k^a = A^a/M^a$ of \mathbb{Q}_p^a is in fact the algebraic closure of the finite field \mathbb{F}_p . But, unlike \mathbb{Q}_p , the field \mathbb{Q}_p^a is neither complete nor locally compact.

Theorem B.6. *Let K/\mathbb{Q}_p be a finite extension and $\alpha \in \mathbb{Q}_p^a$. Let r be the number*

$$r = \min_{\alpha^\sigma \neq \alpha} |\alpha^\sigma - \alpha|_p$$

where α^σ are the conjugates of α . Then $\forall \beta \in B_{<r}(\alpha) = \{x \in \mathbb{Q}_p^a : |x - \alpha|_p < r\}$, we have $K(\alpha) \subset K(\beta)$.

If the polynomial $f = \sum_{i=0}^n a_i X^i$, let $\|f\| = \max_i |a_i|_p$. As consequence of the above theorem, if $f \in K[X]$ is the monic minimal polynomial of α of degree n , then there is $\varepsilon > 0$ such that for any monic polynomial $g \in K[X]$ of degree n with $\|f - g\| < \varepsilon$ has a root $\beta \in K(\alpha)$ and $K(\alpha) = K(\beta)$.

Since the field \mathbb{Q}_p^a is not complete, we need to go to a bigger field that is complete.

Let \mathbb{C}_p , the field of the p -adic complex numbers, be the completion of \mathbb{Q}_p^a with respect to the p -adic norm defined above. The field \mathbb{C}_p has the following properties

- 1- \mathbb{C}_p is algebraically closed.
- 2- \mathbb{C}_p is infinite dimensional over \mathbb{Q}_p .
- 3- \mathbb{C}_p is not locally compact.
- 4- \mathbb{C}_p is separable.
- 5- The residue field of \mathbb{C}_p is the algebraic closure of the finite field \mathbb{F}_p .
- 6- $|\mathbb{C}_p^\times|_p = \{p^r : r \in \mathbb{Q}\} = p^\mathbb{Q}$.

Theorem B.7. *The field \mathbb{C}_p is isomorphic to the field \mathbb{C} of the complex numbers.*

If p is odd, then, by Hensel's lemma, for each $0 \leq i \leq p-1$, there is a number $\omega(i) \in \mathbb{Z}_p$ such that $\omega(i) \equiv i \pmod{p}$ and $\omega(i)^p = 1$. The numbers $\omega(i)$ are called the Teichmüller representatives of the residue classes mod p . The map

$$(\mathbb{Z}/p\mathbb{Z})^\times \rightarrow \mathbb{Z}_p$$

given by $x \mapsto \omega(x)$ defines a multiplicative character called *the Teichmüller character*. For any $x \in \mathbb{Z}_p$, we define $\omega(x)$ to be $\omega(x \bmod p)$. Note that any $x \in \mathbb{Z}_p$ can be written uniquely as $x = \omega(x)\langle x \rangle$ with $\langle x \rangle \in 1 + p\mathbb{Z}_p$.

C. Polyhedral Geometry

A set $X \subseteq \mathbb{R}^d$ is *convex* if for any two points $x, y \in X$ we have $\lambda x + (\lambda - 1)y \in X$, $0 \leq \lambda \leq 1$. The *convex hull* $\text{conv}(A)$ of A is the smallest convex set in \mathbb{R}^d containing A . In other words

$$\text{conv}(A) = \bigcap_{\substack{A \subseteq X \\ X \text{ is convex}}} X$$

or equivalently

$$\text{conv}(A) = \{\lambda_1 a_1 + \cdots + \lambda_n a_n : a_i \in A, \lambda_1 + \cdots + \lambda_n = 1, \lambda_i \geq 0\}.$$

If A is a finite set then $\text{conv}(A)$ is called a *convex polytope*. A *polyhedral cone*, $\text{cone}(A)$, in \mathbb{R}^d is the positive hull of a finite collection of vectors in \mathbb{R}^d , i.e.

$$\begin{aligned} \text{cone}(A) &= \text{pos}(v_1, \dots, v_n) \\ &= \{\lambda_1 v_1 + \cdots + \lambda_n v_n : \lambda_i \geq 0\}. \end{aligned}$$

Every cone C has the form $C = \{x \in \mathbb{R}^d : Mx \leq 0\}$ where M is $n \times d$ matrix.

A *face* of a cone C is determined by a linear functional $\omega \in \mathbb{R}^{d^*}$ by

$$\text{face}_\omega(C) = \{x \in C : \omega \cdot x \leq \omega \cdot y, \quad \forall y \in C\}.$$

We call ω in this case the *inner normal* of the face $\mathcal{F} = \text{face}_\omega(C)$. We say the face \mathcal{F} is a *lower face* (resp. *upper face*) if the last coordinate of ω is positive (resp. negative).

The *Minkowski sum* of two set $P, Q \subseteq \mathbb{R}^d$ is the set

$$P + Q = \{x + y : x \in P, y \in Q\}.$$

A *polyhedron* is a set of the form $\text{conv}(A) + \text{cone}(B)$ where A and B are finite subsets of \mathbb{R}^d . A *polytope* is a bounded polyhedron. The *dimension* of a polyhedron P is the dimension of its affine hull $\{\lambda_1 p_1 + \dots + \lambda_n p_n : p_i \in P, \lambda_1 + \dots + \lambda_n = 1\}$. A *full dimensional* polyhedron is a polyhedron of dimension d .

Another way to describe a polyhedron is the following: $P \subseteq \mathbb{R}^d$ is a polyhedron if it is an intersection of finitely many half spaces, i.e.

$$P = \{x \in \mathbb{R}^d : Mx \leq b\}$$

where M is $n \times d$ matrix and $b \in \mathbb{R}^d$.

A *polyhedral complex* Δ in \mathbb{R}^d is a finite collection of polyhedra in \mathbb{R}^d such that

1. the empty polytope is in Δ ,
2. if a polyhedron is in Δ , then all of its faces are also in Δ ,
3. the intersection of any two polyhedra in Δ is a face of both.

The *support* of Δ is

$$|\Delta| = \bigcup_{P \in \Delta} P.$$

The dimension of Δ is the largest dimension of polyhedra $P \in \Delta$. A maximal face of Δ is a polyhedron in Δ that is not contained in any other polyhedra in Δ . A polyhedral complex is *pure* if all of its maximal faces have the same dimension.

D. Newton Polygon and Regular Polynomials

Let K be an ultrametric field, so it is complete with respect to non-archimedean discrete valuation v . Let K_v denote the residue field of K where K_v is finite of characteristic p .

Definition D.1. Let $f(X) = a_n X^n + a_{n-1} X^{n-1} + \dots + a_1 X + a_0 \in K[X]$. The Newton polygon of f , $\text{Newt}_v(f)$, is the convex hull of the set of points $\{(i, v(a_i)) : i = 0, 1, \dots, n\}$. If K is a p -adic field, we write $\text{Newt}_p(f)$ for the Newton polygon of f .

Theorem D.2. Let $f(X) = a_n X^n + a_{n-1} X^{n-1} + \dots + a_1 X + a_0 \in K[X]$ be such that $a_0 a_n \neq 0$. Let S be the lower edge in the Newton polygon of f connecting the points $(s, v(a_s))$ and $(s', v(a_{s'}))$ with $s > s'$. Then f has exactly $s - s'$ roots with valuation m where $-m$ is the slope of the segment S . Moreover, f can be factorized as

$$f(X) = a_n \prod f_m(X) \tag{2.1}$$

where f_m is a monic polynomial in $K[X]$ with all roots of valuation m .

Proof. See [21, Prop. 3.1.1]. □

Note that the above theorem is true for any non-archimedean field.

Definition D.3. A polynomial $f(X) = a_n X^n + a_{n-1} X^{n-1} + \dots + a_1 X + a_0 \in K[X]$ is regular if for any edge $S = (s, v(a_s)) \leftrightarrow (s', v(a_{s'}))$ of the Newton polygon (with $s > s'$), we have:

1. S does not contain any point from the set $\{(i, v(a_i)) : i = 1, \dots, n\}$ except the points $(s, v(a_s))$ and $(s', v(a_{s'}))$.
2. $p \nmid s - s'$ where $p = \text{char}(K_v)$.

The polynomial $a_{s'}X^{s'} + a_sX^s$ is called the lower binomial of f corresponding to the edge S .

To illustrate the above definitions, consider the following example

Example:

Consider the polynomial $f = X^4 - \frac{2}{3}X^3 - \frac{28}{3}X^2 + 6X + 3 \in \mathbb{Q}_3[X]$, which can be written as $f = (X - 1)(X^2 - 9)(X + \frac{1}{3})$.

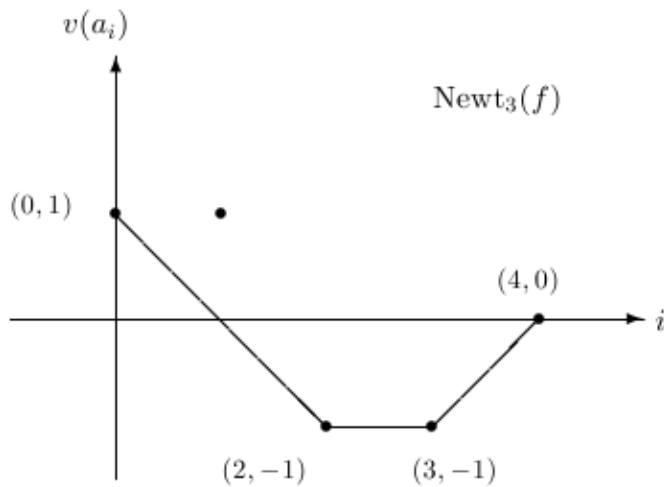


Fig. 1. The Newton polygon of $X^4 - \frac{2}{3}X^3 - \frac{28}{3}X^2 + 6X + 3$

The polynomial f is regular and it has (see Fig. 1):

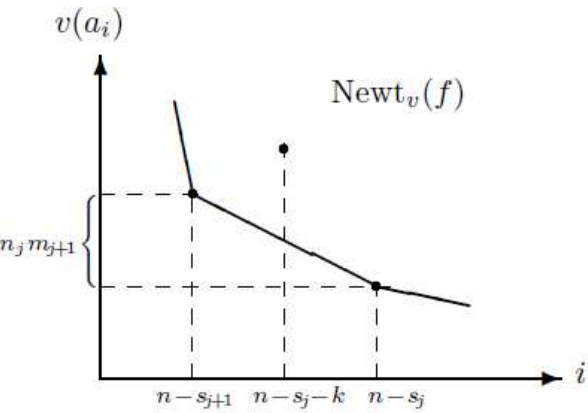
- i- Two roots of valuation $v = 2$ and $f_2 = (X^2 - 9)$. The corresponding edge is $(2, -1) \leftrightarrow (0, 1)$ and the lower binomials is $-\frac{28}{3}X^2 + 3$.
- ii- One root of valuation $v = 0$ and $f_0 = X - 1$. The corresponding edge is $(3, -1) \leftrightarrow$

$(2, -1)$ and the lower binomial is $-\frac{2}{3}X^3 - \frac{28}{3}X^2$.

iii- One root of valuation $v = -1$ and $f_{-1} = X + \frac{1}{3}$. The corresponding edge is $(4, 0) \leftrightarrow (3, -1)$ and the lower binomial is $X^4 - \frac{2}{3}X^3$.

Theorem D.4. *Let $f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0 \in K[X]$ be a regular polynomial. Then all factors $f_m(X)$ in equation (2.1) are also regular.*

Proof. Let $\alpha_1, \alpha_2, \dots, \alpha_n \in \overline{K}$ be all the roots of f . Assume that

$$\begin{aligned} v(\alpha_1) &= \cdots = v(\alpha_{s_1}) = m_1 \\ v(\alpha_{s_1+1}) &= \cdots = v(\alpha_{s_2}) = m_2 \\ &\vdots \\ v(\alpha_{s_j+1}) &= \cdots = v(\alpha_{s_{j+1}}) = m_{j+1} \\ &\vdots \\ v(\alpha_{s_t+1}) &= \cdots = v(\alpha_{s_{t+1}}) = m_{t+1} \end{aligned}$$


where $m_1 < m_2 < \cdots < m_{t+1}$. In order to keep a consistent notation we set $s_0 = 0$ and $s_{t+1} = n$. Let g be the factor $f_{m_{j+1}}$ of f and let $n_j = s_{j+1} - s_j$ be the degree of g .

$$\begin{aligned} g(X) &= (X - \alpha_{s_j+1})(X - \alpha_{s_j+2}) \cdots (X - \alpha_{s_{j+1}}) \\ &= X^{n_j} + b_{n_j-1}X^{n_j-1} + \cdots + b_1X + b_0. \end{aligned}$$

The coefficients b_{n_j-k} and a_{n-s_j-k} , where $0 \leq k \leq n_j$, can be written in terms of the roots of f as where, as usual, an empty product is defined as 1.

Note that in the case $k = 0$, the term $\delta = (-1)^{s_j} \alpha_1 \alpha_2 \cdots \alpha_{s_j}$ appears in the sum corresponding to a_{n-s_j} and it has strictly minimum valuation. This means that $v(\delta) = v(a_{n-s_j}) = n_0 m_1 + n_1 m_2 + \cdots + n_{j-1} m_j$. When $0 < k < n_j$ we can write

$$a_{n-s_j-k} = \delta b_{n_j-k} + \beta \tag{2.2}$$

$$b_{n_j-k} = (-1)^k \sum_{\substack{I \subseteq (s_j, s_{j+1}] \\ |I|=k}} \prod_{i \in I} \alpha_i$$

$$a_{n-s_j-k} = (-1)^{s_j+k} \sum_{\substack{I \subseteq (0, n] \\ |I|=s_j+k}} \prod_{i \in I} \alpha_i$$

where $\beta \in K$ is the sum of all the terms appearing in a_{n-s_j-k} with $I \not\subseteq (0, s_{j+1}]$. This implies that $v(\beta) > n_0 m_1 + n_1 m_2 + \cdots + n_{j-1} m_j + k m_{j+1}$. Since f is a regular polynomial, we have that $v(a_{n-s_j-k}) > n_0 m_1 + n_1 m_2 + \cdots + n_{j-1} m_j + k m_{j+1}$ by the first item in definition D.12, and hence $v(b_{n_j-k}) > k m_{j+1}$. \square

CHAPTER III

ROOT COUNTING

A. Roots of the Reduced Polynomials

Let K be an ultrametric field, so it is complete field with respect to a non-archimedean discrete valuation v . We denote by $A = \{x \in K : v(x) \geq 0\}$ the valuation ring of K , $\mathfrak{M} = \{x \in K : v(x) > 0\}$ the maximal ideal of A , $\pi \in \mathfrak{M}$ a generator of the principal ideal \mathfrak{M} of A and $K_v = A/\mathfrak{M}$ the residue field of K with respect to v . We assume that K_v is finite with q elements and characteristic p and that $v(\pi) = 1$. We also denote by v the unique extension of the valuation of K to its algebraic closure \overline{K} . Consider a monic polynomial $f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0 \in A[X]$. Assume that the discriminant $\Delta = \text{Res}_X(f, f')$ is non-zero and let $r = v(\Delta)$.

Lemma A.1. *For any $\alpha \in \overline{K}$ such that $f(\alpha) = 0$, we have $v(\alpha) \geq 0$.*

Proof. Assume that $v(\alpha) < 0$. Since $f(\alpha) = 0$, we have that

$$\begin{aligned} nv(\alpha) &= v(\alpha^n) = v(a_{n-1}\alpha^{n-1} + \cdots + a_0) \geq \min\{v(a_i\alpha^i) : 0 \leq i < n\} \\ &\geq \min\{v(\alpha^i) : 0 \leq i < n\} = (n-1)v(\alpha) \end{aligned}$$

which implies $v(\alpha) \geq 0$, a contradiction. \square

The following lemma gives a lower bound estimation to the distance between roots in terms of the valuation r of the discriminant.

Lemma A.2. *If $f(X) = \prod_{i=1}^n (X - \alpha_i)$ with $\alpha_i \in \overline{K}$ for $i = 1, \dots, n$, then*

$$v(\alpha_i - \alpha_j) \leq \frac{r}{2} \quad \forall i \neq j.$$

Proof. From the formula of the discriminant $\Delta = \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)^2$ we get $r =$

$2 \sum_{1 \leq i < j \leq n} v(\alpha_i - \alpha_j)$. Since all the roots satisfy $v(\alpha_i) \geq 0$, all the terms in this sum are non-negative. Therefore $v(\alpha_i - \alpha_j)$ can not exceed $r/2$ for any $i \neq j$. \square

Let $f_N \in (A/\pi^N A)[X]$ denote the reduction of the polynomial f modulo π^N . We denote by $\beta_1, \dots, \beta_l \in A$ the roots of f in K (by Lemma A.1 we know that they are in A). It is clear that the reduction of any of these roots modulo π^N is a root of f_N . Unfortunately, the reduction modulo π^N does not give a bijection between the set of roots of f in K and the set of roots of f_N in $A/\pi^N A$ in general. However, we will show that the reduction homomorphism is a bijection between the roots of f and classes of roots of f_N under an equivalence relation. The inverse of the reduction homomorphism is given by a reformulation of the standard Hensel's lemma.

We denote by \bar{x} the reduction modulo $\pi^N A$ of $x \in A$.

Definition A.3. Let $Z_N \subseteq A/\pi^N A$ be the set of roots of f_N . Two roots $x, y \in Z_N$ are in the same equivalence class (denoted by $x \approx y$) if and only if either $x = y$ and $N \leq r$ or $x \equiv y \pmod{\pi^{r+1}}$ and $N > r$. The class containing a root $x \in Z_N$ is written $[x]$ and the set of classes is written Z_N / \approx .

Lemma A.4. If $N > r$ then the number of roots of f in K is not greater than $|Z_N / \approx|$.

Proof. Write $f(X) = (X - \beta_1)(X - \beta_2) \dots (X - \beta_l)g(X)$ where g has no roots in K . Let $\beta_{i,N} = \bar{\beta}_i \in A/\pi^N A$ be the reduction of β_i modulo $\pi^N A$. Since this reduction is a ring homomorphism, $\beta_{i,N}$ is a root of f_N . Take $1 \leq i < j \leq l$. By Lemma A.2, we have $v(\beta_i - \beta_j) \leq r/2 \leq r$, i.e. $\beta_i \not\equiv \beta_j \pmod{\pi^{r+1}}$. Since $N > r$, we also have that $\bar{\beta}_i \not\equiv \bar{\beta}_j \pmod{\pi^{r+1}}$. This implies that $\beta_{i,N} \not\approx \beta_{j,N}$ and hence $[\beta_{i,N}] \neq [\beta_{j,N}]$. \square

Lemma A.5. Let $\gamma \in A$ be such that $v(f(\gamma)) > r$. Then $v(f'(\gamma)) \leq r$.

Proof. Write $\Delta = a(X)f(X) + b(X)f'(X)$ with $a, b \in A[X]$ and evaluate at $X = \gamma$. Since $v(a(\gamma)) \geq 0$, we have that $v(a(\gamma)f(\gamma)) > r$, and therefore $v(b(\gamma)f'(\gamma)) = v(\Delta - a(\gamma)f(\gamma)) = r$. We conclude that $v(f'(\gamma)) \leq r$ because $v(b(\gamma)) \geq 0$. \square

Lemma A.6. *If $N > 2r$ then the number of roots of f in K is not less than $|Z_N/\approx|$.*

Proof. Take $[\beta] \in Z_N/\approx$ and take some $\gamma \in A$ such that $\beta = \bar{\gamma}$. Since $\overline{f(\gamma)} = f_N(\beta) = \bar{0}$, we have that $v(f(\gamma)) \geq N > 2r \geq r$. By Lemma A.5 we have that $v(f'(\gamma)) \leq r$ and then $v(f(\gamma)/f'(\gamma)^2) > 0$. By Hensel's lemma, there exists $\xi \in A$ such that $f(\xi) = 0$ and $\xi \equiv \gamma \pmod{\pi^{N-r}}$ because $v(f(\gamma)/f'(\gamma)) \geq N - r$. Since $N - r > r$ we have that $\xi \equiv \gamma \pmod{\pi^{r+1}}$ and also $\bar{\xi} \equiv \bar{\gamma} \pmod{\bar{\pi}^{r+1}}$ because $N > r$. This means that $[\beta] = [\bar{\xi}]$.

Note that if ξ and ξ' are two different roots of f in A , then $v(\xi - \xi') \leq r/2 \leq r$ by Lemma A.2. This implies that $\xi \not\equiv \xi' \pmod{\pi^{r+1}}$, $\bar{\xi} \not\equiv \bar{\xi}' \pmod{\bar{\pi}^{r+1}}$ and $[\bar{\xi}] \neq [\bar{\xi}']$. We conclude from here that the procedure described above gives a well defined map from the set Z_N/\approx to the set of roots of f in K (we can not lift the same class to two different roots). Moreover, this map is injective, because it is possible to reconstruct the equivalence class from the lifted root. \square

As an immediate consequence of Lemmas A.4 and A.6, we obtain a bijection between the number of roots of f in K and the number of equivalence classes. The following theorem is the main result of this section.

Theorem A.7. *For any $N > 2r$, the number of roots of f in K is equal to $|Z_N/\approx|$. More precisely, the map $x \mapsto [\bar{x}]$ is a bijection between the set of roots of f in A (or in K) and Z_N/\approx .*

Corollary A.8. *Let $g = X^n + b_{n-1}X^{n-1} + \dots + b_0 \in A[X]$ be a polynomial such that $v(a_i - b_i) > 2r$. Then f and g have the same number of roots in K .*

Proof. Since $a_i \equiv b_i \pmod{p^{2r+1}}$, then

$$\text{Res}_X(g, g') \equiv \text{Res}_X(f, f') \equiv \Delta \pmod{p^{2r+1}}.$$

Therefore the discriminant of g has also valuation r . We conclude by applying Theorem A.7 to f and g with $N = 2r + 1$. \square

B. Counting Roots of Regular Polynomials

Corollary B.1. *If $r = 0$ then the number of roots of f in K^\times is equal to the number of roots of f_1 in K_v^\times where f_1 is the reduction of f modulo πA .*

Lemma B.2. *If $f(X) = X^n + a_0$ then the discriminant of f is*

$$\Delta(f) = (-1)^{n(n-1)/2} n^n a_0^{n-1}.$$

Proof. Write $f(X) = X^n + a_0 = \prod_{i=1}^n (X - \alpha_i)$ with $\alpha_i \in \overline{K}$. Then

$$\begin{aligned} \Delta(f) &= (-1)^{n(n-1)/2} \text{Res}(f, f') = (-1)^{n(n-1)/2} \prod_{i=1}^n f'(\alpha_i) \\ &= (-1)^{n(n-1)/2} \prod_{i=1}^n n \alpha_i^{n-1} = (-1)^{n(n-1)/2} n^n \left(\prod_{i=1}^n \alpha_i \right)^{n-1} \\ &= (-1)^{n(n-1)/2} n^n (-1)^{n(n-1)} a_0^{n-1} = (-1)^{n(n-1)/2} n^n a_0^{n-1}. \end{aligned}$$

\square

Lemma B.3. *If $g(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0 \in A[X]$ satisfies $v(a_0) = 0$, $v(a_i) > 0$ for all $1 \leq i < n$ and $p \nmid n$ then the number of roots of g in K^\times is equal to the number of roots of the lower binomial $X^n + a_0$ of g in K^\times .*

Proof. By Lemma B.2, the discriminant of $X^n + a_0$ has valuation 0. On the other hand, the polynomial g satisfies the hypothesis of Corollary A.8 with respect to $f = X^n + a_0$. Then both g and its lower binomial f have the same number of roots in K . \square

Definition B.4. Let $a \in K^\times$ be an element with valuation $v(a) = l$. The first digit of a is $\delta(a) = \overline{a/\pi^l} \in K_v^\times$.

The following result gives a procedure to count the number of roots of a regular polynomial when its Newton polygon consists of only one line segment.

Theorem B.5. Let $f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0 \in A[X]$ with $p \nmid n$ and $a_0 \neq 0$. Write $l = v(a_0)$ and assume that $v(a_{n-i}) > il/n$ for all $i = 1, \dots, n-1$. Then the number R of roots of f in K^\times is equal to the number of roots of the lower binomial $X^n + a_0$ in K^\times . Moreover, if $n \nmid l$ we have $R = 0$, and if $n|l$ then

$$R = \begin{cases} \gcd(n, q-1) & \text{if } -\delta(a_0) \text{ is an } n^{\text{th}} \text{ power in } K_v, \\ 0 & \text{otherwise.} \end{cases}$$

Proof. By Theorem D.2, all the roots of both f and $\tilde{f} = X^n + a_0$ have valuation $e = l/n$. It is clear that if $n \nmid l$, then neither f nor \tilde{f} have a root in K , because all the elements in K have integer valuation. Therefore, we only need to consider the case $n|l$.

Define $h(X) = \pi^{-l}f(\pi^e X)$. It is clear that f and h have the same number of roots in K . Our assumptions on the coefficients of f guarantee that h is a monic polynomial in $A[X]$. Moreover, if $h = X^n + b_{n-1}X^{n-1} + \cdots + b_0$, then $v(b_0) = 0$ and $v(b_{n-i}) > 0$ for all $1 \leq i < n$. By Lemma B.3, the number of roots of h in K coincides with the number of roots of its lower binomial $\tilde{h} = X^n + \pi^{-l}a_0$ in K . Since $\tilde{h}(X) = \pi^{-l}\tilde{f}(\pi^e X)$, then \tilde{f} and \tilde{h} have the same number of roots in K . We conclude that f , \tilde{f} , h and \tilde{h} have all the same number R of roots in K .

It only remains to prove the formula for R . By Lemma B.2, the discriminant of \tilde{h} has valuation 0 (since $p \nmid n$ and $v(b_0) = 0$). Therefore, by Corollary B.1, the number of roots R of \tilde{h} in K equals the number of roots in K_v of the reduction $\tilde{h}_1 = X^n + \delta(a_0)$

of \tilde{h} modulo \mathfrak{M} . If $-\delta(a_0)$ is not an n^{th} power in K_v , then \tilde{h} has no roots. Otherwise, the number of roots of \tilde{h} in K_v coincides with the number of n^{th} roots of the unity in K_v . Since K_v^\times is a cyclic group with $q - 1$ elements, $R = \gcd(q - 1, n)$ in this case. \square

Theorem B.6. *Let $f = a_n X^n + \cdots + a_0 \in K[X]$ be a regular polynomial. Then the number of roots of f in K^\times is equal to the sum of the number of roots in K^\times of all its lower binomials.*

Proof. By Theorem D.2, we can write $f = a_n \prod_{j=0}^t f_j$ where $f_0, \dots, f_t \in K[X]$ are monic polynomials and all the roots of each f_j have the same valuation m_{j+1} . Here $t + 1$ is the number of segments of the Newton polygon of f and $-m_1 > \cdots > -m_{t+1}$ are the slopes of these segments. Following the notation of Theorem D.4 we define $n_{j+1} = \deg(f_j)$ and $s_j = |\{\alpha \in \overline{K} : f(\alpha) = 0 \text{ and } v(\alpha) \leq m_j\}|$. Setting $s_0 = 0$ we have $n_j = s_{j+1} - s_j$. The lower binomials of f are the polynomials $g_j = a_{n-s_j} X^{n-s_j} + a_{n-s_{j+1}} X^{n-s_{j+1}}$. Let R and R_j denote the number of roots in K^\times of f and f_j respectively. It is clear that $R = R_0 + \cdots + R_t$. By Theorem D.4 the polynomials f_j are regular, and then, by Theorem B.5 its number R_j of roots in K^\times depends only on its degree and the first digit of its constant term. In order to conclude we only need to proof that R_j coincides with the number of roots of g_j in K^\times . The number of roots of the lower binomial $g_j = a_{n-s_j} X^{n-s_{j+1}} (X^{s_{j+1}-s_j} + a_{n-s_{j+1}}/a_{n-s_j})$ in K^\times coincide with the number of roots of the regular monic polynomial $X^{s_{j+1}-s_j} + a_{n-s_{j+1}}/a_{n-s_j}$ in K^\times . The degree of this polynomial is $n_j = \deg(f_j)$ and by the equation 3.1 (with $k = n_j$) in the proof of Theorem D.4, the first digit of $a_{n-s_{j+1}}/a_{n-s_j}$ is equal to the first digit of the constant term of f_j . Therefore R_j is also the number of roots of g_j in K^\times . \square

C. Tropical Varieties

Throughout this section we assume that K is an ultrametric field, but the results of the section are still hold for any non-archimedean field. For the following two section, we need the fact that the field K is complete and its residue field is finite. Recall $A = \{x \in K : v(x) \geq 0\}$ is the valuation ring of K and $\mathfrak{M} = \{x \in K : v(x) > 0\}$ is the maximal ideal of A . Again we denote by $K_v = A/\mathfrak{M}$ the residue field of K with respect to its valuation v . We assume that v is normalized, i.e. $\mathfrak{M} = \langle \pi \rangle$ where $\pi \in A$ has $v(\pi) = 1$. For any $x \in K^\times$, we denote by $\delta(x) = \pi^{-v(x)}x \pmod{\mathfrak{M}}$ the first digit of x .

Definition C.1. Let $f = \sum_{i=1}^t a_i X^{\alpha_i} \in K[X_1^{\pm 1}, \dots, X_n^{\pm 1}]$ be a polynomial with t terms where $a_i \in K^\times$ and $\alpha_i = (\alpha_{i1}, \dots, \alpha_{in}) \in \mathbb{Z}^n$ for all $i = 1, \dots, t$. We define

- $l_i(f; w) = v(a_i) + \alpha_i \cdot w, \quad w \in \mathbb{R}^n$
- $H_i(f) = \{(w, h) : h = l_i(f; w)\} \subseteq \mathbb{R}^{n+1}$
- $L_{ij}(f) = H_i(f) \cap H_j(f)$
- $L_{ij}^*(f) = \{(w, h) \in L_{ij}(f) : h \leq l_k(f; w) \forall k\}$
- $L(f) = \bigcup_{1 \leq i < j \leq t} L_{ij}^*(f)$
- $\text{Trop}(f) = \text{proj}(L(f)) \subseteq \mathbb{R}^n$

where $\text{proj} : \mathbb{R}^{n+1} \rightarrow \mathbb{R}^n$ represents the projection to the first n coordinates. The set $\text{Trop}(f)$ is called the torpical variety of f .

If we define the half space $H_i^+(f) = \{(w, h) : h \leq l_i(f; w)\} \subseteq \mathbb{R}^{n+1}$ and let $P(f)$ be the polyhedron define by

$$P(f) = \bigcup_{i=1}^n H_i^+(f)$$

Then $\text{Trop}(f)$ is the projection of the *corner set*, $L(f)$, of the upper hull of $P(f)$. To illustrate the above definition, consider the following example.

Example:

Let $K = \mathbb{Q}_3$ and $f(X) = X^2Y^2 + 9XY^2 + 5X + 3 \in \mathbb{Q}_3[X, Y]$. The for any $w = (w_1, w_2) \in \mathbb{R}^2$, we have:

$$l_1(f; w) = 2w_1 + 2w_2.$$

$$l_2(f; w) = 2 + w_1 + 2w_2.$$

$$l_3(f; w) = w_1.$$

$$l_4(f; w) = 1.$$

In order to compute the tropical variety, $\text{Trop}(f)$, of f , we need to find $L_{12}^*, L_{13}^*, L_{14}^*, L_{23}^*, L_{24}^*$ and L_{34}^* .

$$L_{12} = \{(w_1, w_2, h) : h = 2w_1 + 2w_2 = 2 + w_1 + 2w_2\} = \{(2, w_2, 4 + 2w_2)\}.$$

$$L_{12}^* = \{(2, w_2, 4 + 2w_2) : w_2 \leq -3/2\}.$$

$$L_{13} = \{(w_1, w_2, h) : h = 2w_1 + 2w_2 = w_1\} = \{(-2w_2, w_2, -2w_2)\}.$$

$$L_{13}^* = \{(-2w_2, w_2, -2w_2) : w_2 \geq -1/2\}.$$

$$L_{14} = \{(w_1, w_2, h) : h = 2w_1 + 2w_2 = 1\} = \{(1/2 - w_2, w_2, 1)\}.$$

$$L_{14}^* = \{(1/2 - w_2, w_2, 1) : -3/2 \leq w_2 \leq -1/2\}.$$

$$L_{23} = \{(w_1, w_2, h) : h = 2 + w_1 + 2w_2 = w_1\} = \{(w_1, -1, w_1)\}.$$

$$L_{23}^* = \{(w_1, -1, w_1) : w_1 \geq 2, w_1 \leq 1\} = \phi.$$

$$L_{24} = \{(w_1, w_2, h) : h = 2 + w_1 + 2w_2 = 1\} = \{(-1 - 2w_2, w_2, 1)\}.$$

$$L_{24}^* = \{(-1 - 2w_2, w_2, 1) : w_2 \leq -3/2\}.$$

$$L_{34} = \{(w_1, w_2, h) : h = w_1 = 1\} = \{(1, w_2, 1)\}.$$

$$L_{34}^* = \{(1, w_2, 1) : w_2 \geq -1/2\}.$$

Therefore,

$$\begin{aligned}
 \text{Trop}(f) &= \text{proj}(L_{12}^* \cup L_{13}^* \cup L_{14}^* \cup L_{23}^* \cup L_{32}^* \cup L_{34}^*) \\
 &= \{(2, w_2) : w_2 \leq -3/2\} \cup \{(-2w_2, w_2) : w_2 \geq -1/2\} \\
 &\cup \{(1/2 - w_2, w_2) : -3/2 \leq w_2 \leq -1/2\} \\
 &\cup \{(-1 - 2w_2, w_2) : w_2 \leq -3/2\} \\
 &\cup \{(1, w_2) : w_2 \geq -1/2\}.
 \end{aligned}$$

See Fig. 2.

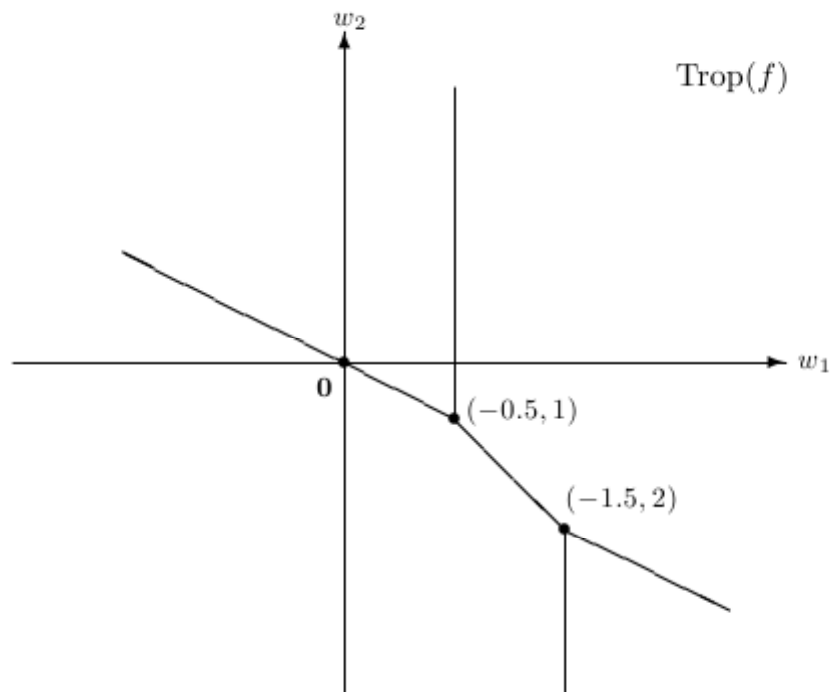


Fig. 2. The tropical variety of $X^2Y^2 + 9XY^2 + 5X + 3$

The following lemma characterizes the points in the tropical variety and it coincides with the more standard definition of tropical variety.

Lemma C.2. *Let $f \in K[X_1^{\pm 1}, \dots, X_n^{\pm 1}]$ be a polynomial with t terms and $w \in \mathbb{R}^n$. Then $w \in \text{Trop}(f)$ if and only if there are two indices $1 \leq i < j \leq t$ such that $l_i(f; w) = l_j(f; w) \leq l_k(f; w)$ for all $k = 1, \dots, t$.*

Proof. Assume that there are $1 \leq i < j \leq t$ such that $h = l_i(f; w) = l_j(f; w) \leq l_k(f; w)$ for all $k = 1, \dots, t$. Therefore the point (w, h) is in $L_{ij}^*(f) \subseteq L(f)$ and $w \in \text{proj}(L(f)) = \text{Trop}(f)$. Conversely, if $w \in \text{Trop}(f)$, there exists $h \in \mathbb{R}$ such that $(w, h) \in L(f) = \bigcup_{1 \leq i < j \leq t} L_{ij}^*(f)$. This implies that for some $1 \leq i < j \leq t$ we have $(w, h) \in L_{ij}^*(f)$. For these indices we have, by definition, $h = l_i(f; w) = l_j(f; w) \leq l_k(f; w)$ for all $k = 1, \dots, t$. \square

Note that for any $x \in (K^\times)^n$, the valuation of the i -th term of f at x is given by $l_i(f; v(x))$. The following proposition states an important fact that the tropical variety contains the valuations of the roots of the polynomial.

Proposition C.3. *Let $f \in K[X_1^{\pm 1}, \dots, X_n^{\pm 1}]$ and $x \in (K^\times)^n$ be a zero of f , then $v(x) \in \text{Trop}(f)$.*

Proof. Sort all the t monomials of f according to their valuation at x

$$l_{i_1}(f; v(x)) \leq l_{i_2}(f; v(x)) \leq \dots \leq l_{i_t}(f; v(x)).$$

Since the sum of all the monomials at x is zero, the first two valuations in this list must coincide. We conclude from Lemma C.2 that $w \in \text{Trop}(f)$. \square

Lemma C.4. *Let $f \in K[X_1^{\pm 1}, \dots, X_n^{\pm 1}]$, $a, b_1, \dots, b_n \in K^\times$ and $\alpha \in \mathbb{Z}^n$. Then we have*

1. $\text{Trop}(aX^\alpha f) = \text{Trop}(f)$
2. $\text{Trop}(f(b_1X_1, \dots, b_nX_n)) = \text{Trop}(f) - (v(b_1), \dots, v(b_n))$.

Proof. It is clear, by the symmetry of the statements, that in both cases it is enough to prove only the inclusion (\subseteq). Let t be the number of monomials of the polynomial f .

1. Let $w \in \text{Trop}(aX^\alpha f)$. Note that $l_i(aX^\alpha f; w) = v(a) + \alpha \cdot w + l_i(f; w)$. By Lemma C.2, there are two indices $1 \leq i < j \leq t$ such that $l_i(aX^\alpha f; w) = l_j(aX^\alpha f; w) \leq l_k(aX^\alpha f; w)$ for all $k = 1, \dots, t$. Subtracting $v(a) + \alpha \cdot w$ to all the terms in this inequality, we conclude that $l_i(f; w) = l_j(f; w) \leq l_k(f; w)$ for all $k = 1, \dots, t$. Therefore, by Lemma C.2, we have $w \in \text{Trop}(f)$.
2. Let $g = f(b_1X_1, \dots, b_nX_n)$, $b = (b_1, \dots, b_n)$ and $w \in \text{Trop}(g)$. Note that $l_i(g; w) = l_i(f; w) + \alpha_i \cdot v(b) = l_i(f; w + v(b))$. By Lemma C.2, there are two indices $1 \leq i < j \leq t$ such that $l_i(g; w) = l_j(g; w) \leq l_k(g; w)$ for all $k = 1, \dots, t$. This implies, by Lemma C.2, that $v(b) + w \in \text{Trop}(f)$. \square

Lemma C.5. *Let $f \in K[X_1^{\pm 1}, \dots, X_n^{\pm 1}]$. For any $w \in \text{Trop}(f)$ there exists a unique $h \in \mathbb{R}$ such that $(w, h) \in L(f)$. Moreover, h is given by $h = \min\{l_k(f; w) : 1 \leq k \leq t\}$.*

Proof. Since $w \in \text{Trop}(f) = \text{proj}(L(f))$, then there exists $h \in \mathbb{R}$ such that $(w, h) \in L$. The point (w, h) is in some $L_{ij}^*(f)$. This means that $h = l_i(f; w) = l_j(f; w) \leq l_k(f; w)$ for all $k = 1, \dots, t$. In particular $h = \min\{l_k(f; w) : 1 \leq k \leq t\}$. This proves the uniqueness and the formula of h . \square

Definition C.6. *Let $f \in K[X_1^{\pm 1}, \dots, X_n^{\pm 1}]$ be the polynomial $f = \sum_{i=1}^t a_i X^{\alpha_i}$ and $w \in \text{Trop}(f)$. We define $h(f; w)$ to be the unique $h \in \mathbb{R}$ provided by Lemma C.5 i.e.*

$$h(f; w) = \min\{l_k(f; w) : 1 \leq k \leq t\}.$$

We also define the lower polynomial $f^{[w]}$ of f with respect to the valuation vector $w \in \text{Trop}(f)$ by

$$f^{[w]} = \sum_{i: l_i(f; w) = h(f; w)} a_i X^{\alpha_i}.$$

Lemma C.7. *Let $f \in K[X_1^{\pm 1}, \dots, X_n^{\pm 1}]$. Let $a \in K^\times$, $b = (b_1, \dots, b_n) \in (K^\times)^n$ and $\alpha \in \mathbb{Z}^n$. For any $w \in \text{Trop}(f)$ we have:*

1. $h(aX^\alpha f; w) = h(f; w) + v(a) + \alpha \cdot w$.
2. $(aX^\alpha f)^{[w]} = aX^\alpha f^{[w]}$.
3. $h(f(b_1X_1, \dots, b_nX_n); w) = h(f; w + v(b))$.
4. $f(b_1X_1, \dots, b_nX_n)^{[w]} = f^{[w+v(b)]}(b_1X_1, \dots, b_nX_n)$.

Proof. 1. It follows immediately from the identity

$$l_i(aX^\alpha f; w) = l_i(f; w) + v(a) + \alpha \cdot w.$$

2. By definition of lower polynomials, the indices of the monomials of f that are in $(aX^\alpha f)^{[w]}$ correspond with the indices that minimize the value of $l_i(aX^\alpha f; w)$. Since $v(a) + \alpha \cdot w$ is a constant, these indices also minimize $l_i(f; w)$, i.e. they correspond to the monomials of f in $f^{[w]}$. Therefore $(aX^\alpha f)^{[w]} = aX^\alpha f^{[w]}$.

3. It follows immediately from the identity

$$l_i(f(b_1X_1, \dots, b_nX_n); w) = l_i(f; w + v(b)).$$

4. The indices of the monomials of f that are in $f(b_1X_1, \dots, b_nX_n)^{[w]}$ minimize the expression $l_i(f(b_1X_1, \dots, b_nX_n); w)$. These are the same indices that we have in $f^{[w+v(b)]}(b_1X_1, \dots, b_nX_n)$. Therefore $f(b_1X_1, \dots, b_nX_n)^{[w]} = f^{[w+v(b)]}(b_1X_1, \dots, b_nX_n)$.

□

Lemma C.8. *Let $f \in K[X_1^{\pm 1}, \dots, X_n^{\pm 1}]$ and $w' \in \text{Trop}(f^{[w]})$. Then the ray $w + \lambda(w' - w)$ with $\lambda \geq 0$ is contained in $\text{Trop}(f^{[w]})$. In particular, the tropical variety $\text{Trop}(f^{[w]})$ is a cone centered at w .*

Proof. Let t be the number of non-zero terms of f . We know that $f^{[w]} = a_{i_1}X^{\alpha_{i_1}} + \dots +$

$a_{i_r} X^{\alpha_{i_r}}$ where $1 \leq i_1 < i_2 < \dots < i_r \leq t$ are all the indices that minimize the linear function $l_i(f; w)$. In particular $l_{i_k}(f^{[w]}; w) = l_{i_k}(f; w) = h(f; w)$ for all $k = 1, \dots, r$. Since $w' \in \text{Trop}(f^{[w]})$ we have, by Lemma C.2, two indices $1 \leq n < m \leq r$ such that $l_n(f^{[w]}; w') = l_m(f^{[w]}; w') \leq l_k(f^{[w]}; w')$ for all $k = 1, \dots, r$. Subtracting $h(f; w)$, multiplying by $\lambda \geq 0$ and then adding $h(f; w)$ to these inequalities we get

$$\begin{aligned} l_n(f^{[w]}; w + \lambda(w' - w)) &= l_m(f^{[w]}; w + \lambda(w' - w)) \\ &\leq l_k(f^{[w]}; w + \lambda(w' - w)) \end{aligned}$$

for all $k = 1, \dots, r$. This implies, by Lemma C.2, that $w + \lambda(w' - w)$ is in $\text{Trop}(f^{[w]})$. \square

Lemma C.9. *Let $f \in K[X_1^{\pm 1}, \dots, X_n^{\pm 1}]$ and $w \in \text{Trop}(f)$. Then there exists $\varepsilon > 0$ such that $\text{Trop}(f) \cap B_\varepsilon(w) = \text{Trop}(f^{[w]}) \cap B_\varepsilon(w)$.*

Proof. Let t be the number of terms of f . Let $I = \{1 \leq i \leq t : l_i(f; w) = h(f; w)\}$ be the set of indices of monomials of f in $f^{[w]}$. Note that $l_i(f; w) < l_k(f; w)$ for all $i \in I$ and $k \notin I$. Since the functions $l_i(f; \cdot) : \mathbb{R}^n \rightarrow \mathbb{R}$ are continuous, there exists $\varepsilon > 0$ such that

$$l_i(f; w') < l_k(f; w') \quad \forall w' \in B_\varepsilon(w), \forall i \in I, \forall k \notin I. \quad (3.1)$$

Take $w' \in \text{Trop}(f) \cap B_\varepsilon(w)$. By Lemma C.2, there are two indices $1 \leq i < j \leq t$ such that $l_i(f; w') = l_j(f; w') \leq l_k(f; w')$ for all $k = 1, \dots, t$. By the inequalities (3.1), we conclude that $i, j \in I$. Therefore, by Lemma C.2, $w' \in \text{Trop}(f^{[w]})$.

Now take $w' \in \text{Trop}(f^{[w]}) \cap B_\varepsilon(w)$. By Lemma C.2 we have two different indices $i, j \in I$ such that $l_i(f; w') = l_j(f; w') \leq l_k(f; w')$ for all $k \in I$. By (3.1), this inequality holds also for $k \notin I$. This means, by Lemma C.2, that $w' \in \text{Trop}(f)$. \square

D. Multivariate Root Counting

1. Semiregular Polynomial Systems

Definition D.1. *Consider a system*

$$F = \begin{cases} f_1(X_1, \dots, X_n) = 0 \\ \vdots \\ f_n(X_1, \dots, X_n) = 0 \end{cases}$$

of n equations in n variables and the equations are given by polynomials in $K[X_1^{\pm 1}, \dots, X_n^{\pm 1}]$.

We define the tropical set $S(F) = \text{Trop}(f_1) \cap \text{Trop}(f_2) \cap \dots \cap \text{Trop}(f_n)$. For any $w \in S(F)$ we denote by $F^{[w]}$ to the system of equations given by the lower polynomials $f_1^{[w]}, \dots, f_n^{[w]}$.

By Proposition C.3, any solution $x \in (K^\times)^n$ of F satisfies $v(x) \in S(F)$. In other words, the tropical set contains the valuations of the roots of the system.

Lemma D.2. *Let F be a system of n equations in $K[X_1^{\pm 1}, \dots, X_n^{\pm 1}]$. If w is an isolated point of $S(F)$, then $S(F^{[w]}) = \{w\}$ and all the solutions $x \in (K^\times)^n$ of $F^{[w]}$ have valuation vector $v(x) = w$.*

Proof. By Lemma C.9, the tropical sets $S(F)$ and $S(F^{[w]})$ coincide in a neighborhood of w . In particular, there exists $\varepsilon > 0$ such that $S(F^{[w]}) \cap B_\varepsilon(w) = \{w\}$. On the other hand, by Lemma C.8, the tropical set $S(F^{[w]})$ is a cone centered at w . This implies that $S(F^{[w]}) = \{w\}$. Therefore, by Lemma C.3, all the solutions of $F^{[w]}$ have valuation vector $v(x) = w$. \square

Lemma D.3. *Let $F \in (K[X_1^{\pm 1}, \dots, X_n^{\pm 1}])^n$ be a polynomial system in K and $w \in S(F)$. Let JF denote the Jacobian of F , more precisely,*

$$JF = \det(\partial f_i / \partial X_j)_{1 \leq i, j \leq n}.$$

For any $x \in (K^\times)^n$ with $F(x) = 0$ and $v(x) = w$, we have

$$v(JF(x)) \geq h(f_1; w) + \cdots + h(f_n; w) - (w_1 + \cdots + w_n).$$

Proof. The result follows easily from the following claim.

claim: $v\left(\frac{\partial f_i}{\partial X_j}(x)\right) \geq h(f_i; w) - w_j$.

proof of claim: Write $f_i = \sum_{k=0}^m a_k X^{\alpha_k}$, then

$$\frac{\partial f_i}{\partial X_j} = \sum_{k=1}^m a_k \alpha_k^j X^{\alpha_k - e_j}$$

where e_j is the standard basis vector of \mathbb{R}^n and $\alpha_k = (\alpha_k^1, \dots, \alpha_k^n)$. Hence,

$$\begin{aligned} v\left(\frac{\partial f_i}{\partial X_j}(x)\right) &\geq \min_k \{v(a_k \alpha_k^j) + (\alpha_k - e_j) \cdot w\} \\ &\geq \min_k \{(v(a_k) + \alpha_k \cdot w) - w_j\} \quad (\text{since } \alpha_k^j \in \mathbb{Z}) \\ &= h(f_i; w) - w_j. \end{aligned}$$

That proves the claim.

Now,

$$\begin{aligned} v(JF(x)) &= v\left(\sum_{\sigma} (-1)^{|\sigma|} \frac{\partial f_1}{\partial X_{\sigma(1)}}(x) \cdots \frac{\partial f_n}{\partial X_{\sigma(n)}}(x)\right) \\ &\geq \min_{\sigma} \left\{v\left(\frac{\partial f_1}{\partial X_{\sigma(1)}}(x)\right) + \cdots + v\left(\frac{\partial f_n}{\partial X_{\sigma(n)}}(x)\right)\right\} \\ &\geq \min_{\sigma} \left\{(h(f_1; w) - w_{\sigma(1)}) + \cdots + (h(f_n; w) - w_{\sigma(n)})\right\} \\ &= h(f_1; w) + \cdots + h(f_n; w) - (w_1 + \cdots + w_n). \end{aligned}$$

□

Definition D.4. Let $F = \{f_1 = \cdots = f_n = 0\}$ be a system of n equations in

$K[X_1^{\pm 1}, \dots, X_n^{\pm 1}]$. We say that F is semiregular at $w = (w_1, \dots, w_n)$ if

$$v(JF(x)) = h(f_1; w) + \dots + h(f_n; w) - (w_1 + \dots + w_n)$$

for any zero $x \in (K^\times)^n$ of F with valuation vector $v(x) = w$. We say that F is normalized at w if $h(f_1; w) = \dots = h(f_n; w) = 0$.

Lemma D.5. *Let $F = \{f_1 = \dots = f_n = 0\}$ be a system of n equations in $K[X_1^{\pm 1}, \dots, X_n^{\pm 1}]$. Let $a_1, \dots, a_n \in K^\times$, $\alpha_1, \dots, \alpha_n \in \mathbb{Z}^n$ and $w \in S(F)$. Then F is semiregular at w if and only if the system $\tilde{F} = \{a_1 X^{\alpha_1} f_1 = \dots = a_n X^{\alpha_n} f_n = 0\}$ is semiregular at w .*

Proof. It is clear that F and \tilde{F} have the same solutions in $(K^\times)^n$. On the other hand, by the item (1) in Lemma C.7, we have $h(a_i X^{\alpha_i} f_i; w) = h(f_i; w) + v(a_i) + \alpha_i \cdot w$ for all $i = 1, \dots, n$. Therefore, it is enough to show that for any zero $x \in (K^\times)^n$ of F with $v(x) = w$, we have

$$v(J\tilde{F}(x)) = v(JF(x)) + \sum_{i=1}^n (v(a_i) + \alpha_i \cdot w).$$

This identity is an immediate consequence of the fact that

$$J\tilde{F}(x) = a_1 x^{\alpha_1} \dots a_n x^{\alpha_n} JF(x)$$

for any zero $x \in (K^\times)^n$ of F . This expression can be derived from the product rule for derivatives and the multilinearity of the determinant. \square

Lemma D.6. *Let $F = \{f_1 = \dots = f_n = 0\}$ be a system of n equations in $K[X_1^{\pm 1}, \dots, X_n^{\pm 1}]$. Let $b = (b_1, \dots, b_n) \in (K^\times)^n$ and $w \in S(F)$. Then F is semiregular at w if and only if the system $\tilde{F} = \{f_1(b_1 X_1, \dots, b_n X_n) = \dots = f_n(b_1 X_1, \dots, b_n X_n) = 0\}$ is semiregular at $w - v(b)$.*

Proof. By the item (3) in Lemma C.7, we have $h(f_i(b_1 X_1, \dots, b_n X_n); w - v(b)) =$

$h(f_i; w)$ for all $i = 1, \dots, n$. Therefore, it is enough to show that

$$v(J\tilde{F}(x)) - v(b_1) - \dots - v(b_n) = v(JF(b_1x_1, \dots, b_nx_n))$$

for all zero $x = (x_1, \dots, x_n) \in (K^\times)^n$ of \tilde{F} with valuation $v(x) = w$. This identity is an immediate consequence of the fact that

$$J\tilde{F}(x) = b_1 \cdots b_n JF(b_1x_1, \dots, b_nx_n)$$

for all $x \in (K^\times)^n$. This expression can be easily derived from the chain rule and the multilinearity of the determinant. \square

In order to proceed, we need a multivariate version of Hensel's lemma.

Lemma D.7 (Hensel). *Let F be a system of n equations in $A[X_1^{\pm 1}, \dots, X_n^{\pm 1}]$ and denote by \bar{F} to the system reduced modulo \mathfrak{M} . Let $\bar{x} \in (K_v^\times)^n$ be a solution of \bar{F} such that $J\bar{F}(\bar{x}) \neq 0$. Then there exists a unique solution $x \in (A \setminus \mathfrak{M})^n$ of F such that $\bar{x} \equiv x \pmod{\mathfrak{M}}$.*

Proof. We are going to construct a sequence $x^{(k)} \in A^n$ which satisfies the following three conditions:

- 1- $x^{(1)} \equiv \bar{x} \pmod{\mathfrak{M}}$.
- 2- $x^{(k+1)} \equiv x^{(k)} \pmod{\mathfrak{M}^k} \quad \forall k \geq 1$.
- 3- $F(x^{(k)}) \equiv 0 \pmod{\mathfrak{M}^k} \quad \forall k \geq 1$.

The sequence $x^{(k)}$ is a Cauchy sequence (by condition 2) and by the completeness of K , it converges to a limit $x \in A^n$ since A^n is a closed subset. Therefore $F(x) = 0$ since $F(x^{(k)}) \rightarrow 0$ as $k \rightarrow \infty$ by condition 3. Note that $x \in (A \setminus \mathfrak{M})^n$ since $0 \neq \bar{x} \equiv x^{(1)} \equiv x^{(k)} \equiv x \pmod{\mathfrak{M}}$.

Now let's construct the sequence $x^{(k)}$ inductively. Let $x^{(1)} \in A^n$ be any element such that $x^{(1)} \equiv \bar{x} \pmod{\mathfrak{M}}$. Assume we have $x^{(1)}, x^{(2)}, \dots, x^{(k)} \in A^n$ satisfy the conditions

1, 2 and 3. Define $x^{(k+1)} = x^{(k)} + \pi^k \Delta_k$ for some $\Delta_k \in A^n$ and by condition 3, we can write $F(x^{(k)}) = \pi^k \delta_k$ for some $\delta_k \in A^n$. Hence

$$\begin{aligned} F(x^{(k+1)}) &= F(x^{(k)} + \pi^k \Delta_k) \\ &= F(x^{(k)}) + DF(x^{(k)})\pi^k \Delta_k + O(\pi^{2k}) \\ &= \pi^k (\delta_k + DF(x^{(k)})\Delta_k) + O(\pi^{2k}). \end{aligned}$$

If we choose $\Delta_k = -DF(x^{(k)})^{-1}\delta_k$, then $x^{(k+1)}$ satisfies the conditions 2 and 3. Hence our construction of the sequence $x^{(k)}$ proves the existence of the root x .

To show uniqueness, we assume there are two solutions $x, y \in A^n$, hence $F(x) = F(y) = 0$ and $x \equiv y \equiv \bar{x} \pmod{\mathfrak{M}}$.

claim: $x \equiv y \pmod{\mathfrak{M}^k} \quad \forall k \geq 1$.

proof of claim: by induction. The statement is obviously true for $k = 1$. Assume it is true for k , i.e. $x \equiv y \pmod{\mathfrak{M}^k}$. Write $y = x + \pi^k \phi$ for some $\phi \in A^n$. Then we have

$$F(y) = F(x) + DF(x)\pi^k \phi + O(\pi^{2k}).$$

The above equation implies $DF(x)\pi^k \phi \equiv 0 \pmod{\mathfrak{M}^{k+1}}$ which means $DF(x)\phi \equiv 0 \pmod{\mathfrak{M}}$. Therefore $\overline{DF(x)\phi} = 0$ in $(K_v)^n$, i.e. $\bar{\phi} = 0$ and this shows $y \equiv x \pmod{\mathfrak{M}^{k+1}}$, proving the claim. \square

Lemma D.8. *Let F be a system of n equations in $K[X_1^{\pm 1}, \dots, X_n^{\pm 1}]$ such that $0 \in S(F)$. Assume also that F is normalized and semiregular at 0. Then all the coefficients of F are in the valuation ring A . Moreover, the reduction map $\pmod{\mathfrak{M}} : A \rightarrow K_v$ is a bijection between the set of zeros of F with in $(K^\times)^n$ with valuation vector 0 (i.e. in $(A \setminus \mathfrak{M})^n$) and the set of zeros of \bar{F} in $(K_v^\times)^n$.*

Proof. Suppose that $F = \{f_1 = \dots = f_n = 0\}$. Since the system is normalized at 0, we have $h(f_i; 0) = 0$ for all $i = 1, \dots, n$. Since $h(f_i; 0)$ is the minimum valuation of

the coefficients of f_i , by Definition C.6 with $w = 0$, then all the coefficients of f_i have valuation at least 0, i.e. $f_i \in A[X_1^{\pm 1}, \dots, X_n^{\pm 1}]$. It is also clear that the reduction of any solution $x \in (K^\times)^n$ (with valuation vector $v(x) = 0$) of F modulo \mathfrak{M} is a zero $\bar{x} \equiv x \pmod{\mathfrak{M}}$ of \bar{F} in $(K_v^\times)^n$. Moreover, the semiregularity of F at 0 says, by Definition D.4, that $v(JF(x)) = 0$, which is equivalent to $J\bar{F}(\bar{x}) \neq 0$. Our statement becomes a reformulation of Hensel's Lemma D.7. \square

Lemma D.9. *Let F be a system of n equations in $K[X_1^{\pm 1}, \dots, X_n^{\pm 1}]$ and let $w \in S(F)$. Then F is semiregular (resp. normalized) at w if and only if $F^{[w]}$ is semiregular (resp. normalized) at w .*

Proof. 1- If F is normalized at w , then it is clear it is that F^w is normalized at w .
2- If $w \in S(F) \cap \mathbb{Z}^n$, then let's consider the system $F(\pi^{w_1}X_1, \dots, \pi^{w_n}X_n)$. By Lemma D.6, $F(X_1, \dots, X_n)$ is semiregular at w if and only if $F(\pi^{w_1}X_1, \dots, \pi^{w_n}X_n)$ is semiregular at 0. By Lemma C.7 item (4), we have

$$F(\pi^{w_1}X_1, \dots, \pi^{w_n}X_n)^{[0]} = F^{[w]}(X_1, \dots, X_n).$$

Now we only need to prove the result for $w = 0 \in S(F)$ and we can assume F is normalized at w . If $x \in (K^\times)^n$ is such that $F(x) = 0$ and $v(x) = 0$, then

$$JF(x) = \det\left(\frac{\partial f_i}{\partial x_j}\right)_{1 \leq i, j \leq n} \Rightarrow v(JF(x)) = 0.$$

Therefore, $J\bar{F} = \overline{JF^{[0]}} \in K_v^\times$ which implies that F is semiregular at 0. \square

Theorem D.10. *Let F be a system of n equations in $K[X_1^{\pm 1}, \dots, X_n^{\pm 1}]$. Let $w \in S(F)$ and suppose that F is semiregular at w . Then the number of zeros of F and $F^{[w]}$ in $(K^\times)^n$ with valuation vector w coincide and it is bounded above by $|K_v^\times|^n$.*

Proof. The case $w = 0$ and F normalized at 0 follows immediately from Lemmas D.8

and D.9 and the fact that the reductions of F and $F^{[0]}$ modulo \mathfrak{M} coincide. Note that the assumption that F is normalized at 0 can be easily removed by pre-multiplying each equation in F by a suitable constant in K^\times . The case $w \notin \mathbb{Z}^n$ is trivial, because there are not elements in $(K^\times)^n$ with valuation vector w . In the rest of the proof we assume that $w \in \mathbb{Z}^n$. Let $b = (b_1, \dots, b_n) \in (K^\times)^n$ with valuation vector $v(b) = w$ and define $\hat{F} = F(b_1X_1, \dots, b_nX_n)$. By Lemma D.6, the system \hat{F} is semiregular at 0. It is clear that the map $(x_1, \dots, x_n) \mapsto (b_1x_1, \dots, b_nx_n)$ is a bijection between the set of solutions of \hat{F} with valuation vector 0 and the zeros of F with valuation w . Moreover, by the item (4) of Lemma C.7, we have $F^{[w]}(b_1X_1, \dots, b_nX_n) = \hat{F}^{[0]}$. In particular, the same map is a bijection between the solutions of $\hat{F}^{[0]}$ with valuation 0 and the zeros of $F^{[w]}$ with valuation w . This provides the reduction to the case $w = 0$. \square

Corollary D.11. *Let F be a system of n equations in $K[X_1^{\pm 1}, \dots, X_n^{\pm 1}]$. If $S(F)$ is finite and F is semiregular at all the points $w \in S(F)$ then F has at most $|S(F)| \cdot |K_v^\times|^n$ solutions in $(K^\times)^n$.*

2. Regular Polynomial Systems

In this section, we are going to find a class of polynomial systems where we can compute the exact number of roots.

Definition D.12. *For any $w \in \mathbb{R}^n$, let $F^{[w]}$ denote the lower polynomial system of F .*

The system

$$F = \begin{cases} f_1(X_1, \dots, X_n) = 0 \\ \vdots \\ f_n(X_1, \dots, X_n) = 0 \end{cases}$$

of n equations in n variables is regular if and only if the following three conditions are true:

1- $S(F)$ is a finite set.

2- $\forall w \in S(F)$, $F^{[w]}$ is a binomial system, hence it can be written in the form

$$F^{[w]} = \begin{cases} a_1 X^{\alpha_1} - b_1 X^{\beta_1} = 0 \\ \vdots \\ a_n X^{\alpha_n} - b_n X^{\beta_n} = 0 \end{cases}$$

3- $\forall w \in S(F)$, if $w \in \mathbb{Z}^n \Rightarrow \text{char}(K_v) \nmid \det(M_w)$ where M_w is the $n \times n$ matrix

$$M_w = \begin{bmatrix} \alpha_1 - \beta_1 \\ \vdots \\ \alpha_n - \beta_n \end{bmatrix}.$$

The key tool to compute the number of roots a binomial system is Smith Normal Form which is the statement of the following theorem.

Theorem D.13. If $A \in \mathbb{Z}^{n \times n}$ is a square matrix, then there are invertible $n \times n$ matrices $P, Q \in \mathbb{Z}^{n \times n}$ and a diagonal matrix

$$\mathbf{D} = \begin{pmatrix} d_1 & & & & & & \\ & \ddots & & & & & \\ & & d_r & & & & \\ & & & 0 & & & \\ & & & & \ddots & & \\ & & & & & & 0 \end{pmatrix}$$

with d_i divides d_{i+1} such that $A = PDQ$.

Definition D.14. Given $x \in (K^\times)^n$ and $A \in \mathbb{Z}^{n \times n}$, we define

$$\mathbf{x}^{\mathbf{A}} = \begin{pmatrix} x^{A_1} \\ x^{A_2} \\ \vdots \\ x^{A_n} \end{pmatrix}$$

where

$$\mathbf{A} = \begin{pmatrix} A_1 \\ A_2 \\ \vdots \\ A_n \end{pmatrix}$$

Some of the properties of the above notation are stated in the following proposition.

Proposition D.15. 1- $(x^B)^A = x^{AB}$ for any $A, B \in \mathbb{Z}^{n \times n}$.

2- If $A \in \mathbb{Z}^{n \times n}$ is invertible, then the map $x \mapsto x^A$ is a bijection.

3- $v(x^A) = Av(x)$.

Proposition D.16. Let B be the regular binomial system

$$B = \begin{cases} a_1 X^{\alpha_1} - b_1 X^{\beta_1} = 0 \\ \vdots \\ a_n X^{\alpha_n} - b_n X^{\beta_n} = 0 \end{cases}$$

Then we have the following:

1- The matrix

$$M = \begin{bmatrix} \alpha_1 - \beta_1 \\ \vdots \\ \alpha_n - \beta_n \end{bmatrix}$$

is invertible.

2- If $M = PDQ$ is Smith normal form of M then consider the following condition:

$$(\delta(b_1/a_1), \dots, \delta(b_n/a_n))_i^{P-1} \text{ is not a } d_i^{\text{th}} \text{ power in } K_v^\times \text{ for some } i. \quad (*)$$

Then the number m of roots of B in $(K^\times)^n$ is given by

$$m = \begin{cases} 0 & \text{if condition } (*) \text{ is true} \\ \prod_{i=1}^n \gcd(d_i, |K_v^\times|) & \text{otherwise.} \end{cases}$$

Proof. 1- Note that $S(a_1X^{\alpha_i} - b_1X^{\beta_i})$ is a hyperplane with normal vector $\alpha_i - \beta_i$, therefore $S(B)$ is a finite intersection of hyperplanes and that implies $\det(M) \neq 0$.

2- If $M = PDQ$ is Smith normal form of M then $D = \text{diag}(d_1, d_2, \dots, d_n)$ where $d_i > 0 \forall i$. The system B has the same number of roots as the system

$$X^M = X^{PDQ} = \begin{bmatrix} b_1/a_1 \\ b_2/a_2 \\ \vdots \\ b_n/a_n \end{bmatrix}.$$

Let $Y = X^Q$, then

$$Y^D = (X^Q)^D = \begin{bmatrix} b_1/a_1 \\ b_2/a_2 \\ \vdots \\ b_n/a_n \end{bmatrix}^{P-1} = \begin{bmatrix} r_1 \\ r_2 \\ \vdots \\ r_n \end{bmatrix}$$

i.e.

$$Y_1^{d_1} = r_1$$

$$Y_2^{d_2} = r_2$$

\vdots

$$Y_n^{d_n} = r_n.$$

Now reduce the above system mod \mathfrak{M} to get

$$\begin{aligned} Y_1^{d_1} &= \delta(r_1) \\ Y_2^{d_2} &= \delta(r_2) \\ &\vdots \\ Y_n^{d_n} &= \delta(r_n). \end{aligned} \tag{**}$$

If $\delta(r_i)$ is not a d_i^{th} power in K_v^\times then we can not solve the system (**), and therefore B has no roots. Otherwise, the number of solutions of (**) is $\prod_{i=1}^n \gcd(d_i, |K_v^\times|)$ which equals to m . \square

Finally, we need to show that the regular polynomial systems are in fact a subclass of the semiregular polynomial systems and hence we can apply Theorem D.10 for every valuation vector w in the tropical set of any given regular system.

Proposition D.17. *If the system $F \in (K[X_1^{\pm 1}, \dots, X_n^{\pm 1}])^n$ is regular, then F is also semiregular.*

Proof. If F is regular at $w \in S(F)$, then $F^{[w]}$ is a binomial system which can be written as

$$F^{[w]} = \begin{cases} f_1^{[w]} = a_1 X^{\alpha_1} - b_1 X^{\beta_1} \\ \vdots \\ f_n^{[w]} = a_n X^{\alpha_n} - b_n X^{\beta_n} \end{cases}$$

Let M_w be the matrix

$$M_w = \begin{bmatrix} \alpha_1 - \beta_1 \\ \vdots \\ \alpha_n - \beta_n \end{bmatrix} \in \mathbb{Z}^{n \times n}.$$

If $w \notin \mathbb{Z}^n$, then F has no roots in $(K^\times)^n$ so we have nothing to prove. Assume $w \in \mathbb{Z}$ and define $\tilde{F} = F(\pi^{w_1} X_1, \dots, \pi^{w_n} X_n)$, so by Lemma D.5 F is semiregular at w iff \tilde{F}

is semiregular at 0. Now, we have

$$\tilde{F}^{[0]} = \begin{cases} a_1 \pi^{w \cdot \alpha_1} X^{\alpha_1} - b_1 \pi^{w \cdot \beta_1} X^{\beta_1} \\ \vdots \\ a_n \pi^{w \cdot \alpha_n} X^{\alpha_n} - b_n \pi^{w \cdot \beta_n} X^{\beta_n} \end{cases}$$

By Lemma D.6, \tilde{F} is semiregular at 0 iff $\tilde{F}^{[0]}$ is also semiregular at 0. By Lemma D.9, \tilde{F} is semiregular at 0 iff G is semiregular at 0 where

$$G = \begin{cases} \frac{a_1}{b_1} \pi^{w \cdot (\alpha_1 - \beta_1)} X^{\alpha_1 - \beta_1} - 1 \\ \vdots \\ \frac{a_n}{b_n} \pi^{w \cdot (\alpha_n - \beta_n)} X^{\alpha_n - \beta_n} - 1 \end{cases} \\ = \begin{cases} c_n X^{\alpha_n - \beta_n} - 1 \\ \vdots \\ c_n X^{\alpha_n - \beta_n} - 1 \end{cases}$$

Since $v(c_i) = 0$ we have $h(c_i X^{\alpha_i - \beta_i} - 1) = 0 \forall i$. On the other hand, for $x \in (K^\times)^n$ a root of G with $v(x) = 0$, we have

$$JG(x) = \det(M_w) \prod c_i \prod \frac{x^{\alpha_i - \beta_i}}{x_i}.$$

Since the $\text{char}(K_v)$ does not divide $\det(M_w)$ we conclude $v(JG(x)) = 0 + 0 + 0 = 0$ and that shows G is semiregular at 0. \square

CHAPTER IV

DESCARTES' BOUNDS

A. Univariate Bounds

Throughout this section, the field K is a finite extension of \mathbb{Q}_p . The goal of the section is to find a bound for the number of roots of a given univariate polynomial $f \in K[X]$.

Definition A.1. For $k, n \in \mathbb{Z}_{\leq 0}$, define $d_k(n)$ to be the least common multiple of all integers that can be written as a product of at most k pairwise distinct positive integers that are at most n . We also define $d_k(n)$ if $k = 0$ or $n = 0$ by taking the empty product to be 1.

To illustrate the above definition, consider the following examples

Examples

- i- For $n = 4$, $d_0(4) = 1$ and $d_1(4) = l.c.m\{1, 2, 3, 4\} = 12$.
- ii- For $n = 6$, $d_0(6) = 1$, $d_1(6) = l.c.m\{1, 2, 3, 4, 5, 6\} = 60$
and $d_2(6) = l.c.m\{1, 2, \dots, 6, 2 \times 3, \dots, 2 \times 6, \dots, 5 \times 6\} = 360$.

Proposition A.2. i- $d_k(n)$ divides $n!$ with equality if $n \leq k$.

ii- $md_k(m-1)$ divides $d_k(n)$ if $1 \leq m \leq n$ and $k \geq 1$.

Proposition A.3. Let $k, n \in \mathbb{Z}_{\leq 0}$ and $T \subset \mathbb{Z}$ such that $|T| = k + 1$. Then there is a polynomial $h \in \mathbb{Z}[X]$ such that for all $t \in T$ we have

$$h(t) = d_k(n) \binom{t}{n}.$$

Proof. See [9, Prop. 2.2]. □

Corollary A.4. *Let $k, n \in \mathbb{Z}_{\leq 0}$ with $n > k$ and $T \subset \mathbb{Z}$ such that $|T| = k + 1$. Then there are rational numbers c_0, c_1, \dots, c_k such that for each i the denominator of c_i divides $\frac{d_k(n)}{i!}$ and for all $t \in T$ one has*

$$\binom{t}{n} = \sum_{i=0}^t c_i \binom{t}{i}.$$

Proof. See [9, Cor. 2.3]. □

Proposition A.5. *Let p be a prime number and $k, n \in \mathbb{Z}_{\leq 0}$ with $k \geq 0$ and $n \geq 1$.*

Then we have

$$\text{ord}_p(d_k(n)) \leq k \left\lceil \frac{\log n}{\log p} \right\rceil$$

where $[x]$ denotes the largest integer $\leq x$.

Proof. See [9, Prop. 2.4]. □

The following result gives an estimation for the number of roots close to 1. It is a key tool in proving the existence of the bound and it is true for more general fields.

Theorem A.6. *For all p, k, r where p is a prime number $k \in \mathbb{Z}_{>0}$ and $r \in \mathbb{R}_{>0}$, there exists a positive integer $C = C(p, k, r)$ with following property:*

Let K be a field of characteristic 0 and valuation v such that $v(p) = 1$ and $f \in K[X]$ be a polynomial with at most $k+1$ nonzero terms. Then f has at most C zeros $x \in K$ such that $v(x - 1) \geq r$ counted with multiplicities.

Proof. define

$$D = \max\{ir - \text{ord}_p(i!) : 0 \leq i \leq k\}$$

and

$$C(p, k, r) = \max\{m \geq 0 : mr - \text{ord}_p(d_k(m)) \leq D\}.$$

Since $r > 0$, we have $mr - \text{ord}_p d_k(m) \rightarrow \infty$ as $m \rightarrow \infty$, by Proposition A.5. Therefore $C(p, k, r)$ is well-defined and $C \geq k$ since $d_k(k) = k!$.

Without loss of generality, we assume K is algebraically closed. Write

$$f(X) = \sum_{\alpha \in \Lambda} a_{\alpha} X^{\alpha}$$

where $\Lambda \subseteq \mathbb{Z}_{\geq 0}$, $|\Lambda| = k + 1$ and $a_{\alpha} \in K$. Define $g \in K[X]$ by

$$g(X) = f(1 + X) = \sum_{i \geq 0} b_i X^i.$$

Then we have

$$b_i = \sum_{\alpha \in \Lambda} a_{\alpha} \binom{\alpha}{i} \quad \text{for } i \geq 0$$

note that $g \neq 0$ since $f \neq 0$.

Let

$$\begin{aligned} m &= |\{x : f(x) = 0 \text{ and } v(x_1) \geq r\}| \\ &= |\{y : g(y) = 0 \text{ and } v(y) \geq r\}|. \end{aligned}$$

By the theory of Newton polygon we have

$$\frac{v(b_m) - v(b_i)}{m - i} \leq -r$$

or

$$v(b_m) + mr \leq v(b_i) + ir \quad \forall i.$$

If $m \leq k$, then $m < C$. Suppose that $m > k$, then by Corollary A.4 there are rational numbers c_0, c_1, \dots, c_k with the denominator of c_i dividing $d_k(m)/i!$ such that

$$\binom{\alpha}{m} = \sum_{i=0}^k c_i \binom{\alpha}{i} \quad \forall \alpha \in \Lambda.$$

Hence

$$\begin{aligned}
b_m &= \sum_{\alpha \in \Lambda} a_\alpha \binom{\alpha}{m} \\
&= \sum_{i=0}^k c_i \left(\sum_{\alpha \in \Lambda} a_\alpha \binom{\alpha}{i} \right) \\
&= \sum_{i=0}^k c_i b_i.
\end{aligned}$$

Therefore, we have

$$v(b_m) \geq \min\{v(c_i) + v(b_i) : 0 \leq i \leq k\}.$$

Now we have $v(c_i) \geq \text{ord}_p(i!) - \text{ord}_p(d_k(m))$ and $v(b_i) \geq v(b_m) + mr - ir$. Therefore

$$v(b_m) \geq \min\{\text{ord}_p(i!) - \text{ord}_p(d_k(m)) + v(b_m) + mr - ir : 0 \leq i \leq k\}.$$

Since $b_m \neq 0$, we have

$$mr - \text{ord}_p(d_k(m)) \leq D$$

which implies that $m < C$. □

Now we are ready to state and prove the main result of this section, which is existence of a bound for the number of roots of any univariate polynomial over local fields.

Theorem A.7. *Let K be a finite extension of \mathbb{Q}_p . For any $k \in \mathbb{Z}_{>0}$ there exists a positive integer $B(k, K)$ with the following property:*

Let $f \in K[X]$ be non-zero polynomial with at most $k + 1$ non-zero terms and with $f(0) \neq 0$. Then f has at most B zeros in K , counted with multiplicities.

Proof. Assume the valuation v on K is normalized i.e. $v(p) = 1$. Let e be the ramification index of K over \mathbb{Q}_p , A be the valuation ring, \mathfrak{M} be its maximal ideal

and $q = |K_v|$ the cardinality of the residue field K_v .

If $f \in K[X]$ be non-zero polynomial with at most $k + 1$ non-zero terms, then by Theorem A.6 there exists $C = C(p, k, e)$ such that f has at most C zeros in $1 + \mathfrak{M}$. Apply this result to $f(uX), u \in A^\times$, we have that f has at most $(q - 1)C$ zeros in $u + \mathfrak{M}$. Therefore has at most C zeros in A^\times . Similarly, f has at most $(q - 1)C$ zeros in aA^\times for any $a \in K^\times$ which means f has at most $(q - 1)C$ zeros of a given finite valuation. By the theory of Newton polygon $|\{v(x) : f(x) = 0, x \in K^\times\}| \leq k$. We conclude that f has at most $k(q - 1)C = B$ zeros in K^\times . \square

B. Multivariate Bounds

Descartes' Rule of Signs implies that the number of real roots of any polynomial $f \in \mathbb{R}[X]$ with $t \geq 1$ non-zero terms are at most $2t - 1$. In the previous section we have seen that H.W Lenstra Jr. gave an analogue to Descartes' bound over the p -adics.

A. Khovanski generalized Descartes' bound to sparse systems of multivariate polynomials. Here in this section we are discussing Rojas' ultrametric analogue of Khovanski's bound. Given a system of polynomials $F \in (K[X_1, \dots, X_n])^k$, we are interested in counting the number of geometrically isolated roots of the system F counted with multiplicities. Recall that the isolated roots are the zero dimensional components of the algebraic variety $\mathbb{V}_{\overline{K}}(F)$ where \overline{K} denotes the algebraic closure of the field K . Again, we are assuming that K is a finite extension of \mathbb{Q}_p .

Definition B.1. *Given polynomials f_1, \dots, f_k with f_i an n -variate m_i -nomial for all i , we call the system $F = (f_1, \dots, f_k)$ a $k \times n$ fewnomial system of type (m_1, \dots, m_k) . If the total of distinct exponent vectors among the f_i is t , then we can call F a t -sparse $k \times n$ fewnomial system.*

In order to proceed, we need the following notations.

Notations:

1- For the system $F = (f_1, \dots, f_k)$, we write

$$\text{Newt}_v(F) := (\text{Newt}_v(f_1), \dots, \text{Newt}_v(f_k))$$

2- For closed subsets $B_1, \dots, B_n \subseteq \mathbb{R}^d$, we write

$$\text{face}_\omega(B_1, \dots, B_n) := (\text{face}_\omega(B_1), \dots, \text{face}_\omega(B_n))$$

3- Let $\mathcal{M}(\cdot)$ denote the *normalized* mixed volume which means

$$\mathcal{M}(\text{Conv}(\{0, e_1, \dots, e_d\}), \dots, \text{Conv}(\{0, e_1, \dots, e_d\})) = 1$$

where e_i is the standard basis vector of \mathbb{R}^d .

4- For any $r = (r_1, \dots, r_n) \in \mathbb{R}_{>0}^n$, let Λ_r denote the set

$$\Lambda_r = \{\hat{s} = (s_1, \dots, s_n, 1) : s_i \geq r_i \quad \forall i\}.$$

The following result characterizes when the mixed volumes vanish.

Lemma B.2. *Given polytopes $P_1, \dots, P_n \subseteq \mathbb{R}^n$, we have $\mathcal{M}(P_1, \dots, P_n) > 0$ if and only if there are linearly independent vectors v_1, \dots, v_n with v_i parallel to an edge of P_i for all i .*

Proof. See [16, Lemma 3]. □

As a consequence of the properties of polytopes and mixed volume we have the following result which gives a bound for the mixed volume.

Theorem B.3. *Let $G(g_1, \dots, g_n)$ be any $n \times n$ polynomial system and $r = (r_1, \dots, r_n) \in$*

$\mathbb{R}_{>0}^n$. Let

$$\tau(g_i, r) = \text{proj}\left(\bigcup_{\hat{s} \in \Lambda_r} \text{face}_{\hat{s}}(\text{Newt}_p(g_i))\right) \quad \forall i.$$

Then

$$\sum_{\hat{s} \in \Lambda} \mathcal{M}(\text{proj}(\text{face}_{\hat{s}}(\text{Newt}_p(G)))) \leq \mathcal{M}(\text{Conv}(\tau(g_1, r), \dots, \text{Conv}(\tau(g_n, r)))).$$

In particular, if $Q_i \subseteq \{(t_1, \dots, t_n) \in \mathbb{R}^n : t_1 r_1, \dots + r_n t_n \leq \alpha_i \text{ and } t_j \geq 0 \text{ for all } j\}$ for all $i \in [n]$, then $\mathcal{M}(Q_1, \dots, Q_n) \leq \prod_{i=1}^n \frac{\alpha_i}{r_i}$.

Proof. See [16, Lemma 8]. □

Theorem B.4 (Simrnov's Theorem). *Let K be any algebraically closed field with non-Archimedean valuation v . Then for any $n \times n$ polynomial system F over K , the number of geometrically isolated roots $(x_1, \dots, x_n) \in (K^\times)^n$ of F satisfying $v(x_i) = r_i$ for all i (counted with multiplicities) is no more than $\mathcal{M}(\text{proj}(\text{face}_{\hat{r}}(\text{Newt}_v(F))))$ where $\hat{r} = (r_1, \dots, r_n)$.*

Proof. See [19, Theorem 3.4]. □

Simrnov's Theorem can be used to find a bound for the number of roots of sparse system of polynomials by looking at the Minkowski sum of Newton polygons of the polynomial, see [16, Example 3]. Let's assume that the field K is a finite extension for \mathbb{Q}_p of degree d .

Lemma B.5. *Suppose $F = (f_1, \dots, f_k)$ is any $k \times n$ polynomial system over K with $k > n$ and let D be the maximum of degrees of the f_i and $S \subseteq \mathbb{Z}$ any set of such that $|S| > kD^n$. Then there is an $n \times k$ matrix $[a_{ij}]$ with entries in S such that $\mathbb{V}_{\mathbb{C}_p}(F) \subseteq \mathbb{V}_{\mathbb{C}_p}(G)$ and $\mathbb{V}_{\mathbb{C}_p}(F) \setminus \mathbb{V}_{\mathbb{C}_p}(G)$ is finite where $G = (\sum_{i=1}^k a_{1i} f_i, \dots, \sum_{i=1}^k a_{ni} f_i)$.*

Proof. See [16, Lemma 1]. □

The above lemma allows us to reduce to the case $k = n$. We will also need the following fact on the roots of sparse polynomial systems over most infinite fields.

Lemma B.6. *Suppose F is a t -sparse polynomial system over a field L with characteristic zero and let $B(L, t, k, n)$ denote the maximum number of geometrically isolated roots in L^n of F . If $t \leq n$ or $k < n$ then $B = 0$. Also, $B(L, t, k, n) \leq B(L, t_1, \dots, t_n)$, where $t_1, \dots, t_n \leq t - n + 1$.*

Proof. See [16, Lemma 2]. □

Lemma B.7. *Let $c := \frac{e}{e-1}$ and $t_1, r_1, \dots, t_n, r_n > 0$. Then*

$$\begin{aligned} \sum_{i=1}^n (r_i t_i - (t-1) \log_p t_i) &\leq (t-1) \sum_{i=1}^n r_i \Rightarrow \\ \sum_{i=1}^n r_i t_i &\leq (c(t-1) \left[r_1 + \dots + r_n + \log_p \left(\frac{(t-n)^n}{r_1 \dots r_n \log^n p} \right) \right]). \end{aligned}$$

Proof. See [16, Lemma 7]. □

Rojas' bound follows from Theorem B.8 below which estimates the number of roots in \mathbb{C}_p close to the point $(1, \dots, 1)$.

Theorem B.8. *Let F be any t -sparse $k \times n$ polynomial system over \mathbb{C}_p . Also let $r_1, \dots, r_n > 0$, $r := (r_1, \dots, r_n)$ and let ord_p be the usual p -adic valuation. Finally, let $C_p(t, n, r)$ denote the maximum number of geometrically isolated roots $(x_1, \dots, x_n) \in \mathbb{C}_p^n$ of F with $\text{ord}_p(x_i - 1) \geq r_i$ for all i , counted with multiplicities. Then $C_p(t, n, r) = 0$ (if $t \leq n$ or $k < n$) and*

$$C_p(t, n, r) \leq \left\lfloor \left(c(t-n) \left[r_1 + \dots + r_n + \log_p \left(\frac{(t-n)^n}{r_1 \dots r_n \log^n p} \right) \right] \right)^n / \prod_{i=1}^n r_i \right\rfloor$$

(if $t \geq n + 1$ and $k \geq n$), where $c := e/(e-1) \leq 1.582$.

Furthermore, when $k = n$ we can obtain a more refined bound as follows:

Let $[n] := \{1, 2, \dots, n\}$. Let m_i denote the number of distinct exponent vectors in f_i , $\bar{m} := (m_1, \dots, m_n)$ and $\bar{N} := (N_1, \dots, N_n)$ where, for each i , $N_i \subseteq [n]$ is the set of all j such that x_j appears with nonzero exponent in the same monomial term of f_i . Then, letting $C_p(\bar{m}, \bar{N}, r)$ denote the obvious analogue of $C_p(t, n, r)$, we have $C_p(\bar{m}, \bar{N}, r) = 0$ (if $m_i \leq 1$ for some i) and

$$C_p(\bar{m}, \bar{N}, r) \leq \left[c^n \prod_{i=1}^n \left((m_i - 1) \left[\left(\sum_{j \in N_i} r_j \right) + \log_p \left(\frac{(m_i - 1)^{|N_i|}}{\left(\prod_{j \in N-i} r_j \right) \log^{|N_i|} p} \right) \right] / r_i \right) \right]$$

(if $m_i, \dots, m_n \geq 2$).

Proof. See [16, Theorem 2]. □

Below we are stating Rojas' bound for the number of geometrically isolated roots of sparse systems of polynomials with coefficients in K . Let q denote the cardinality of the residue field of K over \mathbb{Q}_p .

Theorem B.9. *Let K be a finite extension of \mathbb{Q}_p of degree d and let F be a t -sparse $k \times n$ polynomial system over K . Then the number of geometrically isolated roots in $(K^\times)^n$ is no more than $O([n(q-1)(t-n) \log(t-n)]^n)$ if $t > n$ and $k > n+1$.*

Proof. see [16, Theorem 1]. □

C. Semiregular Polynomials Bounds

In this section, we assume K is an ultrametric field. Let F be the following system of polynomial equations

$$F = \begin{cases} f_1(X_1, \dots, X_n) = 0 \\ \vdots \\ f_n(X_1, \dots, X_n) = 0 \end{cases}$$

where $f_i \in K[X_1^{\pm 1}, \dots, X_n^{\pm 1}]$ has t_i monomial terms and $\sum_i t_i = t$.

Define the polynomial $\hat{F} \in K[X_1^{\pm 1}, \dots, X_n^{\pm 1}, Y_1^{\pm 1}, \dots, Y_n^{\pm 1}]$ as follows

$$\hat{F} = Y_1 f_1 + Y_2 f_2 + \dots + Y_n f_n.$$

Lemma C.1. *For any $w_0 \in \mathbb{R}^n$, we have $w_0 \in S(F)$ if and only if $w_0 \times \mathbb{R}^n \subset \text{Trop}(\hat{F})$.*

Proof. (\Rightarrow) Let $w_0 \in S(F)$ and $u \in \mathbb{R}^n$. We want to show that point $(w_0, u) \in \text{Trop}(\hat{F})$. We need the following fact:

for any i and $1 \leq r_i \leq t_i$, we have

$$l_{r_i}(f_i, w_0) + u_i = l_a(\hat{F}, (w_0, u)) \text{ for some } 1 \leq a \leq t.$$

Now, since $w_0 \in S(F)$ we have $w_0 \in \text{Trop}(f_i) \forall i$ and hence we have

$$l_{i_1}(f_1, w_0) = l_{j_1}(f_1, w_0) \leq l_{k_1}(f_1, w_0) \quad \forall 1 \leq k_1 \leq t_1$$

\vdots

$$l_{i_n}(f_n, w_0) = l_{j_n}(f_n, w_0) \leq l_{k_n}(f_n, w_0) \quad \forall 1 \leq k_n \leq t_n.$$

Add u_i to all sides in each inequality to get

$$l_{i_1}(f_1, w_0) + u_1 = l_{j_1}(f_1, w_0) + u_1 \leq l_{k_1}(f_1, w_0) + u_1 \quad \forall 1 \leq k_1 \leq t_1$$

\vdots

$$l_{i_n}(f_n, w_0) + u_n = l_{j_n}(f_n, w_0) + u_n \leq l_{k_n}(f_n, w_0) + u_n \quad \forall 1 \leq k_n \leq t_n.$$

Now we take the minimum of $l_{k_i}(f_i, w_0)$ over $i_1, j_1, i_2, j_2, \dots, i_n, j_n$ and use the above fact to conclude that $(w_0, u) \in S(\hat{F})$.

(\Leftarrow) Let $w_0 \times \mathbb{R}^n \subset S(\hat{F})$. Suppose that $w_0 \notin S(F)$, therefore $w_0 \notin \text{Trop}(f_i)$ for some i . Without loss of generality, assume $w_0 \notin \text{Trop}(f_1)$. Let $l_{s_1}(f_1, w_0) = \min\{l_{i_1}(f_1, w_0)\}$ and hence

$$l_{s_1}(f_1, w_0) < l_{i_1}(f_1, w_0) \quad \forall i_1 \neq s_1.$$

Choose $u_1 \in \mathbb{R}$ such that

$$l_{s_1}(f_1, w_0) + u_1 < l_{i_j}(f_j, w_0)$$

for all $2 \leq j \leq n$ and $1 \leq i_j \leq t_j$. Now consider the point $u = (u_1, 0, \dots, 0)$, so we have $h(\hat{F}, (w_0, u)) = l_{s_1}(f_1, w_0) + u_1$. But $h(\hat{F}, (w_0, u))$ is attained once and that means the point $(w_0, u) \notin \text{Trop}(\hat{F})$, a contradiction. Hence $w_0 \in S(F)$. \square

In order to proceed, we use the following version of the upper bound theorem. Here $\lfloor x \rfloor$ denote the integer part of $x \in \mathbb{R}$.

Theorem C.2. *The intersection of t half-spaces in \mathbb{R}^d is a convex polytope with at most $O(t^{\lfloor d/2 \rfloor})$ faces of dimension at least $\lfloor d/2 \rfloor$.*

Proof. see [6, Theorem 6.12]. \square

The following result gives an upper bound for semiregular systems with a finite tropical set.

Corollary C.3. *If the system $F \in (K[X_1^{\pm 1}, \dots, X_n^{\pm 1}])^n$ is semiregular and $S(F)$ is a finite set, then the number of roots of F is no greater than $O(t^n |K_v^\times|^n)$.*

Proof. Since $S(F)$ is finite, then the number of roots of F is bounded by $|S(F)| |K_v^\times|^n$. Now we need to estimate the cardinality of $S(F)$. Consider the polynomial $\hat{F} = Y_1 f_1 + \dots + Y_n f_n$.

claim: $|S(F)| \leq$ the number of faces of $S(\hat{F})$ of dimension at least n .

proof of claim: If $w, w' \in S(F)$, then $w \times \mathbb{R}^n \cap w' \times \mathbb{R}^n \neq \emptyset$. Assume that $w \times \mathbb{R}^n$ and $w' \times \mathbb{R}^n$ both in the same face in $S(\hat{F})$, then this face is of dimension $> n$. If we take any point w_0 lies in the line segment between w and w' then $w_0 \times \mathbb{R}^n$ is subset of the the common face which means $w_0 \times \mathbb{R}^n \subset S(\hat{F})$. By the last lemma we have

$w_0 \in S(F)$ contradicting that fact that $S(F)$ is finite, so we must have $w \times \mathbb{R}^n$ and $w' \times \mathbb{R}^n$ are in different faces and that proves the claim.

Now by the above claim and the upper bound theorem applied to $P(\hat{F})$ we have $|S(F)| \leq O(t^n)$ and hence the number of roots of F can not exceed $O(t^n |K_v^\times|^n)$. \square

CHAPTER V

COMPLEXITY THEORY

A. Complexity and Feasibility

1. Overview of Some Complexity Classes

Here, we define some of the important complexity classes and for more details about those classes and other related classes one can see [13].

P The family of decision problems which can be done in polynomial-time.

NP The family of decision problems where a 'YES' answer can be certified within polynomial-time.

coNP The family of decision problems where a 'NO' answer can be certified within polynomial-time.

BPP The family of decision problems admitting randomized polynomial-times algorithms that terminate with an answer that is correct with probability at least $\frac{2}{3}$.

ZPP The family of decision problems where the correct answer is given always (i.e. in a probability more than $\frac{1}{2}$) in polynomial-time on average.

2. The Feasibility Problem

Definition A.1. Let $\text{FEAS}_{\mathbb{F}_{\text{primes}}}$ denote the problem of deciding, for an input polynomial system $F \in \bigcup_{k,n \in \mathbb{N}} (\mathbb{Z}[x_1, \dots, x_n])^k$ **and** an input prime p , whether F has a root in \mathbb{F}_p^n . Also let $\text{FEAS}_{\mathbb{F}_{\text{primes}}}(\mathcal{I})$ denote the natural restriction of $\text{FEAS}_{\mathbb{F}_{\text{primes}}}$ to inputs in \mathcal{I} . Also, when \mathcal{F} is a family of polynomial systems, we will abuse notation slightly by letting $\text{FEAS}_{\mathbb{F}_{\text{primes}}}(\mathcal{F})$ denote the restriction of $\text{FEAS}_{\mathbb{F}_{\text{primes}}}$ to inputs in $\mathcal{F} \times \mathbb{P}$. The underlying input size for all these problems is $\text{size}_p(F) := \text{size}(F) + \log p$.

Lemma A.2. Given any cyclic group G , $a \in G$, and an integer d , the following 3 conditions are equivalent:

1. the equation $x^d = a$ has a solution $a \in G$.
2. the order of a divides $\frac{|G|}{\gcd(d, |G|)}$.
3. $a^{|G|/\gcd(d, |G|)} = 1$.

Also, \mathbb{F}_q^\times is cyclic for any prime power q , and $(\mathbb{Z}/p^\ell\mathbb{Z})^\times$ is cyclic for any (p, ℓ) with p an odd prime or $\ell \leq 2$. Finally, for $\ell \geq 3$,

$$(\mathbb{Z}/2^\ell\mathbb{Z})^\times = \{\pm 1, \pm 5, \pm 5^2, \pm 5^3, \dots, \pm 5^{2^{\ell-2}-1} \pmod{2^\ell}\}.$$

Proof. See [1, Theorem 5.7.2 and Theorem 5.6.2]. □

Theorem A.3. For any $s \in \mathbb{N}$, $\delta > 0$, a failure probability $\varepsilon \in (0, 1/2)$, and $n \in \mathbb{N}$, we can find — within $O\left(\left(\frac{n}{\varepsilon}\right)^{\frac{3}{2}+\delta} + (n \log(n) + \log\left(\frac{s}{\varepsilon}\right))^{7+\delta}\right)$ randomized bit operations — a sequence $P = (p_i)_{i=1}^n$ of consecutive primes and a positive integer c such that the following hold:

1. $\log(c)$, $\log\left(\prod_{i=1}^n p_i\right) = O(n \log(n) + \log(s/\varepsilon))$
2. for any $S \subset \mathbb{N}$ of cardinality s , the number $p := 1 + c \prod_{i=1}^n p_i$ is prime and **not** in S with probability $\geq 1 - \varepsilon$.

Proposition A.4. *Given any $f_1, \dots, f_k \in \mathbb{Z}[x_1]$ of maximum degree d and maximum coefficient absolute value H , let*

$$\tilde{f}(x_1) = x^d(f_1(x_1)f_1(1/x_1) + \dots + f_k(x_1)f_k(1/x_1)).$$

Then $f_1 = \dots = f_k = 0$ has a root on the complex unit circle iff \tilde{f} has a root on the complex unit circle. In particular, if $f_i \in \mathcal{F}_{1,\mu_i}$ and $\mu_i \leq m$ for all i , then $\tilde{f} \in \mathcal{F}_{1,\mu}$ for some μ with $\mu \leq ((m-1)m+1)k$ and \tilde{f} has maximum coefficient bit-size $O(\log(kmH))$. \square

Lemma A.5. *(See, e.g., [7, Ch. 12, Sec. 1, pp. 397–402].) Suppose $f(x_1) = a_0 + \dots + a_d x_1^d$ and $g(x_1) = b_0 + \dots + b_{d'} x_1^{d'}$ are polynomials with indeterminate coefficients. Define their **Sylvester matrix** to be the $(d+d') \times (d+d')$ matrix*

$$\mathcal{S}_{(d,d')}(f, g) := \begin{bmatrix} a_0 & \dots & a_d & 0 & \dots & 0 \\ & \ddots & & & \ddots & \\ 0 & \dots & 0 & a_0 & \dots & a_d \\ b_0 & \dots & b_{d'} & 0 & \dots & 0 \\ & \ddots & & & \ddots & \\ 0 & \dots & 0 & b_0 & \dots & b_{d'} \end{bmatrix} \left. \begin{array}{l} \left. \vphantom{\begin{matrix} a_0 \\ \dots \\ a_d \end{matrix}} \right\} d' \text{ rows} \\ \left. \vphantom{\begin{matrix} b_0 \\ \dots \\ b_{d'} \end{matrix}} \right\} d \text{ rows} \end{array} \right\}$$

*and their **Sylvester resultant** to be $\mathcal{R}_{(d,d')}(f, g) := \det \mathcal{S}_{(d,d')}(f, g)$. Then, assuming $f, g \in K[x_1]$ for some field K and $a_d b_{d'} \neq 0$, we have that $f = g = 0$ has a root in the algebraic closure of K iff $\mathcal{R}_{(d,d')}(f, g) = 0$. Finally, if we assume further that f and g have complex coefficients of absolute value $\leq H$, and f (resp. g) has exactly m (resp. m') monomial terms, then $|\mathcal{R}_{(d,d')}(f, g)| \leq m^{d/2} m'^{d'/2} H^{d+d'}$. \square*

Lemma A.6. *Suppose $D \in \mathbb{N}$ and $f \in \mathbb{Z}[x_1] \setminus \{0\}$ has degree d , exactly m monomial terms, and maximum coefficient absolute value H . Also let p be any prime congruent to 1 mod D . Then*

1. f vanishes at a complex D^{th} root of unity \iff f vanishes at a D^{th} root of unity in \mathbb{Q}_p .
2. f vanishes at a complex D^{th} root of unity \implies the mod p reduction of f vanishes at a D^{th} root of unity in \mathbb{F}_p .
3. With the exception of $O(d + D \log(mH))$ primes p , f vanishes at **no** complex D^{th} root of unity \implies f vanishes at **no** D^{th} root of unity in \mathbb{F}_p .

We call the primes for which the implication in Assertion 3 fails exceptional (for (f, D)).

Recall that any Boolean expression of one of the following forms:

$$(\heartsuit) \quad y_i \vee y_j \vee y_k, \quad \neg y_i \vee y_j \vee y_k, \quad \neg y_i \vee \neg y_j \vee y_k, \quad \neg y_i \vee \neg y_j \vee \neg y_k, \quad \text{with } i, j, k \in [3n],$$

is a 3CNFSAT **clause**. Let us first refine slightly Plaisted's elegant reduction from 3CNFSAT to feasibility testing for univariate polynomial systems over the complex numbers [14, Sec. 3, pp. 127–129].

Definition A.7. Letting $P := (p_1, \dots, p_n)$ denote any strictly increasing sequence of primes, let us inductively define a semigroup homomorphism \mathcal{P}_P — the **Plaisted morphism with respect to P** — from certain Boolean expressions in the variables y_1, \dots, y_n to $\mathbb{Z}[x_1]$, as follows: (0) $D_P := \prod_{i=1}^n p_i$,

$$(1) \quad \mathcal{P}_P(0) := 1, \quad (2) \quad \mathcal{P}_P(y_i) := x_1^{D_P/p_i} - 1,$$

(3) $\mathcal{P}_P(\neg B) := (x_1^{D_P} - 1) / \mathcal{P}_P(B)$, for any Boolean expression B for which $\mathcal{P}_P(B)$ has already been defined,

(4) $\mathcal{P}_P(B_1 \vee B_2) := \text{lcm}(\mathcal{P}_P(B_1), \mathcal{P}_P(B_2))$, for any Boolean expressions B_1 and B_2 for which $\mathcal{P}_P(B_1)$ and $\mathcal{P}_P(B_2)$ have already been defined. \diamond

Lemma A.8. Suppose $P = (p_i)_{k=1}^n$ is an increasing sequence of primes with $\log(p_k) = O(k^\gamma)$ for some constant γ . Then, for all $n \in \mathbb{N}$ and any clause C of the form (\heartsuit) , we have $\text{size}(\mathcal{P}_P(C))$ polynomial in n . In particular, \mathcal{P}_P can be evaluated at any such C

in time polynomial in n . Furthermore, if K is any field possessing D_P distinct D_P^{th} roots of unity, then a 3CNFSAT instance $B(y) := C_1(y) \wedge \cdots \wedge C_k(y)$ has a satisfying assignment iff the univariate polynomial system $F_B := (\mathcal{P}_P(C_1), \dots, \mathcal{P}_P(C_k))$ has a root $\zeta \in K$ satisfying $\zeta^{D_P} = 1$. \square

Proof. See [14, Section 3] \square

Plaisted actually proved the special case $K = \mathbb{C}$ of the above lemma, in slightly different language, in [14]. However, his proof extends with no difficulty whatsoever to the more general family of fields detailed above.

B. p -adic Feasibility

Definition B.1. Let $\text{FEAS}_{\mathbb{Q}_{\text{primes}}}$ denote the problem of deciding, for an input polynomial system $F \in \bigcup_{k,n \in \mathbb{N}} (\mathbb{Z}[x_1, \dots, x_n])^k$ **and** an input prime p , whether F has a root in \mathbb{Q}_p^n . Also let $\text{FEAS}_{\mathbb{Q}_{\text{primes}}}(\mathcal{I})$ denote the natural restriction of $\text{FEAS}_{\mathbb{Q}_{\text{primes}}}$ to inputs in \mathcal{I} . Also, when \mathcal{F} is a family of polynomial systems, we will abuse notation slightly by letting $\text{FEAS}_{\mathbb{Q}_{\text{primes}}}(\mathcal{F})$ denote the restriction of $\text{FEAS}_{\mathbb{Q}_{\text{primes}}}$ to inputs in $\mathcal{F} \times \mathbb{P}$. The underlying input size for all these problems is $\text{size}_p(F)$ (cf. Definition ??). Finally, let $(\mathbb{Z} \times (\mathbb{N} \cup \{0\}))^\infty$ denote the set of all infinite sequences of pairs $((c_i, a_i))_{i=1}^\infty$ with $c_i = a_i = 0$ for i sufficiently large.

Theorem B.2. $\text{FEAS}_{\mathbb{Q}_{\text{primes}}}(\mathcal{F}_{1,2}) \in \mathbf{P}$.

Proof. First note that we can easily reduce to the special case $f(x) := x^d - \alpha$ with $\alpha \in \mathbb{Q}$, since we can divide any input by a suitable monomial term, and arithmetic over \mathbb{Q} is doable in polynomial time. The case $\alpha = 0$ always results in the root 0, so let us also assume $\alpha \neq 0$. Clearly then, any p -adic root ζ of $x^d - \alpha$ satisfies $d \text{ord}_p \zeta = \text{ord}_p \alpha$. Since we can compute $\text{ord}_p \alpha$ and reductions of integers mod d in

polynomial-time [1, Ch. 5], we can then assume that $d \mid \text{ord}_p \alpha$ (for otherwise, f would have no roots over \mathbb{Q}_p). Replacing $f(x_1)$ by $p^{-\text{ord}_p \alpha} f(p^{\text{ord}_p \alpha / d} x_1)$, we can assume further that $\text{ord}_p \alpha = \text{ord}_p \zeta = 0$. In particular, if $\text{ord}_p \alpha$ was initially a nonzero multiple of d , then $\log \alpha \geq d \log_2 p$. So $\text{size}(f) \geq d$ and our rescaling at worst doubles $\text{size}(f)$.

Letting $k := \text{ord}_p d$, note that $f'(x) = dx^{d-1}$ and thus $\text{ord}_p f'(\zeta) = \text{ord}_p(d) + (d-1)\text{ord}_p \zeta = k$. So by Hensel's Lemma, it suffices to decide whether the mod p^ℓ reduction of f has a root in $(\mathbb{Z}/p^\ell \mathbb{Z})^*$, for $\ell = 1 + 2k$. Note in particular that $\text{size}(p^\ell) = O(\log(p) \text{ord}_p d) = O(\log(p) \log(d) / \log p) = O(\log d)$ which is linear in our notion of input size. By Lemma A.2, we can then clearly decide whether $x^d - \alpha$ has a root in $(\mathbb{Z}/p^\ell \mathbb{Z})^*$ within \mathbf{P} (via a single fast exponentiation), provided $p^\ell \notin \{8, 16, 32, \dots\}$.

To dispose of the remaining cases $p^\ell \in \{8, 16, 32, \dots\}$, first note that we can replace d by its reduction mod $2^{\ell-2}$ since every element of $(\mathbb{Z}/2^\ell \mathbb{Z})^*$ has order dividing $2^{\ell-2}$, and this reduction can certainly be computed in polynomial-time. Let us then write $d = 2^h d'$ where $2 \nmid d'$ and $h \in \{0, \dots, \ell-3\}$, and compute $d'' := 1/d' \pmod{2^{\ell-2}}$. Clearly then, $x^d - \alpha$ has a root in $(\mathbb{Z}/2^\ell \mathbb{Z})^*$ iff $x^{2^h} - \alpha'$ has a root in $(\mathbb{Z}/2^\ell \mathbb{Z})^*$, where $\alpha' := \alpha^{d''}$ (since exponentiation by any odd power is an automorphism of $(\mathbb{Z}/2^\ell \mathbb{Z})^*$). Note also that α' , d' , and d'' can clearly be computed in polynomial time.

Since $x^{2^h} - \alpha'$ always has a root in $(\mathbb{Z}/2^\ell \mathbb{Z})^*$ when $h=0$, we can then restrict our root search to the cyclic subgroup $\{1, 5^2, 5^4, 5^6, \dots, 5^{2^{\ell-2}-2}\}$ when $h \geq 1$ and α' is a square (since there can be no roots when $h \geq 1$ and α' is not a square). Furthermore, we see that $x^{2^h} - \alpha'$ can have no roots in $(\mathbb{Z}/2^\ell \mathbb{Z})^*$ if $\text{ord}_2 \alpha'$ is odd. So, by rescaling x , we can assume further that $\text{ord}_2 \alpha' = 0$, and thus that α' is odd. Now an odd α' is a square in $(\mathbb{Z}/2^\ell \mathbb{Z})^*$ iff $\alpha' \equiv 1 \pmod{8}$ [1, Ex. 38, pg. 192], and this can clearly be checked in \mathbf{P} . So we can at last decide the existence of a root in \mathbb{Q}_2 for $x^d - \alpha$ in \mathbf{P} : Simply combine fast exponentiation with Assertion 3 of Lemma A.2 again, applied to $x^{2^h} - \alpha'$ over the cyclic group $\{1, 5^2, 5^4, 5^6, \dots, 5^{2^{\ell-2}-2}\}$. \square

Theorem B.3. $\text{FEAS}_{\mathbb{Q}_{\text{primes}}}(\mathbb{Z}[x_1]) \in \mathbf{NP}$ for most inputs.

Proof. First note that $x \in \mathbb{Q}_p \setminus \mathbb{Z}_p \iff \frac{1}{x} \in p\mathbb{Z}_p$. Letting $f^*(x) := x^{\deg f} f(1/x)$ denote the reciprocal polynomial of f , note that the set of p -adic rational roots of f is simply the union of the p -adic integer roots of f and the reciprocals of the p -adic integer roots of f^* . So it suffices to derive succinct certificates for the roots of f in \mathbb{Z}_p , and do so for the stated fraction of inputs (f, p) . Let $\text{Newt}_p(f)$ denote the **p -adic Newton polygon** of f .

Observe that the p -adic valuations of all the roots of f in \mathbb{C}_p can be computed in polynomial-time. This is easily seen via two facts: (1) convex hulls of subsets of \mathbb{Z}^2 can be computed in polynomial-time (see, e.g., [6]), and (2) the valuation of any root of $f(x) = \sum_{i=1}^m c_i x^{a_i}$ is a ratio of the form $\frac{\text{ord}_p(c_i) - \text{ord}_p(c_j)}{a_j - a_i}$, where $(a_i, \text{ord}_p(c_i))$ and $(a_j, \text{ord}_p(c_j))$ are respectively the left and right vertices of a lower edge of $\text{Newt}_p(f)$ (cf. Lemma ??). Since $\text{ord}_p(c_i) \leq \log_p(c_i) \leq \text{size}(c_i)$, note in particular that every root $\zeta \in \mathbb{C}_p$ of f satisfies $|\text{ord}_p \zeta| \leq 2 \max_i \text{size}(c_i) \leq 2 \text{size}(f) < 2 \text{size}_p(f)$.

Since $\text{ord}_p(\mathbb{Z}_p) = \mathbb{N} \cup \{0\}$, we can clearly assume that $\text{Newt}_p(f)$ has an edge with nonnegative integral slope, for otherwise f would have no roots in \mathbb{Z}_p . Letting a denote the smallest nonzero exponent in f , $g(x) := f'(x)/x^{a-1}$, and $\zeta \in \mathbb{Z}_p$ any p -adic integer root of f , note then that $\text{ord}_p f'(\zeta) = (a-1)\text{ord}_p(\zeta) + \text{ord}_p g(\zeta)$. Note also that $\mathcal{D}_{\mathcal{A}}(f) = \text{Res}_{a_m, a_m - a_1}(f, g)$ so if $p \nmid \mathcal{D}_{\mathcal{A}}(f)$ then f and g have no common roots in the algebraic closure of \mathbf{F}_p by Lemma A.5. In particular, $p \nmid \mathcal{D}_{\mathcal{A}}(f) \implies g(\zeta) \not\equiv 0 \pmod{p}$; and thus $p \nmid \mathcal{D}_{\mathcal{A}}(f, g) \implies \text{ord}_p f'(\zeta) = (a-1)\text{ord}_p(\zeta)$. Furthermore, by the convexity of the lower hull of $\text{Newt}_p(f)$, it is clear that $\text{ord}_p(\zeta) \leq \frac{\text{ord}_p c_i - \text{ord}_p c_0}{i} \leq \frac{2 \max_i \log_p |c_i|}{a_1}$. So $p \nmid \mathcal{D}_{\mathcal{A}}(f) \implies \text{ord}_p f'(\zeta) < 2 \text{size}(f)$. Our fraction of inputs admitting a succinct certificate will then correspond precisely to those (f, p) such that $p \nmid \mathcal{D}_{\mathcal{A}}(f)$. In particular, let us define E to be the union of all pairs (f, p) such that $p \mid \mathcal{D}_{\mathcal{A}}(f)$, as \mathcal{A}

ranges over all finite subsets of $\mathbb{N} \cup \{0\}$. It is then easily checked that E is a countable union of hypersurfaces.

Fix $\ell = 4\text{size}(f)$. Clearly then, by Hensel's Lemma, for any $(f, p) \in (\mathbb{Z}[x_1] \times \mathbb{P}) \setminus E$, f has a root $\zeta \in \mathbb{Z}_p \iff f$ has a root $\zeta_0 \in \mathbb{Z}/p^\ell\mathbb{Z}$.

Since $\log(p^\ell) = O(\text{size}(f) \log p) = O(\text{size}_p(f)^2)$, and since arithmetic in $\mathbb{Z}/p^\ell\mathbb{Z}$ can be done in time polynomial in $\log(p^\ell)$ [1, Ch. 5], we have thus at last found our desired certificate: a root $\zeta_0 \in (\mathbb{Z}/p^\ell\mathbb{Z})^*$ of f with $\ell = 4\text{size}(f)$.

□

Theorem B.4. $\text{FEAS}_{\mathbb{Q}_{\text{primes}}}(\mathbb{Z}[x_1])$ is **NP-hard** under **ZPP-reductions**.

Proof. We will prove a (**ZPP**) randomized polynomial-time reduction from **3CNFSAT** to $\text{FEAS}_{\mathbb{Q}_{\text{primes}}}(\mathbb{Z}[x_1])$, making use of the intermediate input families $\{(\mathbb{Z}[x_1])^k \mid k \in \mathbb{N}\}$ and $\mathbb{Z}[x_1] \times \{x_1^D - 1 \mid D \in \mathbb{N}\}$ along the way.

Toward this end, suppose $B(y) := C_1(y) \wedge \dots \wedge C_k(y)$ is any **3CNFSAT** instance. The polynomial system $(\mathcal{P}_P(C_1), \dots, \mathcal{P}_P(C_k))$, for P the first n primes (employing Lemma A.8), then clearly yields the implication $\text{FEAS}_{\mathbb{C}}(\{(\mathbb{Z}[x_1])^k \mid k \in \mathbb{N}\}) \in \mathbf{P} \implies \mathbf{P} = \mathbf{NP}$. Composing this reduction with Proposition A.4, we then immediately obtain the implication $\text{FEAS}_{\mathbb{C}}(\mathbb{Z}[x_1] \times \{x_1^D - 1 \mid D \in \mathbb{N}\}) \in \mathbf{P} \implies \mathbf{P} = \mathbf{NP}$.

At this point, we need only find a means of transferring from \mathbb{C} to \mathbb{Q}_p . This we do by preceding our reductions above by a judicious (possibly new) choice of P . In particular, by applying Theorem A.3 with $\varepsilon = 1/3$ and $S_P = \emptyset$ (cf. Lemma A.6) we immediately obtain the implication $\text{FEAS}_{\mathbb{Q}_{\text{primes}}}(\mathbb{Z}[x_1] \times \{x_1^D - 1 \mid D \in \mathbb{N}\}) \in \mathbf{ZPP} \implies \mathbf{NP} \subseteq \mathbf{ZPP}$.

To conclude, observe that if $\chi \in \{1, \dots, p-1\}$ is a quadratic non-residue mod p then $\text{ord}_p \chi = 0$ and thus any root (x, y) of the quadratic form $x^2 - \chi y^2$ must satisfy

$\text{ord}_p x = \text{ord}_p y$.

By homogeneity we can then assume $\text{ord}_p x = \text{ord}_p y = 0$ (if $xy \neq 0$), and by reduction mod p we thus obtain that the first base- p digits of x and y must both be 0: a contradiction unless $x = y = 0$. Therefore, the only p -adic rational root of $x^2 - \chi y^2$ is $(0, 0)$. Since such a χ can be found in **ZPP** (via random sampling and polynomial-time Jacobi symbol calculation [1, Cor. 5.7.5 & Thm. 5.9.3, pg. 110 & 113]), we thus easily obtain a **ZPP**-reduction from $\text{FEAS}_{\mathbb{Q}_{\text{primes}}}(\mathbb{Z}[x_1] \times \{x_1^D - 1 \mid D \in \mathbb{N}\})$ to $\text{FEAS}_{\mathbb{Q}_{\text{primes}}}(\mathbb{Z}[x_1])$: simply map any instance $(f(x_1), x_1^D - 1, p)$ of the former problem to $(f(x_1)^2 - (x_1^D - 1)^2 \chi, p)$. So we are done.

□

CHAPTER VI

CONCLUSIONS AND FUTURE WORK

Our root counting method, given in Theorems B.5 and B.6, works only with regular polynomials. Is it possible to give a similar procedure for general polynomials? We believe that the result in Theorem A.7 could be a first step in that direction.

Some of the results in this dissertation could be a step towards a formulation and a solution of the Smale's 17th problem over the p -adic numbers. The problem, as originally stated by S. Smale [18], asks the following question:

Can a zero of n complex polynomial equations in n unknowns be found approximately, on average, in polynomial time with a uniform algorithm?

Over the p -adics, one needs to follow Blum, Shub, and Smale model of computation, see for example [4] and [11], and introduces a normal probability distribution over \mathbb{Q}_p . In addition, he or she might need to develop Newton's method over the p -adic numbers and give a condition for the approximate root of a given polynomial with coefficients in \mathbb{Q}_p .

REFERENCES

- [1] Bach, E. and Shallit, J.: Algorithmic Number Theory. I: Efficient Algorithms, MIT Press, Cambridge, MA, (1996)
- [2] Basu, S., Pollack R. and Roy, M.-F.: Algorithms in Real Algebraic Geometry. Algorithms and Computations in Mathematics 10. Springer, New York (2003)
- [3] Bihan, F. and Sottile, F.: New fewnomial upper bounds from Gale dual polynomial systems. Mosc. Math. J. 7 (2007)
- [4] Blum L., Shub M. and Smale S.: On a theory of computation and complexity over the real numbers: NP-completeness, recursive functions and universal machines. Bull. Amer. Math. Soc. 21 (1), 1-46 (1989)
- [5] Denef, J. and van den Dries, L., p -adic and real subanalytic sets. Annals of Mathematics 128 (1), 79-138 (1988)
- [6] Edelsbrunner, H.: Algorithms in Combinatorial Geometry. EATCS Monographs on Theoretical Computer Science, 10, Springer-Verlag, Berlin, (1987)
- [7] Gel'fand, I. M., Kapranov, M. M. and Zelevinsky, A. V.: Discriminants, Resultants and Multidimensional Determinants. Birkhäuser, Boston (1994)
- [8] Khovanski, A.: Fewnomials. AMS Press, Providence, RI (1991)
- [9] Lenstra (Jr.), H. W.: On the factorization of lacunary polynomials. Number Theory in Progress 1, 277-291 (1999)
- [10] Lipshitz, L.: p -adic zeros of polynomials. J. Reine Angew. Math. 390 , 208–214 (1988)

- [11] Maller, M. and Whitehead, J.: Computational complexity over the p -adic numbers. *J. Complexity* 13 (2), 195-207 (1997)
- [12] Murty, M.R.: Introduction to p -Adic Analytic Number Theory. American Mathematical Society, Providence, RI (2002)
- [13] Papadimitriou, C. H.: Computational Complexity. Addison-Wesley, Reading, MA (1994)
- [14] Plaisted, D. A.: New NP-hard and NP-complete polynomial and integer divisibility problems. *Theoret. Comput. Sci.* 31 (1-2), 125-138 (1984)
- [15] Robert, A. M.: A Course in p -Adic Analysis. Graduate Texts in Mathematics, 198, Springer-Verlag, New York (2000)
- [16] Rojas, J. M., Arithmetic multivariate Descartes' Rule. *American Journal of Mathematics* 126 (1), 1-30 (2004)
- [17] Schikhof, W.H.: Ultrametric Calculus, An Introduction to p -Adic Analysis. Cambridge Studies in Adv. Math. 4, Cambridge Univ. Press, New York (2007)
- [18] Smale, S.: Mathematical problems for the next century. *Mathematical Intelligencer* 20, 7-15 (1998)
- [19] Smirnov, A. L.: Torus schemes over a discrete valuation ring. *St. Petersburg Math. J.* 8 (4), 651-659 (1997)
- [20] Sturm, T. and Weispfenning V.: p -adic root isolation. *RACSAM, Rev. R. Acad. Cien. Serie A. Mat.* 98 (1-2), 239-258 (2004)
- [21] Weiss, E.: Algebraic Number Theory. McGraw-Hill, New York (1963)

VITA

Ashraf Ibrahim Abdelhalim was born Dongola, Republic of Sudan. He received his B.S. degree in mathematics and computer science from Khartoum University in Khartoum, Sudan in 1999. He received his M.S. degree in mathematics from the Southern Illinois University in 1999. He started his doctoral studies at Texas A&M University in September 2004 and received his Ph.D. in the area of computational algebraic geometry in December 2009. He can be reached at: Department of Mathematics, Texas A&M University, College Station, TX 77843-3368. e-mail: aibrahim@math.tamu.edu.

The typist for this dissertation was Ashraf Ibrahim Abdelhalim.