

# Algebraic Independence: Criteria and Structural Results over Diverse Fields

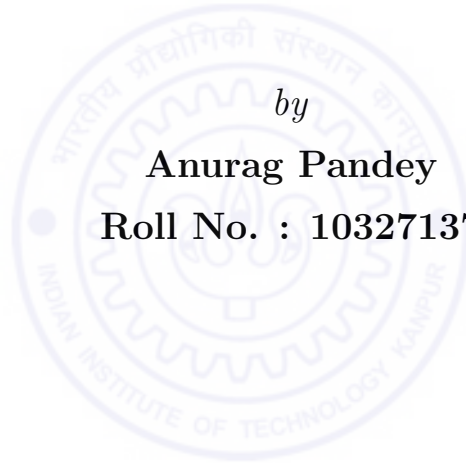
*A Thesis Submitted  
in Partial Fulfilment of the Requirements  
for the Degree of*

**Master of Technology**

*by*

**Anurag Pandey**

**Roll No. : 10327137**




Department of Electrical Engineering  
Indian Institute of Technology Kanpur

August, 2015

## CERTIFICATE


It is certified that the work contained in the thesis entitled "*Algebraic Independence: Criteria and Structural Results over Diverse Fields*", by "Anurag Pandey", has been carried out under our supervision and that this work has not been submitted elsewhere for a degree.

  
Dr. Yatindra Nath Singh

Deptt. of Electrical Engineering

Indian Institute of Technology

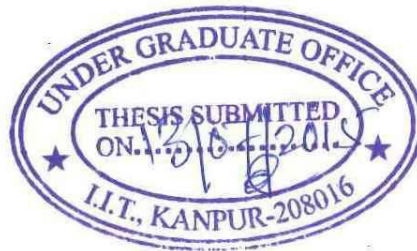
Kanpur-208016.

  
Dr. Nitin Saxena

Deptt. of Computer Science & Engineering

Indian Institute of Technology

Kanpur-208016.



# Abstract

We consider the property of algebraic independence of elements over a field. This is a higher degree generalization of linear independence. Polynomials  $f_1, \dots, f_m \in \mathbb{F}[x_1, \dots, x_n]$  are said to be algebraically dependent over the field  $\mathbb{F}$  if there exists a non-zero polynomial  $A \in \mathbb{F}[y_1, \dots, y_m]$  such that  $A(f_1, \dots, f_m) = 0$ . If no such polynomial exists, we say that  $f_1, \dots, f_m$  are algebraically independent.

We consider the problem of testing whether a given set of polynomials is algebraically independent. The problem has an efficient (randomized polynomial time) algorithm based on the Jacobian criterion when the polynomials are given over a field of zero characteristic. However this criterion fails when the polynomials are over fields of positive characteristic. The best known algorithm for the positive characteristic case is due to the Witt-Jacobian criterion which puts the problem in the complexity class  $\mathbf{NP}\#\mathbf{P}$ . The thesis aims to find alternative criteria and algorithms to test algebraic independence of polynomials.

We propose a technique based on polynomial maps and other faithful transformations which in some special cases, gives a polynomial time algorithm for testing independence over fields of positive characteristic. We also give an alternative criterion for positive characteristic case based on the  $p$ -adic valuation of the Jacobian determinant. This reduces the problem of testing algebraic independence to checking if a rational function solution exists to a linear first order partial differential equation modulo a prime. We further prove using Lüroth's theorem that two algebraically dependent polynomials over a field of positive characteristic can be lifted such that they become dependent over the rationals. This again gives a differential equation based criterion for testing independence over fields of positive characteristic. We also prove that the minimal annihilating polynomial of two supersparse polynomials over the rationals is sparse in most of the cases, giving as well the exact characterization of those cases. We further use this result to give an alternative randomized polynomial time algorithm for testing independence of two supersparse polynomials over the rationals. We finally give an efficient higher derivatives based Jacobian like criterion to test algebraic independence in a special case over  $\mathbb{F}_2$ .

# Acknowledgments

I wish to express my profound gratitude to my thesis supervisors Prof. Nitin Saxena and Prof. Y. N. Singh.

I am indebted to Prof. Nitin Saxena for the countless discussion sessions. He inspired me to do research and give my best by setting himself as an example with his dedication towards research. His courses and expositions are the very reasons I'm pursuing this area. While making crucial academic and research decisions, his guidance and advice has always been very enlightening. I am extremely proud of my fortune for having him as a supervisor.

I am grateful to Prof. Y. N. Singh for giving me the absolute freedom to pursue whatever I wanted to. I am thankful to him for being a fatherly figure to me by supporting me emotionally, giving his invaluable advice about research and other things and for being there whenever I needed him.

I am thankful to Prof. Manindra Agrawal for taking out time despite his busy schedule for insightful discussions on the topic. The simplicity and elegance with which he approaches a problem has always been inspiring.

I would also like to thank Prof. Daniel Huybrechts, Prof. János Kollár and Prof. Alin Bostan for useful email conversations. I am also thankful to Prof. Shobha Madan for patiently clearing all my doubts, irrespective of how ill-posed they were.

Thanks to Amit Kumar Sinhababu for all his help as a friend and a coworker. Parts of this thesis were done jointly with him. His insights and and curious questions were very helpful in looking at the problem from different viewpoints. I thank him for all the mathematical and non-mathematical discussions.

I also want to express my gratitude to all my friends who were always there to cheer me up in times of crisis. I thank them for giving me constructive suggestions throughout my life and for generously sharing with me what they learn from their lives and their invaluable perspectives towards it.

This work wouldn't have been possible without the incessant support and motivation provided by my parents and sisters. I thank them for always supporting me and my decisions.

Finally, I would like to thank the place IIT Kanpur....well, for everything!

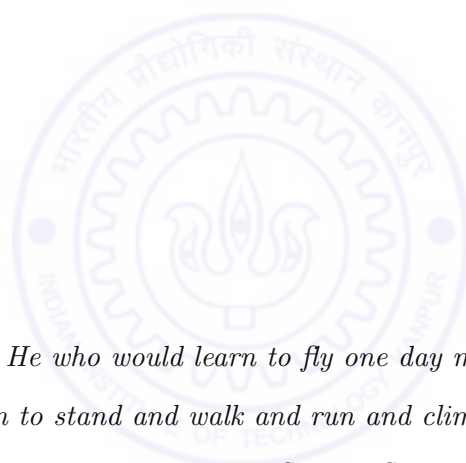
Anurag Pandey

July, 2015



*Dedicated to*

My parents who are my greatest asset



*He who would learn to fly one day must first  
learn to stand and walk and run and climb and dance;  
one cannot fly into flying.*

– Friedrich Nietzsche

# Contents

<b>Abstract</b>	<b>ii</b>
<b>Contents</b>	<b>vi</b>
<b>1 Introduction</b>	<b>1</b>
1.1 Overview	1
1.2 The Problem	2
1.3 Previous Work	3
1.4 Contribution of the thesis	4
1.5 Organization of the Thesis	5
<b>2 Transcendence and Algebraic Independence of Numbers and Power Series</b>	<b>6</b>
2.1 Basic Definitions	6
2.2 Properties of Algebraic Numbers	8
2.3 Known Transcendental Numbers	8
2.3.1 Liouville's Theorem: First transcendental Construction	9
2.3.2 Lindemann-Weierstrass Theorem: Transcendence of $e$ and $\pi$	11
2.3.3 Hilbert's Seventh Problem: Gelfond-Schneider Theorem	12
2.4 Siegel-Shidlovskii result on values of E-functions	12
2.4.1 G functions	13
2.5 Some Transcendence Proofs: Power Series	14
2.5.1 Mahler's Construction	15
<b>3 Algebraic Independence of Polynomials</b>	<b>17</b>
3.1 Basic definitions	17
3.2 Testing Algebraic Independence	18
3.2.1 Degree bound on Annihilating Polynomial	18
3.3 Hardness of Computing Annihilating Polynomial	19
3.4 Efficient Computation: The decision problem	19
3.4.1 The Jacobian Criterion	20
3.4.2 A Randomized Polynomial Time Algorithm	21
3.5 Algebraic Independence and Resultant	21
3.6 Algebraic Independence over Fields of positive characteristic	22
3.6.1 Jacobian Failure:	22
<b>4 Jacobian Correction</b>	<b>24</b>
4.1 Jacobian seen over Rationals:	24

4.2	Jacobian Correcting Transformations . . . . .	25
4.2.1	Taking p-th root of the polynomials . . . . .	26
4.2.2	Applying polynomial map . . . . .	27
4.2.3	Taking polynomials from the ring or the function field of the given polynomials . . . . .	28
4.3	Jacobian Correction in special cases . . . . .	29
4.3.1	Monomials: The Monomial Map . . . . .	29
4.4	Sum of Univariates . . . . .	33
4.4.1	The Algorithm . . . . .	34
4.4.2	Proof of Correctness . . . . .	35
4.4.3	Time Complexity . . . . .	35
4.5	Characterization of zero Jacobian . . . . .	35
<b>5</b>	<b>Alternative Criterion for positive characteristic: Jacobian Lifting</b>	<b>37</b>
5.1	Preliminaries . . . . .	38
5.1.1	Witt Jacobian Criterion . . . . .	38
5.1.2	Lüroth's Theorem . . . . .	39
5.2	Main Results . . . . .	39
5.3	Proof of the theorems: . . . . .	40
5.3.1	Proof of theorem 5.9: p-adic valuation lifting . . . . .	40
5.3.2	Proof of theorem 5.10: Lifting to Rationals . . . . .	45
5.4	Lifting to rationals: Independence testing criteria . . . . .	45
<b>6</b>	<b>Alternative Criterion over Zero Characteristic: Supersparse Polynomials</b>	<b>47</b>
6.1	Preliminaries . . . . .	47
6.2	Main Results . . . . .	48
6.2.1	Degree bound on annihilating polynomial . . . . .	48
6.2.2	Algebraic independence testing algorithm . . . . .	48
6.2.3	Annihilating polynomial of homogeneous polynomials . . . . .	48
6.3	Proof of Theorem 6.2 . . . . .	49
6.4	Independence Testing Algorithm: . . . . .	53
6.4.1	Proof of Correctness . . . . .	53
6.5	Homogeneous Polynomials . . . . .	54
<b>7</b>	<b>Higher Derivatives</b>	<b>56</b>
7.1	Preliminaries . . . . .	56
7.1.1	Separability . . . . .	56
7.1.2	The Operator $\mathcal{H}_2$ . . . . .	58
7.2	Main Results . . . . .	59
7.2.1	Separable Extension: Jacobian Criterion . . . . .	59
7.2.2	Inseparable extension: inseparable index 1 . . . . .	61
<b>8</b>	<b>Conclusions and Future Directions</b>	<b>65</b>
8.1	Summary/Conclusion . . . . .	65
8.2	Future Directions . . . . .	66
	<b>Bibliography</b>	<b>67</b>



# Chapter 1

## Introduction

### 1.1 Overview

In 1910, Ernst Steinitz published the prominent paper “Algebraische Theorie der Körper” (Algebraic Theory of Fields) [Ste10]. The paper is the first to axiomatically study the properties of fields and define many crucial field theoretic concepts like prime field, perfect field and the transcendence degree of a field extension.

The motivation of this thesis is to explore the problem of finding transcendence degree of a field extension in a special case, when the generators of the extension field over the base field are known and they come from a bigger extension field whose transcendence degree ( $\geq 1$ ) over the base field is already known.

Some known interesting cases of the above problem are:

**Problem 1 (Transcendence of Numbers):** Finding the transcendence degree of the field extension  $\mathbb{Q}(\alpha)/\mathbb{Q}$ ,  $\alpha \in \mathbb{C}$ , i.e. finding if  $\alpha$  is transcendental over  $\mathbb{Q}$ , or simply: *finding whether a given number  $\alpha \in \mathbb{C}$  is transcendental?*

**Problem 2 (Algebraic Independence of Numbers):** Finding the transcendence degree of the field extension  $\mathbb{Q}(\alpha_1, \dots, \alpha_n)/\mathbb{Q}$ ,  $\alpha_i$ 's  $\in \mathbb{C}$ . In particular, if all the  $\alpha_i$ 's are transcendental, finding whether the transcendence degree of the extension is  $n$ , or simply: *finding whether the given numbers  $\alpha_1, \dots, \alpha_n$  are algebraically independent?*

Note that Problem 2 is a just generalization of Problem 1.

**Problem 3 (Algebraic Independence of Polynomials):** Finding the transcendence degree of the field extension  $\mathbb{F}(f_1, \dots, f_m)/\mathbb{F}$ , where  $f_1, \dots, f_m \in \mathbb{F}[x_1, \dots, x_n]$ . In particular if  $f_1, \dots, f_m$  are all non-constant polynomials, finding whether the transcendence degree of the extension is  $n$ , or simply: *finding whether the given polynomials  $f_1, \dots, f_m$  are algebraically independent?*

The thesis begins with a brief survey on Problem 1 and 2. Due to Cantor's uncountability of real numbers [Can92], it follows that almost all complex numbers are transcendental [BT04]. Still, it has been very difficult to identify them. There are results like transcendence of Liouville's and Mahler's numbers, transcendence of  $e$  and  $\pi$  (Hermite, Lindemann-Weierstrass Theorem) and, transcendence of  $e^\pi$  and  $\sqrt{2}^{\sqrt{2}}$  (Hilbert's seventh problem, Gelfond-Schneider Theorem). However, transcendence of many interesting numbers are still open: for eg:  $e^e$ ,  $\pi^e$ ,  $\zeta(3)$ ,  $\gamma_0$  (Euler-Mascheroni's Constant),  $e\pi$ ,  $e + \pi$ . Similarly, little progress is there in case of Problem 2 i.e. algebraic independence of numbers. Main results are Shidlovskii's results on E-function and Nesterenko's result on algebraic independence of  $\pi$ ,  $e^\pi$  and  $\Gamma(1/4)$ . Open problems include: Is the transcendence degree of the extension  $\mathbb{Q}(e, \pi)/\mathbb{Q} = 2$ ? i.e. whether  $e$  and  $\pi$  are algebraically independent.

Problem 3 is of a different nature. Here the elements (polynomials) come from a finitely generated extension ( $\mathbb{F}(x_1, \dots, x_n)$ ) over the base field; unlike the case of numbers where the extension  $\mathbb{C}/\mathbb{Q}$  has infinite transcendence degree. We look at the computational aspects of the problem and ask for algorithms to test (efficiently) algebraic independence of polynomials. which is the focus of this thesis.

## 1.2 The Problem

We first give a formulation of the property of algebraic independence of polynomials over a field in terms of the annihilating polynomial.

Polynomials  $f_1, \dots, f_m \in \mathbb{F}[x_1, \dots, x_n]$  are said to be algebraically dependent over the field  $\mathbb{F}$  if there exists a non-zero polynomial  $A \in \mathbb{F}[y_1, \dots, y_m]$  such that  $A(f_1, \dots, f_m) = 0$ . We call  $A$  an annihilating polynomial of  $f_1, \dots, f_m$ . If no such polynomial  $A$  exists, we say that  $f_1, \dots, f_m$  are algebraically independent.

The problem we investigate is:

*Given polynomials  $f_1, \dots, f_m \in \mathbb{F}[x_1, \dots, x_n]$  over a field  $\mathbb{F}$ , decide whether they are algebraically independent in polynomial (or randomized polynomial) time (in the bit-size of the input).*

Algebraic independence of polynomials is a fundamental concept in commutative algebra. It is to polynomial rings what linear independence is to vector spaces [MSS12]. The computational problem is motivated by several applications in computer science as well. For instance, [Kal85, ASSS12] use it proving circuit lower bounds, [DGW09, Dvi12] use it in construction of randomness extractors, [BMS13, ASSS12, MSS12] use it in identity testing, [L'v84] uses it in program invariants, and [For92, DF93] show its application in control theory.

### 1.3 Previous Work

A priori it is not clear whether testing algebraic independence of polynomials is even computable. It is because of Perron's degree bound on the annihilating polynomial [Per32, Plo05], we have a polynomial space algorithm for the problem. Gröbner bases can also be used to test algebraic independence (see [KR08], Proposition 3.6.1). This suggests a doubly exponential time algorithm. We however would want an efficient algorithm for the problem. A randomized polynomial time algorithm is indeed there using the rank of the Jacobian matrix [DGW09, BMS13]. This however works only for fields of zero (or large) characteristic [DGW09]. For fields of (small) positive characteristic, the criterion is only one-sided correct [Sin15]. The only criterion which works for all prime characteristic is due to [MSS12] - the Witt Jacobian criterion, which improves the complexity of independence testing over  $\mathbb{F}_p$  from **PSPACE** to **NP<sup>#P</sup>**.

So in the literature, we have the problem of testing algebraic independence of polynomials over fields of zero or large characteristic in the complexity class **BPP**, whereas over the fields of (small) prime characteristic, it is in the complexity class **NP<sup>#P</sup>**. We however believe the independence testing over  $\mathbb{F}_p$  should also be in **BPP** (recall that  $\text{BPP} \subseteq \text{NP}^{\#P} \subseteq \text{PSPACE} \subseteq \text{EXP}$ ). Thus, there is still a huge gap between what is known and what we would ideally want (a randomized polynomial time algorithm). There is not much progress known even for interesting special cases. The thesis attempts to bridge this gap.

## 1.4 Contribution of the thesis

The first approach we pursue is to transform the input polynomials such that the usual Jacobian criterion works. We achieve it in certain special cases by transforming given polynomials using appropriate maps, taking  $p$ -th roots, and using ring operations. We get the correction algorithm for two binomials with exponential degree, and for two polynomials given as sum of univariates. These correction algorithms are all polynomial time in input size.

We also prove that  $n$  polynomials are algebraically dependent if and only if the  $p$ -adic valuation of their Jacobian determinant can be increased arbitrarily by lifting the polynomials. Thus, we reduce testing algebraic independence of polynomials over fields of positive characteristic to finding if a rational function solution exists to a linear first order partial differential equation modulo  $p$ .

We also show that if two polynomials are dependent over  $\mathbb{F}_p$ , they can be lifted such that they become dependent over rationals. We find the above lifting using Lüroth's theorem. Combining above idea with a known theorem on sparse decomposition, we come up with an alternative randomized polynomial time algorithm for testing algebraic independence of two super-sparse polynomials over fields of zero characteristic. The algorithm doesn't depend on the Jacobian criterion and seems to have a chance of generalization to the positive characteristic case.

We finally give a higher derivatives based efficient criterion to test algebraic independence in a special case over  $\mathbb{F}_2$ .

## 1.5 Organization of the Thesis

Chapter 2 and 3 discuss the preliminaries and the survey related to transcendence and algebraic independence. Chapter 2 focuses on results on numbers and power series whereas chapter 3 covers the case of algebraic independence of polynomials. The chapters 4, 5, 6 and 7 span the results. We finally conclude in chapter 8 summarizing our work and stating the possible future directions this thesis seems to suggest.



## Chapter 2

# Transcendence and Algebraic Independence of Numbers and Power Series

In this chapter, we introduce the notion of transcendence and algebraic independence. We explore the concept in the context of numbers and power series. We present a survey on progress on the transcendence theory of numbers and power series.

### 2.1 Basic Definitions

**Definition 2.1.** (Algebraic Number) A number  $\alpha \in \mathbb{C}$  is said to be *algebraic* if it is a zero of some nonzero polynomial  $p(z) \in \mathbb{Z}[z]$ . Or more generally,

**Definition 2.2.** (Algebraic Element) Let  $\mathbb{F}$  be a field and  $\mathbb{E}/\mathbb{F}$  be an extension field. An element  $\alpha \in \mathbb{E}$  is said to be algebraic over  $\mathbb{F}$  if it is a zero of some nonzero polynomial  $p(z) \in \mathbb{F}[z]$ .

**Definition 2.3.** (Irreducible Polynomial) A polynomial  $p(z) \in \mathbb{Z}[z]$  is called *irreducible* if it cannot be factored into two polynomials in  $\mathbb{Q}[z]$  each having degree smaller than  $\deg(p)$ .

**Definition 2.4.** (Minimal Polynomial) If  $\alpha$  is algebraic, then there exists a unique irreducible polynomial  $p(z) \in \mathbb{Z}[z]$  with properties that  $\alpha$  is a zero of  $p(z)$ ; the leading coefficient of  $p(z)$  is positive; and the coefficients of  $p(z)$  are relatively prime integers. We call this polynomial  $p(z)$  the *minimal polynomial* associated with  $\alpha$ . We define degree of  $\alpha$ ,  $\deg(\alpha)$ , to be the degree of its minimal polynomial  $p(z)$ . The zeros of  $p(z)$  other than  $\alpha$  are called *conjugates* of  $\alpha$ .

**Example 2.1.** (Algebraic numbers/elements)

$0$  is trivially algebraic.

$2$  is an algebraic number with the minimal polynomial  $z - 2$ .

$\frac{2}{5}$  is an algebraic number with minimal polynomial  $5z - 2$ .

$\sqrt[3]{5}$  is an algebraic number with minimal polynomial  $z^3 - 5$ .

$\sqrt{2} + \sqrt{3}$  is an algebraic number with minimal polynomial  $z^4 - 10z^2 + 1$ .

$i$  is an algebraic number with minimal polynomial  $z^2 + 1$ .

$\sqrt{x}$  is algebraic over  $\mathbb{F}(x)$  with minimal polynomial  $z^2 - x$ .

**Definition 2.5.** (Transcendental Number) A number  $\alpha \in \mathbb{C}$  is said to be transcendental if it is not algebraic. Similarly, in general

**Definition 2.6.** (Transcendental Element) An element  $\alpha \in \mathbb{E}/\mathbb{F}$  is said to be transcendental over  $\mathbb{F}$  if it is not algebraic over  $\mathbb{F}$ .

**Example 2.2.** (Transcendental number/elements)

$e, \pi$  are transcendental numbers.

$y \in \mathbb{Q}(x, y)$  is transcendental over  $\mathbb{Q}(x)$ .

**Definition 2.7.** (Algebraic and Transcendental Extension) A field extension  $\mathbb{E}/\mathbb{F}$  is said to be algebraic if all the elements of  $\mathbb{E}$  are algebraic over  $\mathbb{F}$ . A field extension is said to be transcendental if it is not algebraic.

**Example 2.3.** (Algebraic and Transcendental Extension)

$\mathbb{Q}(\sqrt{2})$  is algebraic over  $\mathbb{Q}$ .

$\mathbb{Q}(x, y)$  is transcendental over  $\mathbb{Q}(x)$ .

We can easily generalize the notion of transcendence, which is a property of an element, to algebraic independence, which is a property of a set of elements.

**Definition 2.8.** (Algebraically Independence of Numbers) A given set of numbers  $\{\alpha_1, \alpha_2, \dots, \alpha_k\} \in \mathbb{C}$  is said to be *algebraically independent* if there exists no non-zero polynomial  $p(z_1, z_2, \dots, z_k) \in \mathbb{Z}[z_1, z_2, \dots, z_k]$  such that  $p(\alpha_1, \alpha_2, \dots, \alpha_k) = 0$ . If such a polynomial exists, we call the set  $\{\alpha_1, \alpha_2, \dots, \alpha_k\}$  *algebraically dependent* and we call such a polynomial  $p(z_1, z_2, \dots, z_k)$  an *annihilating polynomial* of  $\{\alpha_1, \alpha_2, \dots, \alpha_k\}$ .

**Example 2.4.**  $\sqrt{\pi}$  and  $\pi$  are algebraically dependent with annihilating polynomial  $z_1^2 - z_2$ .

*If in a given set, one or more numbers are algebraic, the set is trivially algebraically dependent. The annihilating polynomial(s) of the algebraic number(s) present in the set by definition is (are) also the annihilating polynomial(s) of the whole set. Hence, the problem of algebraic independence of a set of numbers is interesting only when every number in the given set is transcendental.*

## 2.2 Properties of Algebraic Numbers

**Proposition 2.9.** *The set of all algebraic numbers,  $\mathbb{A}$  is a field.*

**Proposition 2.10.** *The set of algebraic numbers is a countable set.*

## 2.3 Known Transcendental Numbers

Cantor's proof of uncountability of set of real numbers [Can92], together with Proposition 2.10 implies that almost all complex numbers are transcendental. However, there has been little progress in constructing methods to show a given number to be transcendental.



### 2.3.1 Liouville's Theorem: First transcendental Construction

**Theorem 2.11. (Liouville's theorem)** Let  $\alpha$  be an algebraic over  $\mathbb{Q}$  and satisfies the monic irreducible polynomial equation  $\alpha^n + a_{n-1}\alpha^{n-2} + \cdots + a_0 = 0$  with  $a_i \in \mathbb{Q}$ . Now, suppose  $\epsilon$  and  $c > 0$  are given. Then, there are only finitely many rationals  $p/q$  in lowest terms such that

$$\left| \alpha - \frac{p}{q} \right| < \frac{c}{q^{n+\epsilon}} \quad (2.1)$$

*Proof.* There is a polynomial  $f(x) = b_n x^n + b_{n-1} x^{n-1} + \cdots + b_0$  with  $b_i \in \mathbb{Z}, b_n \neq 0$ . So,  $f(\alpha) = 0$ .

Suppose  $\left| \alpha - \frac{p}{q} \right| < \frac{c}{q^{n+\epsilon}}$ . Also, since  $f(x)$  is irreducible, we have  $\left| f\left(\frac{p}{q}\right) \right| \neq 0$ . Thus,

$$\left| f\left(\frac{p}{q}\right) \right| = \left| b_n \left(\frac{p}{q}\right)^n + b_{n-1} \left(\frac{p}{q}\right)^{n-1} + \cdots + b_0 \right| \quad (2.2)$$

$$= \frac{|b_n(p)^n + b_{n-1}(p)^{n-1}q + \cdots + b_0q^n|}{|q^n|} \quad (2.3)$$

Clearly, numerator is a positive integer. Thus

$$\left| f\left(\frac{p}{q}\right) \right| \geq \frac{1}{|q^n|} = \frac{1}{q^n} \quad (2.4)$$

So, the value of  $\left| f\left(\frac{p}{q}\right) \right|$  cannot be too small. Now, by the Mean Value Theorem from calculus, we have

$$\frac{1}{q^n} \leq \left| f\left(\frac{p}{q}\right) \right| = \left| f\left(\frac{p}{q}\right) - f(\alpha) \right| = |f'(\lambda)| \left| \frac{p}{q} - \alpha \right|; \quad \lambda \in \left(\frac{p}{q}, \alpha\right) \quad (2.5)$$

Now, as supposed,

$$|\alpha - \frac{p}{q}| < \frac{c}{q^{n+\epsilon}} \leq c, \text{ or} \quad (2.6)$$

$$|\frac{p}{q}| \leq |\alpha| + c \quad (2.7)$$

$$|\lambda| \leq |\alpha| + c \text{ since } \lambda \in (\frac{p}{q}, \alpha) \quad (2.8)$$

Now, since  $f(x)$  is a polynomial, there exists a bound  $M$  such that  $|f'(x)| \leq M$  for  $|x| \leq |\alpha| + c$ . This gives

$$|f(\frac{p}{q}) - f(\alpha)| \leq M|\frac{p}{q} - \alpha| \quad (2.9)$$

$$\frac{1}{q^n} \leq M|\frac{p}{q} - \alpha| < M\frac{c}{q^{n+\epsilon}}q^\epsilon \leq cM \quad \epsilon, c > 0 \text{ using (2.5)} \quad (2.10)$$

This bounds  $q$  as the above gives  $q \leq (cM)^{1/\epsilon}$  which using (2.7) yields  $|p| \leq (cM)^{1/\epsilon}(|\alpha| + c)$ . So,  $|p|$  and  $q$  both are bounded. Hence we get that there will be only finitely many good rational approximations  $\frac{p}{q}$  for a given algebraic number  $\alpha$ .  $\square$

**Corollary 2.12.** *To show  $\alpha \in \mathbb{R}$  is transcendental, it is enough to find an infinite sequence of very good rational approximations  $\{\frac{p_i}{q_i}\}$  (as sought in the above theorem).*

**Example 2.5. Liouville's Number:**  $\sum_{n=0}^{\infty} 10^{-n!}$

For the above number, consider the rational sequence of rational approximations  $\frac{p_i}{q_i} =$

$$\sum_{n=0}^i 10^{-n!}$$

$$i.e. \frac{p_i}{q_i} = \sum_{n=0}^i 10^{-n!} = \frac{\sum_{n=0}^i 10^{(i!-n!)}}{10^{i!}}$$

$$\text{So, } |\alpha - \frac{p_i}{q_i}| = |\sum_{n=i+1}^{\infty} 10^{-n!}| = |10^{-(i+1)!}(1 - 10^{-(i+2)!} + \dots)| \leq 2 \cdot 10^{-(i+1)!} = \frac{2}{(10^{i!})^{i+1}} = \frac{2}{(q_i)^{i+1}}$$

Thus, we have an infinite sequence of good approximations for the given number. Hence, it is transcendental.

**Theorem 2.13. (Roth's Theorem,)** [Rot55]. *If  $\alpha$  is algebraic  $\notin \mathbb{Q}$ ,  $\epsilon > 0$ , there are only finitely many  $\frac{p}{q} \in \mathbb{Q}$  such that*

$$|\alpha - \frac{p}{q}| < \frac{1}{q^{2+\epsilon}}. \quad (2.11)$$

### 2.3.2 Lindemann-Weierstrass Theorem: Transcendence of $e$ and $\pi$

Johann Heinrich Lambert in 1761 conjectured that  $e$  and  $\pi$  were both transcendental in his paper [Lam98] proving irrationality of  $\pi$ .

Finally Hermite settled the conjecture about  $e$  after a century.

**Theorem 2.14.** (*Hermite, 1873 [Her74]*)  $e$  is transcendental.

Lindemann generalized the proof technique of Hermite to prove a result which settled the transcendence of  $\pi$ .

**Theorem 2.15.** (*Lindemann, 1882 [Lin82]*)  $e^\alpha$  is transcendental when  $\alpha$  is algebraic.

**Corollary 2.16.**  $\pi$  is transcendental.

*Proof.* Assume for the sake of contradiction that  $\pi$  is algebraic. So,  $i\pi$  is also algebraic. This implies from above theorem that  $e^{i\pi}$  is transcendental. This contradicts Euler's identity  $e^{i\pi} = -1$ . □

Weierstrass provided a stronger generalization.

**Theorem 2.17.** (*Lindemann-Weierstrass Theorem*), [Wei04]. If  $\alpha_1, \dots, \alpha_n$  are algebraic numbers which are linearly independent over  $\mathbb{Q}$ , then  $e^{\alpha_1}, \dots, e^{\alpha_n}$  are algebraically independent over  $\mathbb{Q}$  i.e. the extension field  $\mathbb{Q}(e^{\alpha_1}, \dots, e^{\alpha_n})$  has transcendence degree  $n$  over  $\mathbb{Q}$ .

**Open Problem:** To prove algebraic independence (or dependence) of  $e$  and  $\pi$ . Even much weaker question like transcendence of  $e\pi$ ,  $e + \pi$  remain unresolved.

*Conjecture 1. (Schanuel)* Given  $\alpha_1, \dots, \alpha_n \in \mathbb{C}$  which are linearly independent over  $\mathbb{Q}$ , the extension  $\mathbb{Q}(\alpha_1, \dots, \alpha_n, e^{\alpha_1}, \dots, e^{\alpha_n})/\mathbb{Q}$  has transcendence degree at least  $n$ . See [Lan66].

The conjecture is very strong as it generalizes several known results in transcendental number theory including the Lindemann-Weierstrass theorem. It also resolves algebraic independence of  $e$  and  $\pi$  by simply taking  $n = 2$  and setting  $\alpha_1 = 1$  and  $\alpha_2 = i\pi$ . It was given in 1960s, and is still unresolved. However James Ax in 1971 resolved the power series version of the conjecture.

**Theorem 2.18.** (*Ax, 1971*) [*Ax71*] Let  $f_1, \dots, f_n \in t\mathbb{C}[[t]]$  be linearly independent over  $\mathbb{Q}$ . Then the extension  $\mathbb{C}(t, f_1, \dots, f_n, e^{f_1}, \dots, e^{f_n})/\mathbb{C}(t)$  has transcendence degree at least  $n$ .

### 2.3.3 Hilbert's Seventh Problem: Gelfond-Schneider Theorem

In 1900, along with 22 other problems fundamental to mathematics, Hilbert posed the following problem:

**Hilbert's seventh problem:** Is  $a^b$  always transcendental for algebraic  $a \notin \{0, 1\}$  and irrational algebraic  $b$ ?

**Gelfond-Schneider theorem** provides an affirmative answer to Hilbert's Seventh Problem. It was proved independently by Gelfond [*Gel34*] and Schneider [*Sch34*] in 1934.

**Corollary 2.19.**  $2^{\sqrt{2}}$  is transcendental

**Corollary 2.20.**  $e^\pi = (e^{i\pi})^{-i} = (-1)^{-i}$  is transcendental

## 2.4 Siegel-Shidlovskii result on values of E-functions

**Definition 2.21.** (See [*Mor51*], [*Sie14*], [*NoFRS09*]). A function

$$f(z) = \sum_{n=0}^{\infty} c_n \frac{z^n}{n!} \tag{2.12}$$

is said to be an **E-function** if

(i) All coefficients  $c_n$  belong to the same algebraic number field  $K$  of finite degree over the rational number field  $\mathbb{Q}$ ,

- (ii) If  $\epsilon > 0$  is any positive number, then  $|\bar{c}_n| = O(n^{\epsilon n})$  as  $n \rightarrow \infty$ , and
- (iii) For any  $\epsilon > 0$ , there exists a sequence of natural numbers  $\{q_n\}_{n \geq 1}$  such that  $q_n c_k \in \mathbb{Z}_K$  for  $k = 0, \dots, n$  and that  $q_n = O(n^{\epsilon n})$ .

Note that their power series expansion is very redolent of the exponential series, hence the term E-function.

Let us now call  $\mathbf{E}$  the set of all E-functions. It is easy to see that E-functions satisfy the following properties [NoFRS09]:

- (i)  $\mathbf{E}$  is a ring under the operations of addition and multiplication.
- (ii)  $f(z) \in \mathbf{E}$  implies that  $f'(z)$  and  $\int_0^z f(t)dt$  are both E-functions.
- (iii)  $f(z) \in \mathbf{E}$  implies that  $f(\alpha z)$  is also in  $\mathbf{E}$  if  $\alpha$  is an algebraic number.

An easy consequence of (iii) is that for any algebraic number  $\alpha$ ,  $e^{\alpha z} \in \mathbf{E}$ .

For the class of E-functions, Shidlovskii proved the following strong theorem relating algebraic independence of values of E-functions to the algebraic independence of the functions whose evaluations the numbers are. See [ŠKB89].

**Theorem 2.22.** (Shidlovskii, 1955) *Let*

$$f_1(z), \dots, f_m(z), \quad m \geq 1, \quad (2.13)$$

*be a set of E-functions which form a solution of the system of differential equations*

$$y'_k = q_{k_0} + \sum_{j=1}^m q_{kj} y_j, \quad q_{kj} \in \mathbb{C}(z), \quad k = 1, \dots, m, \quad (2.14)$$

*and are algebraically independent over  $\mathbb{C}(z)$ . Then  $\alpha \in \mathbb{A}, \alpha \neq 0$  and different from singularities of (2.14), the numbers  $f_1(\alpha), \dots, f_m(\alpha)$  are algebraically independent over  $\mathbb{Q}$ .*

### 2.4.1 G functions

However there are several numbers of interests which are not known to be evaluations of E-functions at algebraic points. For example,  $\pi$  is obtained by evaluating  $4 \arctan(z)$  at  $z = 1$  or by evaluating  $-i \log z$  at  $z = -1$ . However, it can be easily seen that  $\log z$  and

$\arctan(z)$  do not satisfy the definition of E-functions. They belong to a more general class of functions, called G-functions. Siegel introduced them along with the E-functions. The hope was to generalize the results on E-function to a more general class of power series. G-functions' power series expansion are redolent to geometric series. We now give the definition of G-functions.

**Definition 2.23.** A function

$$f(z) = \sum_{n=0}^{\infty} a_n z^n \quad (2.15)$$

is said to be a **G-function** if

- (i) All coefficients  $a_n$  belong to the same algebraic number field  $K$  of finite degree over the rational number field  $\mathbb{Q}$ ,
- (ii)  $f(z)$  satisfies a linear differential equation with coefficients in  $\mathbb{Q}(z)$ , and
- (iii) Both  $|a_n|$  and the common denominator  $\text{den}(a_0, \dots, a_n)$  are bounded by  $c^n$  where  $c > 0$  depends only on  $f$ .

Note that unlike E-functions, at non-zero algebraic points, G-functions may take algebraic values as well. For instance, algebraic functions also satisfy the definition of G-functions. Other examples are  $\arctan(z)$ ,  $-\log(1-z)$ .

However, very little progress is there in case of G-functions. For example, no result analogous to Shidlovskii's result on E-function is known.

## 2.5 Some Transcendence Proofs: Power Series

**Lemma 2.24.** *The exponential function  $f(x) = e^x$  is transcendental.*

*Proof.* Suppose it to be algebraic, and write

$$P_d(x)e^{dx} + P_{d-1}(x)e^{(d-1)x} + \dots + P_0(x) = 0 \quad (2.16)$$

where we choose  $d$  to be least, whence  $P_d \neq 0$ . Then for any  $x \in \mathbb{C}$ ,

$$P_d(x) = -P_{d-1}(x)e^{-x} - \dots - P_0(x)e^{-dx} \quad (2.17)$$

Let  $x \in \mathbb{R}$ ,  $x \rightarrow +\infty$ . Then the right-hand side of the above equation vanishes, which implies  $\lim_{x \rightarrow +\infty} P_d = 0$ , a contradiction.  $\square$

Now, we can run the same argument to prove that  $e^x$  and  $e^{x^2}$  are algebraically independent functions over  $\mathbb{C}(x)$ .

**Theorem 2.25.**  $\log z$  and  $e^z$  are algebraically independent functions over  $\mathbb{C}(z)$ .

*Proof.* Let us assume for the sake of contradiction that  $\log z$  and  $e^z$  are algebraically dependent over  $\mathbb{C}(z)$  such that  $\tilde{A} \in \mathbb{C}[x_1, x_2, x_3]$  annihilates  $\{\log z, z, e^z\}$ . Then there exists a minimal annihilating polynomial  $A \in \mathbb{R}[y_1, y_2, y_3]$  which annihilates  $\{u, e^u, e^{e^u}\}$ . Let  $d := \deg_{x_3} A$ , so that  $A = \sum_{i=d}^0 p_i(x_1, x_2)x_3^i$  which gives

$$\sum_{i=d}^0 p_i(u, e^u)e^{e^u \cdot i} = 0 \quad \text{which gives} \quad (2.18)$$

$$p_d(u, e^u) + \sum_{i=d-1}^0 \frac{p_i(u, e^u)}{(e^{e^u})^{d-i}} = 0 \quad (2.19)$$

sending  $u \rightarrow \infty$  sends  $\sum_{i=d-1}^0 \frac{p_i(u, e^u)}{(e^{e^u})^{d-i}}$  to zero. Thus

$$p_d(u, e^u) = 0 \quad (2.20)$$

Similarly  $p_d(x_1, x_2) = 0$ . Hence  $\text{trdeg}_{\mathbb{R}}\{u, e^u, e^{e^u}\} = 3$   $\square$

This generalizes easily to the result that any arbitrary set of transcendental functions which are all asymptotically apart are algebraically independent over  $\mathbb{C}(z)$ .

### 2.5.1 Mahler's Construction

**Lemma 2.26.** [Duv10] Let  $\Omega = \{x \in \mathbb{C} / |x| < 1\}$ . Then the function

$$f(x) = \sum_{n=0}^{\infty} x^{2^n} \quad (2.21)$$

which is analytic in  $\Omega$ , is transcendental

*Proof.* Note that  $f$  satisfies the functional equation, namely

$$f(x^2) = \sum_{n=0}^{\infty} x^{2^{n+1}} = f(x) - x \quad (2.22)$$

Now for contradiction, we assume  $f$  to be algebraic. Then for every  $x \in \Omega$ ,

$$(f(x))^d + Q_{d-1}(x)(f(x))^{d-1} + \dots + Q_0(x) = 0 \quad (2.23)$$

where the  $Q_i$ 's are rational functions with complex coefficients, and  $d$  is chosen to be least. Now if in above equation, we replace  $x$  by  $x^2$ , we get

$$(f(x) - x)^d + Q_{d-1}(x^2)(f(x) - x)^{d-1} + \dots + Q_0(x^2) = 0 \quad (2.24)$$

Expansion gives

$$(f(x))^d + (Q_{d-1}(x^2) - dx)(f(x))^{d-1} + \dots = 0 \quad (2.25)$$

Subtract this to (12.8). Since  $d$  is the least, we get  $Q_{d-1}(x) = Q_{d-1}(x^2) - dx$ . Now put  $Q_{d-1}(x) = A(x)/B(x)$ , with  $A$  and  $B$  coprime. We have

$$A(x)B(x^2) = A(x^2)B(x) - dxB(x)B(x^2) \quad (2.26)$$

Thus  $B(x^2) | A(x^2)B(x)$ . As  $B(x^2)$  and  $A(x^2)$  are coprime, this implies  $B(x^2) | B(x)$ . Using degree argument, we deduce that  $B(x) = b \in \mathbb{C}$  and (4.9) becomes  $A(x) = A(x^2) - bdx$ . If  $\deg A \geq 1$ , this is impossible. Therefore  $\deg A = 0$  and  $A(x) = a \in \mathbb{C}$ , which implies  $b = 0$ , a contradiction.  $\square$

The above function takes transcendental values at algebraic points.

**Theorem 2.27.** [Duv10] *Let  $\alpha$  be a non-zero algebraic number with  $|\alpha| < 1$ , Then  $f(\alpha) = \sum_{n=0}^{+\infty} \alpha^{2^n}$  is transcendental.*



## Chapter 3

# Algebraic Independence of Polynomials

Having seen the concept of algebraic independence in the case of numbers in the last chapter, we move on to study the case of polynomials. We will see in 3.2.1 that the problem of testing algebraic independence of polynomials over a field is computable. We will then see in 3.4, an efficient criterion (the Jacobian Criterion) for testing algebraic independence over fields of zero characteristic. We finally discuss the failure of the Jacobian Criterion over fields of positive characteristic and discuss the open problem of finding an efficient algorithm to test algebraic independence over fields of positive characteristic.

### 3.1 Basic definitions

**Definition 3.1.** (Algebraic Independence of Polynomials). Let  $\mathbb{F}$  be a field. A set of polynomials  $\{f_1, f_2, \dots, f_m\} \in \mathbb{F}[x_1, x_2, \dots, x_n]$  is said to be *algebraically dependent* over  $\mathbb{F}$  if there exists a non-zero polynomial  $A \in \mathbb{F}[y_1, y_2, \dots, y_m]$  such that  $A(f_1, f_2, \dots, f_m) = 0$ . We call such a polynomial  $A$ , an *annihilating polynomial* of  $f_1, f_2, \dots, f_m$ . If no such polynomial  $A$  exists, we say that the polynomials  $f_1, f_2, \dots, f_n$  are *algebraically independent*.

**Definition 3.2.** (Transcendence Basis). A transcendence basis for a set  $L$  over a field  $K$  is an algebraically independent set  $A$  such that the field extension  $L/K(A)$  is algebraic.

**Definition 3.3.** (Transcendence Degree). For a set  $L$  over a field  $K$ , it is defined as the cardinality of its transcendence basis.

**Lemma 3.4.** *All transcendence bases have same cardinality, i.e. the transcendence degree is well defined.*

For a proof, see [Mil03], Lemma 9.9.

Using the above lemma, we can define the transcendence degree for a set of polynomials as the maximum number of algebraically independent polynomials in the set.

## 3.2 Testing Algebraic Independence

A priori, it is not clear whether the problem of testing algebraic independence of polynomials is computable. We will now see a result which asserts the computability of testing algebraic independence.

### 3.2.1 Degree bound on Annihilating Polynomial

Perron [Per27] established a degree bound for the annihilating polynomial of  $n + 1$  polynomials in  $n$  variables. Kayal [Kay09] established a degree bound for the annihilating polynomial of sets with arbitrary number of polynomials over fields of zero characteristic. His result depended on the transcendence degree and was independent of the number of variables. Mittman [Mit13] generalised Kayal's result to fields of arbitrary characteristic.

**Theorem 3.5.** [Mit13]. *Let  $f_1, \dots, f_m \in \mathbb{F}[x_1, \dots, x_n]$  be polynomials of degree at most  $\delta \geq 1$  and let  $r := \text{trdeg}_{\mathbb{F}}(f_1, \dots, f_m)$ . If  $m > r$ , then there exists a non-zero polynomial  $A \in \mathbb{F}[y_1, \dots, y_m]$  with  $\deg(A) \leq \delta^r$  such that  $A(f_1, \dots, f_m) = 0$ .*

The following example demonstrates that the degree bound given by the above theorem is tight.

**Example 3.1.** [Mit13]. *The set of  $n + 1$  polynomials  $\{x_1, x_2 - x_1^d, x_3 - x_2^d, \dots, x_n - x_{n-1}^d, x_n^d\}$  has transcendence degree  $n$  and its minimal annihilating polynomial has degree  $d^n$ .*

A direct consequence is that the problem of testing algebraic independence becomes computable over an arbitrary field. This upper bound gives a simple (though inefficient) test since  $f_1, \dots, f_m$  are algebraically dependent if and only if  $\{f_1^{d_1} \cdots f_n^{d_n} \mid \sum_{i=1}^m d_i \leq \delta^m\}$  is  $\mathbb{F}$ -linearly dependent. This system of linear equation which is exponential-sized can be solved in **PSPACE**. In the case of constantly many sparse polynomials with low (polynomially bounded) degree, as the degree bound of the annihilating polynomial is polynomial in terms of input size, we can test algebraic independence in randomized polynomial time. But for constantly many polynomials with high (exponential) degree, the degree bound is exponential.

### 3.3 Hardness of Computing Annihilating Polynomial

As the annihilating polynomial's degree bound can be exponential, explicitly computing the annihilating polynomial is definitely computationally intractable. Kayal [Kay09] showed that computing  $A(0, \dots, 0) \pmod{p}$  is  $\#\mathbf{P}$ -hard. If the annihilating polynomial had polynomial sized arithmetic circuit that could be computed efficiently, then  $A(0, \dots, 0) \pmod{p}$  could also be computed efficiently. The paper also showed that annihilating polynomials do not have polynomially bounded (in input size) circuits unless the polynomial hierarchy collapses.

### 3.4 Efficient Computation: The decision problem

Since computing the annihilating polynomial is provably hard, a natural question would be to ask for an efficient algorithm for the decision version of the problem i.e. given a set of polynomials, we want to know whether they are algebraically dependent or independent.

The Jacobian criterion gives an efficient **RP**-algorithm for testing independence in the case of fields of zero characteristic.

### 3.4.1 The Jacobian Criterion

**Definition 3.6. (Jacobian Matrix).** Given polynomials  $f_1, \dots, f_m \in \mathbb{F}[x_1, \dots, x_n]$ , their Jacobian matrix is defined as

$$J(f_1, \dots, f_m) := \begin{bmatrix} \frac{\partial f_1}{\partial x_1} & \frac{\partial f_1}{\partial x_2} & \dots & \frac{\partial f_1}{\partial x_n} \\ \frac{\partial f_2}{\partial x_1} & \frac{\partial f_2}{\partial x_2} & \dots & \frac{\partial f_2}{\partial x_n} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{\partial f_m}{\partial x_1} & \frac{\partial f_m}{\partial x_2} & \dots & \frac{\partial f_m}{\partial x_n} \end{bmatrix} \quad (3.1)$$

**Theorem 3.7. (The Jacobian Criterion)** *If  $\mathbb{F}$  is a field of zero characteristic, then  $f_1, \dots, f_m \in \mathbb{F}[x_1, \dots, x_n]$  are algebraically independent if and only if the Jacobian matrix is full rank. In particular, if  $m = n$ ,  $f_1, \dots, f_m$  are algebraically dependent if and only if the Jacobian determinant  $\det(J(f_1, \dots, f_m)) = 0$ .*

For a proof, one can refer to [BMS13] where it has been shown that the rank of the Jacobian matrix equals the transcendence degree of the set of polynomials.

It always suffices to consider the  $n = m$  case. Since whenever  $n > m$ , we can randomly fix the extraneous variables (possibly from a finite extension of the base field  $\mathbb{F}$ ) to reduce the number of variables to  $m$ . Also whenever  $n < m$ , the polynomials  $f_1, \dots, f_m$  are always algebraically dependent as is shown by the following lemma.

**Lemma 3.8. [For92].** *The polynomials  $f_1, \dots, f_m \in \mathbb{F}[x_1, \dots, x_n]$  are algebraically dependent over  $\mathbb{F}$  if  $m > n$ .*

*Proof.* This is true over an arbitrary field. We consider the extensions:

$$\mathbb{F} \subseteq \mathbb{F}(f_1, \dots, f_m) \subseteq \mathbb{F}(x_1, \dots, x_n) \quad (3.2)$$

From field theory, we have for  $G \subseteq F \subseteq E$ ,  $\text{trdeg}(E/G) = \text{trdeg}(E/F) + \text{trdeg}(F/G)$ . Now since  $\text{trdeg}(\mathbb{F}(x_1, \dots, x_n)/\mathbb{F}) = n$ , the  $\text{trdeg}(\mathbb{F}(f_1, \dots, f_m)/\mathbb{F})$  cannot be more than  $n$ . So, the  $\text{trdeg}\{f_1, \dots, f_m\} \leq n$  since any two transcendence bases of  $\mathbb{E}/\mathbb{F}$  have the same cardinality. But  $n < m$ , which implies that  $f_1, \dots, f_m$  are algebraically dependent.  $\square$

**Abstract formulation of the Jacobian criterion:** (See [Mit13], [MSS12] for a detailed exposition). Over fields  $\mathbb{F}$  of zero characteristic,  $f_1, \dots, f_n \in \mathbb{F}[x_1, \dots, x_n]$  are algebraically dependent if and only if  $df_1 \wedge \dots \wedge df_n = 0$  as it can be shown that

$$df_1 \wedge \dots \wedge df_n = \det(J(f_1, \dots, f_n)) dx_1 \wedge \dots \wedge dx_n \quad (3.3)$$

where we have the wedge product or the exterior product as an anti-commutative product defined by  $(x \wedge y) = -(y \wedge x)$  and the differential is defined by the Leibniz rule  $d(xy) = xdy + ydx$ .

### 3.4.2 A Randomized Polynomial Time Algorithm

Since the Jacobian determinant is also a polynomial in  $\mathbb{F}[x_1, \dots, x_n]$ , and we are interested in knowing if that polynomial is zero or not, the Jacobian criterion reduces the problem of algebraic independence testing to the problem of polynomial identity testing (PIT). Now, PIT has a randomized polynomial time algorithm using the Schwartz-Zippel lemma in the case of a general arithmetic circuit [Sax09]. So, we get an RP algorithm for algebraic independence testing as well for polynomials over fields of zero characteristic.

## 3.5 Algebraic Independence and Resultant

**Definition 3.9.** Resultant of the polynomials  $f_1, f_2 \in \mathbb{F}[x_1, x_2]$  with respect to  $x_1$  is defined as

$$R_{x_1}(f_1 - y_1, f_2 - y_2) = \alpha_0 \prod_{i=1}^l (f_1(\varphi_i) - y_1), \quad (3.4)$$

where  $l$  is the degree of  $f_2$  with respect to the variable  $x_1$  and the  $\varphi_i$  are the roots of the equation  $f_2 - y_2 = 0$  in an appropriate extension of the field  $\mathbb{F}(x_2, y_2)$  so that  $\varphi_i = \varphi_i(x_2, y_2)$ .

**Theorem 3.10.** [L'v84] *Let  $f_1 = \alpha_0 x_1^k + \dots + \alpha_k$  and  $f_2 = \beta_0 x_1^l + \dots + \beta_l$  be polynomials in  $\mathbb{F}[x_1, x_2]$  that have been expanded in powers of  $x_1$ .  $f_1$  and  $f_2$  are algebraically dependent if and only if the expression*

$$\frac{1}{\alpha_0^l} R_{x_1}(f_1 - y_1, f_2 - y_2) \quad (3.5)$$

is free of  $x_2$ . Moreover if  $f_1$  and  $f_2$  are algebraically dependent, then the above expression will be the degree of an indecomposable polynomial  $B(y_1, y_2)$  such that  $B(f_1, f_2) = 0$ , where  $R_{x_1}(f_1 - y_1, f_2 - y_2)$  is the resultant of  $f_1$  and  $f_2$  with respect to  $x_1$ .

## 3.6 Algebraic Independence over Fields of positive characteristic

Motivated by an RP-algorithm for independence testing in the case of polynomials over fields of zero characteristic, one would like to have an efficient criterion over fields of positive characteristic as well. The first point of investigation would be to see if the Jacobian criterion in its original form continues to work in the positive characteristic case too.

### 3.6.1 Jacobian Failure:

The proof of the Jacobian criterion asserts that one side of the Jacobian criterion is true for fields of arbitrary characteristic [BMS13] i.e. if  $f_1, \dots, f_n$  are algebraically dependent, then  $\det(J(f_1, \dots, f_n)) = 0$ . However, the proof of the converse fails in the case of fields of positive characteristic.

Indeed, one can easily see that the converse is false in the positive characteristic case:

**Example 3.2.**  $x_1^p$  and  $x_2^p$  are independent polynomials over  $\mathbb{F}_p$ . But their Jacobian determinant vanishes.

So, we do not have the Jacobian criterion in the case of fields of positive characteristic which leaves us with the **PSPACE**-algorithm based on the annihilating polynomial degree bound which works over arbitrary fields.

There has been little progress in terms of the complexity class of the problem of testing algebraic independence of polynomials in the positive characteristic case. The first improvement over the **PSPACE**-algorithm is the Witt Jacobian Criterion given by [MSS12] which brings the problem in the complexity class  $\mathbf{NP}^{\#P}$ .

Hence, there is still a huge gap between what is best known and what is being hoped. Even for special cases, no progress is known.

Our attempts to solve this problem are driven by the following four approaches:

- Since the Jacobian criterion in its original form does not work, one can try to transform the polynomials so that the Jacobian works. We discuss the approach with the obtained results in Chapter 4.
- One can try to look for a criterion exclusively for the positive characteristic case. We present such a criterion in Chapter 5. The Witt Jacobian criterion too is one such criterion.
- Looking for a more general criterion which works for fields of arbitrary characteristic. We discuss such an idea for a special case in Chapter 6.
- We keep the polynomials same but change the matrix to be considered for checking the dependence. We cover this in Chapter 7.

## Chapter 4

# Jacobian Correction

In the last chapter, we saw (section 3.6.1) that there are examples of polynomials over  $\mathbb{F}_p$  where the usual Jacobian criterion of checking algebraic dependence by checking the zeroness of the determinant of the Jacobian matrix fails. In this chapter, we make an attempt to correct the Jacobian determinant. We explore the transformations which preserve algebraic independence in 4.2. We show in some special cases that applying a combination of such transformations on the input polynomials make the Jacobian criterion work in 4.3. We get a randomized polynomial time algorithm in those special cases. In [Sin15], it was obtained for monomials and two binomials. Using similar techniques, we give an efficient algorithm for the two sum of univariates case in 4.4. Finally in 4.5, we give a characterization of cases with zero Jacobian determinant.

### 4.1 Jacobian seen over Rationals:

In order to get a criterion which works even for  $\mathbb{F}_p$ , one natural question one could ask is whether the Jacobian determinant seen over  $\mathbb{Q}$  already contains the information about the dependence over  $\mathbb{F}_p$ . This can be framed as the following conjecture.

**Conjecture:** Let  $\mathcal{A}$  be the set of Jacobian determinants seen over  $\mathbb{Q}$  of all algebraically dependent pairs of bivariate polynomials  $f_1, f_2 \in \mathbb{F}_p[x_1, x_2]$ ; and let  $\mathcal{B}$  be the set of Jacobian determinants seen over  $\mathbb{Q}$  of all algebraically independent pairs.



Then  $\mathcal{A} \cap \mathcal{B} = \emptyset$ , i.e. *the Jacobian determinant of the dependent and the independent pairs of polynomials go into different disjoint sets.*

Clearly this is true in case of independence testing over  $\mathbb{Q}$  since the Jacobian determinant of dependent polynomials are all zero and no independent polynomials have zero Jacobian. For independence testing over  $\mathbb{F}_p$ , the above conjecture predicts the existence of a Jacobian determinant based criterion though not necessarily as simple as checking its zeroness.

**Counter Example:**  $f_1 = x^3 + x^2y + xy^2 + y^3$  and  $f_2 = x + y$  are dependent polynomials over  $\mathbb{F}_2$  with  $f_1^3 - f_2 = 0$ .

Now consider the polynomials  $f'_1 = x^2 + y^2$  and  $f'_2 = xy$ .

However, the Jacobian determinant seen over  $\mathbb{Q}$  is  $J(f_1, f_2) = J(f'_1, f'_2) = 2x^2 + 2y^2$ .

The counter example to the conjecture is instructive in the sense that it tells that the Jacobian determinant seen over  $\mathbb{Q}$  in itself does not have sufficient information to check dependence over  $\mathbb{F}_p$ . So, it means that we cannot reduce testing algebraic independence to checking some property of the Jacobian determinant (seen over  $\mathbb{Q}$ ).

## 4.2 Jacobian Correcting Transformations

A potential approach to tackle the above problem is to transform the given polynomials so that the zeroness and the non-zeroness of the Jacobian determinant of the transformed polynomials imply respectively the dependence and the independence of the original polynomials [Sin15]. i.e.  $f_1, \dots, f_n \mapsto g_1, \dots, g_n$  such that  $J(g_1, \dots, g_n) = 0 \Leftrightarrow f_1, \dots, f_n$  are algebraically dependent.

We know that one direction of the Jacobian criterion is true even over  $\mathbb{F}_p$  i.e. a non-zero Jacobian determinant of polynomials  $g_1, \dots, g_n$  implies that they are algebraically independent. So, for independent polynomials  $f_1, \dots, f_n$  with failing Jacobian (i.e.  $J(f_1, \dots, f_n) = 0$ ), we are looking for transcendence degree preserving transformation which makes the Jacobian determinant non-zero.

So, we call such  $g_1, \dots, g_n$  as *independence certifying polynomials* for  $f_1, \dots, f_n$ , the transformation as *Jacobian correcting transformation* and any transcendence degree preserving map as a *faithful transformation*.

It is easy to see that many of the faithful transformations will not correct the Jacobian. Transformations like applying algebraically independent polynomial map cannot correct Jacobian because chain rule shows that the Jacobian of the transformed polynomials is a multiple of the Jacobian of the original polynomials. But one faithful transformation can correct the Jacobian, if the polynomials are  $p$ -th powers, we can take the highest possible  $p$ -th root of them and then take the Jacobian. This sometimes may correct the Jacobian.

**Example 4.1.** Take  $x^p, y^p$ . After taking their  $p$ -th roots, Jacobian becomes nonzero.

But there are also algebraically independent polynomials over  $\mathbb{F}_p$ , none of them  $p$ -th powered, yet their Jacobian determinant is zero.

**Example 4.2. Example 2:**  $x^{p-1}y$  and  $xy^{p-1}$  are independent polynomials with zero Jacobian over  $\mathbb{F}_p$ .

Here neither of the polynomials is a  $p$ -th power. Yet, the Jacobian determinant is zero. So it is not always possible to correct the Jacobian by just taking the  $p$ -th root.

We show that many such cases can be converted to  $p$ -th power after applying faithful transformation such that we get a non-zero Jacobian after taking their  $p$ -th root.

Let us see how some natural transformations on the polynomials preserves the transcendence degree and can also help in correcting the Jacobian.

### 4.2.1 Taking $p$ -th root of the polynomials

We show that taking  $p$ -th root is a faithful transformation [Sin15].

**Lemma 4.1.**  $f_1^{p^{\alpha_1}}, \dots, f_m^{p^{\alpha_m}}$  are algebraically dependent over  $\mathbb{F}_p$  if and only if  $f_1, \dots, f_m$  are algebraically dependent over  $\mathbb{F}_p$ .

*Proof.*  $\Rightarrow$  If  $f_1^{p^{\alpha_1}}, \dots, f_m^{p^{\alpha_m}}$  are algebraically dependent over  $\mathbb{F}_p$ , then there exists a non-zero annihilating polynomial  $A \in \mathbb{F}_p[y_1, \dots, y_n]$  satisfying  $A(f_1^{p^{\alpha_1}}, \dots, f_m^{p^{\alpha_m}}) = 0$ . Trivially,  $A(y_1^{p^{\alpha_1}}, \dots, y_n^{p^{\alpha_n}})$  is an annihilating polynomial of  $f_1, \dots, f_m$ .

$\Leftarrow$  If  $f_1, \dots, f_m$  are algebraically dependent over  $\mathbb{F}_p$ , then there exists a non-zero annihilating polynomial  $B$  satisfying  $B(f_1, \dots, f_m) = 0$ . Now let  $\alpha_t := \max(\alpha_1, \dots, \alpha_m)$ . Since over  $\mathbb{F}_p$ , we have:  $(a_1 + \dots + a_n)^{p^{\alpha_t}} = a_1^{p^{\alpha_t}} + \dots + a_n^{p^{\alpha_t}}$  and  $f_i^{p^{\alpha_t}} = (f_i^{p^{\alpha_i}})^{p^{\alpha_t - \alpha_i}}$  so, we take  $p^{\alpha_t}$  power of  $B$ . We get,

$$B^{p^{\alpha_t}}(f_1, \dots, f_m) = B(f_1^{p^{\alpha_t}}, \dots, f_m^{p^{\alpha_t}}) = B((f_1^{p^{\alpha_1}})^{p^{\alpha_t - \alpha_1}}, \dots, (f_m^{p^{\alpha_m}})^{p^{\alpha_t - \alpha_m}}) = 0 \quad (4.1)$$

Thus,  $B(y_1^{p^{\alpha_t - \alpha_1}}, \dots, y_n^{p^{\alpha_t - \alpha_n}})$  works as an annihilating polynomial for  $f_1^{p^{\alpha_1}}, \dots, f_m^{p^{\alpha_m}}$ .

□

## 4.2.2 Applying polynomial map

We define a polynomial map  $\varphi$  as a way of mapping the variables of the polynomials to the polynomials in the same ring i.e.

$$(x_1, \dots, x_n) \mapsto (g_1, \dots, g_n) \quad (4.2)$$

where  $g_i \in \mathbb{F}[x_1, \dots, x_n]$ .

So  $\varphi(f) := f(g_1(x_1, \dots, x_n), \dots, g_n(x_1, \dots, x_n))$ .

**Lemma 4.2.** [*Sin15*] *If  $f_1, \dots, f_n$  are algebraically dependent, then  $\varphi(f_1), \dots, \varphi(f_n)$  are algebraically dependent. For faithful polynomial maps, the converse is also true.*

*Proof.* If  $f_1, \dots, f_n$  are algebraically dependent, clearly the same annihilating polynomial annihilates  $f_1(g_1, \dots, g_n), \dots, f_n(g_1, \dots, g_n)$ . Now, we prove the opposite direction, which requires the map to be algebraically independent. We can view  $\varphi$  as a homomorphism from  $\mathbb{F}[x_1, \dots, x_n] \rightarrow \mathbb{F}[g_1, \dots, g_n]$ . As  $g_1, \dots, g_n$  are algebraically independent,

$\varphi$  is injective. For the sake of contradiction, assume  $f_1, \dots, f_n$  to be algebraically independent but  $\varphi(f_1), \dots, \varphi(f_n)$  to be algebraically dependent. So, there is a nonzero annihilating polynomial  $A$  such that  $A(\varphi(f_1), \dots, \varphi(f_n)) = 0$ . As  $\varphi$  is a homomorphism,  $\varphi(A(f_1, \dots, f_n)) = 0$ . As  $\varphi$  is injective, this means  $A(f_1, \dots, f_n) = 0$ . So, we get a contradiction.  $\square$

### 4.2.3 Taking polynomials from the ring or the function field of the given polynomials

**Lemma 4.3.** *Algebraic independence of any  $m$  elements from  $\mathbb{F}(f_1, \dots, f_m)$  certifies algebraic independence of  $f_1, \dots, f_m$  over the field  $\mathbb{F}$ .*

*Proof.* Consider the field extension:

$$\mathbb{F} \subseteq \mathbb{F}(f_1, \dots, f_m) \subseteq \mathbb{F}(x_1, \dots, x_n) \quad (4.3)$$

with transcendence degree  $\text{trdeg}(\mathbb{F}(f_1, \dots, f_m) : \mathbb{F}) = t$ . So, if we pick  $k$  elements from the the field  $\mathbb{F}(f_1, \dots, f_m)$ , the transcendence degree of the set is bounded by  $t$ . Also, trivially the transcendence degree,  $t$  is bounded by the number of generators  $m$  (i.e.  $t \leq m$ ). Now if the transcendence degree of the chosen set is  $m$ , it implies that the transcendence degree of the extension,  $t \geq m$ . So, we get  $t = m$  from above.

Thus  $f_1, \dots, f_m$  are algebraically independent.  $\square$

Let us see some examples where the above three transformations indeed help in the Jacobian correction [[Sin15](#)].

- $f = x^2y$  and  $g = xy^2$  over  $\mathbb{F}_2$ . The Jacobian determinant of  $f$  and  $g$  is zero. But if we apply the map:

$$x \mapsto x^2/y; \quad y \mapsto y^2/x \quad (4.4)$$

we get  $f \mapsto x^3$  and  $g \mapsto y^3$ . Now, using Lemma 4.1, we take cube root of both  $f$  and  $g$  to get  $x$  and  $y$  respectively. Now the Jacobian is nonzero which by Lemma 4.2 certifies the independence of  $f$  and  $g$  (monomial map and  $p$ -th root).

- $f = x^2 + x^3 + y$  and  $g = x^3 + y$  over  $\mathbb{F}_2$ . The Jacobian determinant is zero here as well. But after applying the map:

$$x \mapsto x; \quad y \mapsto x^3 + y^2 \tag{4.5}$$

we get  $f \mapsto x^2 + y^2$  and  $g \mapsto y^2$  which after taking square root yields  $x + y$  and  $y$  giving a nonzero Jacobian, hence certifying independence of  $f$  and  $g$  (polynomial map and  $p$ -th root).

- The above example could also be corrected by going to the polynomial ring generated by above polynomials. For instance if we pick the polynomials  $f - g$  and  $g$ , we get the polynomials  $x^2$  and  $x^3 + y$ . Taking square root of  $f - g$  yields  $x$  and  $x^3 + y$  which now has a non-zero Jacobian. Thus,  $\sqrt{f - g}$  and  $g$  are algebraically independent which by lemma 4.1 and 4.3 implies that  $f$  and  $g$  are algebraically independent.
- Take  $f = u$  and  $g = v^p u$  where  $u, v \in \mathbb{F}_p[x, y]$  The Jacobian is zero in this case too. But if we take  $f^{p-1}g$ , we get  $u^p v^p$  which on taking taking  $p$ -th root yields  $uv$ . Now if  $J(uv, v) \neq 0$ , we get independence certificate of  $f$  and  $g$  (by lemma 4.1 and 4.3).

### 4.3 Jacobian Correction in special cases

Motivated by the above examples, one can give algorithms to correct the Jacobian determinant for some special classes of polynomials.

#### 4.3.1 Monomials: The Monomial Map

Here we prove that if we are given  $n$  monomials in  $n$ -variables, we can always correct the Jacobian determinant. We do this by using monomial maps.

First we see a criterion for testing algebraic independence for a set of monomials.

**Lemma 4.4.** *[Mit13]. A set of monomials are algebraically dependent over a field  $\mathbb{F}$  if and only if their exponent vectors are linearly dependent over  $\mathbb{Z}$ .*

*Proof.* If  $m_i = c_i x_1^{\alpha_{i1}} \cdots x_n^{\alpha_{in}}$  then  $(\alpha_i) = (\alpha_{i1}, \dots, \alpha_{in})$  is called the exponent vector of the monomial  $m_i$ .

$\Leftarrow$  Now, let us assume that the exponent vectors of the monomials are  $\mathbb{Z}$ -linearly dependent, i.e. for some  $\lambda_i$ 's  $\in \mathbb{Z}$ , we have:

$$\lambda_1 \alpha_1 + \cdots + \lambda_n \alpha_n = 0. \quad (4.6)$$

From this, we can easily show,

$$m_i^{\lambda_1} \cdots m_n^{\lambda_n} = 1. \quad (4.7)$$

This shows that  $m_1, \dots, m_n$  are algebraically dependent.

$\Rightarrow$  Conversely, let  $m_1, \dots, m_n$  be algebraically dependent. If  $t_1, \dots, t_r$  are the terms of the annihilating polynomial then for all  $t_i$ ,  $t_i(m_1, \dots, m_n)$  is a monomial. As all these monomials cancel, there are two distinct terms  $t_1 = y_1^{\lambda_1}, \dots, y_n^{\lambda_n}$  and  $t_2 = y_1^{\mu_1}, \dots, y_n^{\mu_n}$  such that  $t_1(m_1, \dots, m_n) = t_2(m_1, \dots, m_n)$ . Plugging in  $m_1, \dots, m_n$  in  $t_1$  and  $t_2$ , we will get

$$(\lambda_1 - \mu_1) \alpha_1 + \cdots + (\lambda_n - \mu_n) \alpha_n = 0. \quad (4.8)$$

Now, as  $t_1$  and  $t_2$  are distinct, not all  $\lambda_i - \mu_i$  can be zero. This shows that the exponent vectors are linearly dependent.  $\square$

The above lemma shows that for monomials, the question of algebraic independence of monomials over  $\mathbb{F}_p$  is same as their independence over  $\mathbb{Q}$ . Since the Jacobian does not fail over  $\mathbb{Q}$ , testing algebraic independence of monomials over  $\mathbb{F}_p$  becomes easy. We just need to check if the Jacobian determinant over  $\mathbb{Q}$  is nonzero.

However, even in the case of monomials, we would like to correct the Jacobian over  $\mathbb{F}_p$  itself, hoping that the technique used can be deployed to correct Jacobian in other cases of  $\mathbb{F}_p$  as well; since in other cases, we do not have a criterion as strong as testing dependence over  $\mathbb{Q}$  as we have in the case of monomials.

**Lemma 4.5.** [Sin15]. *Jacobian can always be corrected for a set of  $n$ -monomials  $m_1, \dots, m_n \in \mathbb{F}_p[x_1, \dots, x_n]$ .*

*Proof.* Case 1: Jacobian determinant,  $\det(J(m_1, \dots, m_n)) = 0$  over  $\mathbb{Q}$ :

In this case, they are dependent over  $\mathbb{Q}$  and hence over  $\mathbb{F}_p$  as well. So, the Jacobian is already correct.

Case 2:  $\det(J(m_1, \dots, m_n)) \neq 0$  over  $\mathbb{F}_p$ :

Again the Jacobian is already correct and  $m_1, \dots, m_n$  are algebraically independent.

Case 3: Jacobian is nonzero over  $\mathbb{Q}$  but zero over  $\mathbb{F}_p$ :

By the above lemma,  $m_1, \dots, m_n$  are algebraically independent over  $\mathbb{F}_p$ . So, the Jacobian fails in this case.

Let us assume the monomials be  $m_1, \dots, m_n$  such that  $m_i = c_i x_1^{\alpha_{i1}} \dots x_n^{\alpha_{in}}$  and the corresponding exponent vector for  $m_i$  is  $(\alpha_{i1}, \dots, \alpha_{in})$ .

The exponent matrix of the monomials is thus denoted as:

$$A_{n,n} = \begin{pmatrix} \alpha_{11} & \alpha_{12} & \cdots & \alpha_{1n} \\ \alpha_{21} & \alpha_{22} & \cdots & \alpha_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_{n1} & \alpha_{n2} & \cdots & \alpha_{nn} \end{pmatrix}. \quad (4.9)$$

Now computing the Jacobian determinant of  $m_1, \dots, m_n$  from the definition, we get

$$\det(J(m_1, \dots, m_n)) = \prod_{i=1}^n c_i \cdot \det A \cdot \frac{\prod_{i=1}^n m_i}{\prod_{i=1}^n x_i}. \quad (4.10)$$

Thus zero Jacobian over  $\mathbb{F}_p$  means that  $p$  divides  $\det A$ . Let us say  $\det A = \alpha \cdot p^k$ , where  $k$  is the highest power of  $p$  which divides  $\det A$ . We now correct the Jacobian by first introducing a faithful map which sends the variables to a set of algebraically independent monomials.

$$(x_1, \dots, x_n) \mapsto (N_1, \dots, N_n) \quad (4.11)$$

where the exponent matrix of  $N_1, \dots, N_n$  is given by:

$$B_{n,n} = \begin{pmatrix} \beta_{11} & \beta_{12} & \cdots & \beta_{1n} \\ \beta_{21} & \beta_{22} & \cdots & \beta_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ \beta_{n1} & \beta_{n2} & \cdots & \beta_{nn} \end{pmatrix}. \quad (4.12)$$

The monomials  $m_1, \dots, m_n$  gets mapped to  $M_1, \dots, M_n$ . One can easily verify that the exponent matrix  $E_{n,n}$  of  $M_1, \dots, M_n$  becomes:

$$A_{n,n} \mapsto A'_{n,n} = A_{n,n} \cdot B_{n,n} \quad (4.13)$$

Now we know the identity  $A \cdot \text{Adj}A = \det A \cdot I_n$ , where  $\text{Adj}A$  denotes the Adjoint matrix of the matrix  $A$ . Thus if  $B$  is chosen to be the same as  $\text{Adj}A$ ,  $A'$  becomes diagonal i.e. monomials get transformed as

$$(m_1, \dots, m_n) \mapsto (x_1^{\det A}, x_2^{\det A}, \dots, x_n^{\det A}) \quad (4.14)$$

Now since,  $\det A = \alpha \cdot p^k$ , we can take  $p^k$ -th root of all the transformed monomials, they get transformed to  $x_1^\alpha, \dots, x_n^\alpha$ . Now  $\det(J(x_1^\alpha, \dots, x_n^\alpha)) \neq 0$  since  $p$  does not divide  $\alpha$ . □

Let us say  $f = m_1 + m_2 + \cdots + m_k$  and  $g = M_1 + M_2 + \cdots + M_l$ . So  $\det(J(f, g)) = \sum \det(J(m_i, M_j))$  i.e. the Jacobian is equal to the sum of Jacobian of all the monomial pairs. We believe that the failure of the Jacobian in general is because of its failure at the level of monomials of the given polynomials.

**Conjecture:** If Jacobian of no monomial pair,  $\det(J(m_i, M_j))$  fails, then Jacobian  $\det(J(f, g))$  does not fail.

In the spirit of the above conjecture, we believe that several special cases of failing Jacobian can be corrected by correcting the failing monomial pairs.

Using the above monomial map technique, one could also give a polynomial time algorithm for testing algebraic independence of two bivariate binomials (see [Sin15] 3.2.2).



## 4.4 Sum of Univariates

In this section, we give an algorithm to check algebraic independence of two bivariate polynomials where each of them are sum of univariate polynomials over  $\mathbb{F}_p$ . The polynomials are given in the sparse representation where degrees can be exponential in the input size. e.g.  $f(x) = \sum f_i(x_i)$  where each  $f_i(x_i)$  is a polynomial in variable  $x_i$ .

Clearly, the Jacobian criterion does not help directly. We again use the idea of Jacobian correction taking the  $p$ -th root. We first prove the following lemma which helps us in getting the algorithm.

**Lemma 4.6.** *If two super-sparse sum of univariate polynomials have a zero Jacobian determinant, the non  $p$ -th power part of the two polynomials are constant multiple of each other.*

*Proof.* Let the given polynomials be:

$f(x, y) = f_1(x) + f_2(y)$ , and  $g(x, y) = g_1(x) + g_2(y)$ . We can rewrite  $f$  and  $g$  by separating the  $p$ -power parts and the non  $p$ -power parts of  $f_1, f_2, g_1$  and  $g_2$  i.e.

$$f(x, y) = f_p(x, y) + f_{np}(x, y) \text{ and } g(x, y) = g_p(x, y) + g_{np}(x, y)$$

Using both the above way of rewriting  $f$  and  $g$ , we get:

$$f(x, y) = f_{1p}(x) + f_{1np}(x) + f_{2p}(y) + f_{2np}(y) \text{ and}$$

$$g(x, y) = g_{1p}(x) + g_{1np}(x) + g_{2p}(y) + g_{2np}(y),$$

where  $p$  and  $np$  in the subscript denote the  $p$ -power and the non  $p$ -power parts respectively. Now the Jacobian matrix of  $f$  and  $g$ ,

$$J(f, g) = \begin{bmatrix} \partial_x f & \partial_y f \\ \partial_x g & \partial_y g \end{bmatrix} = \begin{bmatrix} \partial_x f_{1np}(x) & \partial_y f_{2np}(y) \\ \partial_x g_{1np}(x) & \partial_y g_{2np}(y) \end{bmatrix} \quad (4.15)$$

Now the Jacobian determinant being zero implies,

$$\det(J(f, g)) = \partial_x f_{1np}(x) \cdot \partial_y g_{2np}(y) - \partial_x g_{1np}(x) \cdot \partial_y f_{2np}(y) = 0. \text{ This gives:}$$

$$\frac{\partial_x f_{1np}(x)}{\partial_x g_{1np}(x)} = \frac{\partial_y f_{2np}(y)}{\partial_y g_{2np}(y)}. \quad (4.16)$$

Note that the L.H.S. is a function independent of  $y$  and the R.H.S. is a function independent of  $x$ . Thus both the L.H.S. and the R.H.S. have to be equal to a field constant i.e.

$$\frac{\partial_x f_{1np}(x)}{\partial_x g_{1np}(x)} = \alpha, \quad \alpha \in \mathbb{F}_p \quad (4.17)$$

$$\partial_x f_{1np}(x) = \alpha \partial_x g_{1np}(x) \quad (4.18)$$

$$d f_{1np}(x) - \alpha d g_{1np}(x) = 0 \quad (4.19)$$

On integration, we get  $f_{1np}(x) - \alpha g_{1np}(x) \in \mathbb{F}_p[x^p]$ . But, we know by definition, that the terms in  $f_{1np}(x)$  or  $g_{1np}(x)$  are neither field constants nor  $p$ -powers. Thus, we get:

$$f_{1np}(x) - \alpha g_{1np}(x) = 0 \quad (4.20)$$

Similarly,

$$f_{2np}(y) - \alpha g_{2np}(y) = 0 \quad (4.21)$$

□

Now, we are in a position to give the independence testing algorithm via Jacobian correction.

#### 4.4.1 The Algorithm

- 
1. **if**  $\det(J(f, g)) \neq 0$  over  $\mathbb{F}_p$ ,  
 $f$  and  $g$  are algebraically independent over  $\mathbb{F}_p$ .
  2. **else, if**  $\det(J(f, g)) = 0$  over  $\mathbb{Q}$ ,  
 $f$  and  $g$  are algebraically dependent over  $\mathbb{Q}$  and hence over  $\mathbb{F}_p$  as well.
  3. **else**, find  $\alpha$  such that  $f_{np} = \alpha \cdot g_{np}$ .  
     **now if**  $\deg(f_p) \geq \deg(g_p)$ ,  
          $f := (\alpha f - g)^{1/p^k}$  and  $g := g$  and go to Step 1, where  $k$  is the highest power of  $p$  which divides  $\alpha f - g$ .  
     **else if**  $\deg(f_p) < \deg(g_p)$ :  
          $g := (\alpha f - g)^{1/p^k}$  and  $f := f$  and go to Step 1.
-

### 4.4.2 Proof of Correctness

To prove the correctness of the algorithm, we prove the following claims:

- (i) The algorithm always terminates after a finite number of steps.
- (ii) If  $f$  and  $g$  are independent, then eventually  $\det(J(f, g))$  becomes non-zero over  $\mathbb{F}_p$ .
- (iii) If  $f$  and  $g$  are dependent, then eventually  $\det(J(f, g))$  becomes zero over  $\mathbb{Q}$ .

*Proof.* (i) Observe that in step (3), if  $\deg(f_p) \geq \deg(g_p)$ ,  $g$  and hence its degree remain unchanged. Now from our choice of  $\alpha$  and Lemma 4.1, it follows that  $\alpha f - g$  is a  $p$ -th power. Hence  $\deg(\alpha f - g) \leq \max(\deg(f_p), \deg(g_p))$ . Further taking  $p^k$ -th root reduces the degree of updated  $f$ . Similar case happens if  $\deg(f_p) < \deg(g_p)$ . Thus in every iteration in step 3, one of the degrees gets decreased. Hence the algorithm terminates after finite number of steps.

(ii) and (iii). To prove these, all we need to establish is that the operations in step 3 preserves the transcendence degree of  $f$  and  $g$  over an arbitrary field.

Well this is also true since it is an easy exercise to show:

a)  $\text{trdeg}(f^p, g) = \text{trdeg}(f, g)$ , and

b)  $\text{trdeg}(\alpha f + \beta g, g) = \text{trdeg}(f, g)$  for  $\alpha \neq 0$ . □

### 4.4.3 Time Complexity

In each iteration, in step 3, one of the degrees gets reduced by a factor  $\geq p$ . Hence if  $d := \max(\deg(f_p), \deg(g_p))$ , the number of times the algorithm visits Step 3  $\leq 2 \log_p d$ . Thus, the number of steps is polynomial in input size. Jacobian determinant's zeroness in Step 1 can also be checked in randomized polynomial time.

Thus, we get an efficient (RP) algorithm to test algebraic independence of two sum of univariates.

## 4.5 Characterization of zero Jacobian

We also give an exact characterization of the cases with zero Jacobian determinant over  $\mathbb{F}_2$ . We use the fact that every polynomial  $f \in \mathbb{F}_p[x_1, x_2]$  can also be viewed as a

polynomial over  $\mathbb{F}_p(x_1^p, x_2^p)$ . For  $\mathbb{F}_2$ , every polynomial  $f$  can be viewed as

$$\tilde{f} = a_0 + a_1x_1 + a_2x_2 + a_3x_1x_2 \quad (4.22)$$

where  $a_i$ 's  $\in \mathbb{F}_2[x_1^2, x_2^2]$ .

Similarly, let us say, we have another polynomial  $g \in \mathbb{F}_2[x_1, x_2]$  such that

$$\tilde{g} = b_0 + b_1x_1 + b_2x_2 + b_3x_1x_2 \quad (4.23)$$

where  $b_i$ 's  $\in \mathbb{F}_2[x_1^2, x_2^2]$ .

**Proposition 4.7.** *Jacobian determinant,  $\det(J(f, g)) = 0$  if and only if  $\frac{a_1}{b_1} = \frac{a_2}{b_2} = \frac{a_3}{b_3}$ .*

*Proof.* Now  $\det(J(f, g)) = 0$  means  $\det(J(\tilde{f}, \tilde{g})) = 0 \equiv d\tilde{f} \wedge d\tilde{g} = 0$ . Now, we have

$$d\tilde{f} = (a_1 + a_3x_2)dx_1 + (a_2 + a_3x_1)dx_2 \quad (4.24)$$

and

$$d\tilde{g} = (b_1 + b_3x_2)dx_1 + (b_2 + b_3x_1)dx_2 \quad (4.25)$$

which on invoking the  $d\tilde{f} \wedge d\tilde{g} = 0$  condition, yields

$$\frac{a_1 + a_3x_2}{b_1 + b_3x_2} = \frac{a_2 + a_3x_1}{b_2 + b_3x_1} \quad (4.26)$$

which gives

$$\begin{vmatrix} a_1 & a_2 \\ b_1 & b_2 \end{vmatrix} \cdot 1 + \begin{vmatrix} a_1 & a_3 \\ b_1 & b_3 \end{vmatrix} \cdot x_1 + \begin{vmatrix} a_3 & a_2 \\ b_3 & b_2 \end{vmatrix} \cdot x_2 = 0 \quad (4.27)$$

Now the coefficients of 1,  $x_1$  and  $x_2$  should all be zero. Hence, we get

$$\frac{a_1}{b_1} = \frac{a_2}{b_2} = \frac{a_3}{b_3}. \quad (4.28)$$

□

## Chapter 5

# Alternative Criterion for positive characteristic: Jacobian Lifting

We have seen that a zero Jacobian determinant over  $\mathbb{F}_p$  implies that the Jacobian determinant is divisible by  $p$  when seen over  $\mathbb{Q}$ . The question we ask is whether we can perturb our input polynomials by adding rational functions which are congruent to zero modulo  $p$  (we call this process as ‘lifting’), such that the Jacobian determinant becomes zero modulo a higher power of  $p$  when seen over  $\mathbb{Q}$ . We show in this chapter (in 5.3.1) that this can be achieved for an arbitrarily high power of  $p$  when the input polynomials are algebraically dependent. We further show using the Witt-Jacobian criterion given in [MSS12], that one cannot achieve this beyond a certain power of  $p$  when the input polynomials are algebraically independent. We finally show in 5.4 using Lüroth’s theorem that a much stronger result can be obtained in the two-polynomials case: we show that the Jacobian determinant can be made zero over  $\mathbb{Q}$  by such perturbations, or equivalently, that the dependence of two polynomials over  $\mathbb{F}_p$  can be lifted to the dependence over  $\mathbb{Q}$ . These results offer differential equation based criteria for testing algebraic independence.

## 5.1 Preliminaries

### 5.1.1 Witt Jacobian Criterion

In [MSS12], a new method was devised to faithfully differentiate polynomials over  $\mathbb{F}_p$ , thereby getting a generalization of the Jacobian - the Witt Jacobian. A key idea is to lift the coefficients of the polynomials from  $\mathbb{F}_p$  to  $\hat{\mathbb{Z}}_p$  ( $p$ -adics), thus moving to a field of zero characteristic.

Let us say the polynomials  $f_1, \dots, f_n \in \mathbb{F}_p[x_1, \dots, x_n]$  get lifted as  $f_1, \dots, f_n \rightarrow \hat{f}_1, \dots, \hat{f}_n$  where  $\hat{f}_1, \dots, \hat{f}_n \in \hat{\mathbb{Z}}_p[x_1, \dots, x_n]$ .

**Definition 5.1.** For  $\ell \geq 1$ , the  $\ell^{\text{th}}$  **Witt-Jacobian polynomial** is defined as,

$$WJP_\ell(f_1, \dots, f_n) = (\hat{f}_1, \dots, \hat{f}_n)^{p^{\ell-1}-1} \cdot \det(J(\hat{f}_1, \dots, \hat{f}_n)) \cdot \prod_{i=1}^n x_i. \quad (5.1)$$

**Definition 5.2.** A Witt-Jacobian polynomial  $f$  is called  $(\ell + 1)$ - **degenerate** if the coefficients of  $x^\alpha := x_1^{\alpha_1} \cdots x_n^{\alpha_n}$  in  $f$  is divisible by  $p^{\min[v_p(\alpha), \ell]+1}$ ,  $\forall \alpha \in \mathbb{N}^n$  where  $v_p(\alpha)$  is the highest power of  $p$  dividing all  $\alpha_n$ .

The explicit Witt-Jacobian criterion for algebraic independence is given as:

**Theorem 5.3.**  $f_1, \dots, f_n$  are algebraically independent over  $\mathbb{F}_p$  if and only if the  $(\ell+1)^{\text{th}}$  Witt-Jacobian polynomial  $WJP_{\ell+1}(f_1, \dots, f_n) = (\hat{f}_1, \dots, \hat{f}_n)^{p^{\ell-1}-1} \cdot \det(J(\hat{f}_1, \dots, \hat{f}_n)) \cdot \prod_{i=1}^n x_i$  is not  $(\ell + 1)$  degenerate for  $\ell \geq \log_p[\mathbb{F}(x_1, \dots, x_n) : \mathbb{F}(f_1, \dots, f_n)]_{\text{insep}}$ .

where  $[\mathbb{F}(x_1, \dots, x_n) : \mathbb{F}(f_1, \dots, f_n)]_{\text{insep}}$  is the inseparability degree of the field extension  $\mathbb{F}(x_1, \dots, x_n)/\mathbb{F}(f_1, \dots, f_n)$  (see [MSS12]). This degree has an upper bound which depends on the transcendence degree of the polynomials:

$$[\mathbb{F}(x_1, \dots, x_n) : \mathbb{F}(f_1, \dots, f_n)]_{\text{insep}} \leq \delta^r, \quad (5.2)$$

where  $r := \text{trdeg}(f_1, \dots, f_n)$  and  $\delta$  is the maximum degree.

We refer to [MSS12] for the proofs.

Since degeneracy testing involves looking at the coefficients of each monomials, and we do not have a sub-exponential bound on the sparsity of the Witt-Jacobian polynomial, it becomes hard to get an efficient algorithm from this criterion to test algebraic independence. The algorithm suggested puts the problem in the complexity class  $\mathbf{NP}\#\mathbf{P}$  i.e. we get a polynomial time algorithm on a Nondeterministic Turing Machine with a  $\#\mathbf{P}$  oracle.

### 5.1.2 Lüroth's Theorem

**Theorem 5.4. (*Lüroth's Theorem*)** *Let  $K$  be a field and  $M$  be an intermediate field between field between  $K$  and  $K(X)$ , for some indeterminate  $X$ . Then there exists a rational function  $f(X) \in K(X)$  such that  $M = K(f(X))$  i.e. every intermediate extension between  $K$  and  $K(X)$  is simple.*

**Theorem 5.5. (*Lüroth's Theorem for Multivariates*)** *If  $k \subset K \subset k(x_1, x_2, \dots, x_n)$ ,  $\text{tr.deg.} K/k = 1$  and  $K \neq k$ , then  $K = k(g)$ ,  $g \in k(x_1, x_2, \dots, x_n)$ .*

**Theorem 5.6. (*Extended Lüroth's Theorem*)** *If, under the assumption of Theorem 5.2,  $K$  contains a non-constant polynomial over  $k$ , then  $K$  has a generator which is a polynomial over  $k$ .*

For a complete exposition of the proofs, we refer to [Sch00]. For an elementary proof of the Lüroth's theorem, see [Ben04].

## 5.2 Main Results

We need some definitions first to state our results.

**Definition 5.7.  $p$ -adic valuation** of a polynomial  $f$  over  $\mathbb{Q}$  is defined as the highest power of  $p$  which divides the coefficients of every monomial of  $f$ .

**Example 5.1.** *2-adic valuation of  $8x^2 + 16x + 4$  is 2 since  $2^2$  divides all the coefficients.*

**Definition 5.8. Lifting** a polynomial  $f$  over  $\mathbb{F}_p$  is adding to it, a polynomial or rational function which is zero over  $\mathbb{F}_p$ , i.e. whose coefficients of every monomial (in the

numerator) is divisible by  $p$ . The added polynomial or rational function is called the lift.

We now state our main theorems:

**Theorem 5.9.** *For polynomials  $f_1, \dots, f_n \in \mathbb{F}_p[x_1, \dots, x_n]$ , the  $p$ -adic valuation of the Jacobian determinant  $\det(J(f_1, \dots, f_n))$  can be increased to an arbitrarily high number by lifting the polynomials if and only if they are algebraically dependent over  $\mathbb{F}_p$ . In particular, for independent polynomials  $f_1, \dots, f_n$ , we cannot increase by lifting, the Jacobian determinant's  $p$ -adic valuation beyond  $\log_p [\mathbb{F}(x_1, \dots, x_n) : \mathbb{F}(f_1, \dots, f_n)]_{\text{insep}}$ .*

For the two polynomials case, we have a much stronger result.

**Theorem 5.10.** *For polynomials  $f_1, f_2 \in \mathbb{F}_p[x, y]$  seen over  $\mathbb{Q}$ , there exist lifts  $\delta_1, \delta_2 \in \mathbb{Q}[x, y]$ , such that  $f_1 + p \cdot \delta_1$  and  $f_2 + p \cdot \delta_2$  are algebraically dependent over  $\mathbb{Q}$  if and only if  $f_1$  and  $f_2$  are algebraically dependent over  $\mathbb{F}_p$ .*

**Corollary 5.11.** *For polynomials  $f_1, f_2 \in \mathbb{F}_p[x, y]$  seen over  $\mathbb{Q}$ , there exists lifts  $\delta_1, \delta_2 \in \mathbb{Q}[x, y]$ , such that the  $p$ -adic valuation of the Jacobian determinant of the lifted polynomials,  $\det(J(f_1 + p \cdot \delta_1, f_2 + p \cdot \delta_2))$  is infinity, if and only if  $f_1$  and  $f_2$  are algebraically dependent over  $\mathbb{F}_p$ .*

The above two theorems also give each a differential equation based criterion to test algebraic independence of polynomials over fields of positive characteristic which we have described later in the chapter.

## 5.3 Proof of the theorems:

### 5.3.1 Proof of theorem 5.9: $p$ -adic valuation lifting

*Proof.*  $\Rightarrow$  (Dependence implies that an arbitrary increase in the  $p$ -adic valuation is possible by lifting). We need the following lemma to prove this direction.

**Lemma 5.12.**  *$p$ -adic valuation of the evaluated annihilating polynomial can be increased to an arbitrarily high number by lifting the polynomials.*



*Proof.* Let us say, we are given polynomials  $f_1, \dots, f_n$  which are algebraically dependent over  $\mathbb{F}_p$  but independent over  $\mathbb{Q}$ . Let  $A(y_1, \dots, y_n)$  be the minimal annihilating polynomial of  $f_1, \dots, f_n$ .

Now this means that  $A(f_1(x_1, \dots, x_n), \dots, f_n(x_1, \dots, x_n))$  is a zero polynomial over  $\mathbb{F}_p$  but this is not a zero polynomial over  $\mathbb{Q}$  since  $f_1, \dots, f_n$  are independent over  $\mathbb{Q}$ . So,  $p$  must divide all the coefficients of the monomials in  $A(f_1(x_1, \dots, x_n), \dots, f_n(x_1, \dots, x_n))$ . We call the highest power of  $p$  dividing all the coefficients, as the  $p$ -adic valuation of the evaluated annihilating polynomial.

Let us say, we have

$$A(y_1, \dots, y_n) = \sum_{i=0}^t a_i y_1^{\alpha_{i,1}} \cdots y_n^{\alpha_{i,n}}. \quad (5.3)$$

On evaluating, we get:

$$A(f_1, \dots, f_n) = \sum_{i=0}^t a_i f_1^{\alpha_{i,1}} \cdots f_n^{\alpha_{i,n}} \equiv 0 \pmod{p}. \quad (5.4)$$

Now, we lift the polynomials as

$$f_1 \mapsto f_1 + p\delta_1, \dots, f_n \mapsto f_n + p\delta_n. \quad (5.5)$$

For increasing the  $p$ -adic valuation by lifting, we want

$$A(f_1 + p\delta_1, \dots, f_n + p\delta_n) \equiv 0 \pmod{p^2} \quad (5.6)$$

which implies

$$\sum_{i=0}^t a_i (f_1 + p\delta_1)^{\alpha_{i,1}} \cdots (f_n + p\delta_n)^{\alpha_{i,n}} \equiv 0 \pmod{p^2}. \quad (5.7)$$

On expansion, we get:

$$\sum a_i f_1^{\alpha_{i,1}} \cdots f_n^{\alpha_{i,n}} + p \sum \delta_k \sum a_i \alpha_{i,k} f_1^{\alpha_{i,1}} \cdots f_k^{\alpha_{i,k}-1} \cdots f_n^{\alpha_{i,n}} \equiv 0 \pmod{p^2} \quad (5.8)$$

$$p^{-1} \left( \sum a_i f_1^{\alpha_{i,1}} \cdots f_n^{\alpha_{i,n}} \right) + \sum \delta_k \sum a_i \alpha_{i,k} f_1^{\alpha_{i,1}} \cdots f_k^{\alpha_{i,k}-1} \cdots f_n^{\alpha_{i,n}} \equiv 0 \pmod{p} \quad (5.9)$$

Note that  $p|A(f_1, \dots, f_n)$ , so  $p^{-1}A(f_1, \dots, f_n)$  makes sense. Using it, we can re-write the above equation as

$$p^{-1}A(f_1, \dots, f_n) + \sum \delta_k (\partial_{y_k} A) |_{(f_1, \dots, f_n)} \equiv 0 \pmod{p}. \quad (5.10)$$

Now due to the minimality of  $A$ , at least one of the  $(\partial_{y_k} A) |_{(f_1, \dots, f_n)} \not\equiv 0 \pmod{p}$ .

We pick one such  $k$  to get the solution

$$\delta_i = 0, i = 1, \dots, n, i \neq k; \quad \delta_k = -\frac{p^{-1}A(f_1, \dots, f_n)}{(\partial_{y_k} A) |_{(f_1, \dots, f_n)}}. \quad (5.11)$$

Such that  $\delta_k \in \mathbb{F}_p(x, y)$ . We can iterate the process  $j$ -times to get the lifted polynomials  $f_k \mapsto f_k + p^2 \delta_{k,0} + \dots + p^{2^{j-1}} \delta_{k,j-1}$  where  $\delta_{k,j-1}$  is the polynomial by which we lift  $f_k$  from  $(j-1)$ -th step to the  $j$ -th step. So after  $j$ -steps, we get

$$A(f_1, \dots, f_n) \equiv 0 \pmod{p^{2^j}} \quad (5.12)$$

Hence lemma 1 follows. □

We now claim that the same lifts used for increasing the  $p$ -adic valuation of the evaluated annihilating polynomial, will increase the  $p$ -adic valuation of the Jacobian determinant,  $\det(J(f_1, \dots, f_n))$  to the same level. To prove the claim, we consider the equation

$$A(y_1, \dots, y_n) |_{(f_1, \dots, f_n)} \equiv 0 \pmod{p^{2^j}} \quad (5.13)$$

Now we apply the formal derivative on the equation to get

$$d(A(f_1, \dots, f_n)) \equiv 0 \pmod{p^{2^j}}, \text{ or} \quad (5.14)$$

$$\partial_{y_1} A(y_1, \dots, y_n) |_{(f_1, \dots, f_n)} df_1 + \dots + \partial_{y_n} A(y_1, \dots, y_n) |_{(f_1, \dots, f_n)} df_n \equiv 0 \pmod{p^{2^j}} \quad (5.15)$$

Minimality of  $A$  implies there will be at least one  $\partial_{y_k} A(y_1, \dots, y_n) |_{(f_1, \dots, f_n)} \not\equiv 0 \pmod{p}$ . So we take wedge-product of  $dA$  with  $df_1 \wedge \dots \wedge df_{k-1} \wedge df_{k+1} \wedge \dots \wedge df_n$ . Now if  $df_1 \wedge \dots \wedge df_{k-1} \wedge df_{k+1} \wedge \dots \wedge df_n \equiv 0 \pmod{p^{2^j}}$ , we trivially get  $df_1 \wedge \dots \wedge df_n \equiv 0 \pmod{p^{2^j}}$ ,

since from chapter 3, we have

$$\det(J(f_1, \dots, f_n)) = \frac{df_1 \wedge \dots \wedge df_n}{dx_1 \wedge \dots \wedge dx_n} \quad (5.16)$$

which gives us that  $\det(J(f_1, \dots, f_n)) \equiv 0 \pmod{p^{2^j}}$ .

While if  $df_1 \wedge \dots \wedge df_{k-1} \wedge df_{k+1} \wedge \dots \wedge df_n \not\equiv 0 \pmod{p^{2^j}}$ , the wedge product yields

$$dA(f_1, \dots, f_n) \wedge (df_1 \wedge \dots \wedge df_{k-1} \wedge df_{k+1} \wedge \dots \wedge df_n) \equiv 0 \pmod{p^{2^j}}, \text{ or} \quad (5.17)$$

$$\left( \sum \partial_{y_m} A(y_1, \dots, y_n) |_{(f_1, \dots, f_n)} df_m \right) \wedge (df_1 \wedge \dots \wedge df_{k-1} \wedge df_{k+1} \wedge \dots \wedge df_n) \equiv 0 \pmod{p^{2^j}} \quad (5.18)$$

and we get:

$$(\partial_{y_k} A(y_1, \dots, y_n) |_{(f_1, \dots, f_n)}) df_1 \wedge \dots \wedge df_n \equiv 0 \pmod{p^{2^j}}. \quad (5.19)$$

Since we picked  $k$  such that  $\partial_{y_k} A(y_1, \dots, y_n) |_{(f_1, \dots, f_n)} \not\equiv 0 \pmod{p}$ , we get  $df_1 \wedge \dots \wedge df_n \equiv 0 \pmod{p^{2^j}}$  and hence  $\det(J(f_1, \dots, f_n)) \equiv 0 \pmod{p^{2^j}}$ .

Thus we have shown that if  $f_1, \dots, f_n$  are algebraically independent over  $\mathbb{F}_p$ , the  $p$ -adic valuation of the  $\det(J(f_1, \dots, f_n))$  can be increased to an arbitrarily high number.

$\Leftarrow$  (Independence implies that  $p$ -adic valuation of the Jacobian cannot be increased beyond a bound). We use Theorem 5.3 for proving this direction. In particular we show that an increase in the  $p$ -adic valuation cannot be attained after  $\log_2(\log_p[\mathbb{F}(x, y) : \mathbb{F}(f, g)]_{insep} + 1)$  steps.

*Proof.* We prove it by assuming the contrary.

We assume that the  $p$ -adic valuation of the  $\det(J(f_1, \dots, f_n))$  can be increased arbitrarily. So after  $j$  steps, we get  $\det(J(f_1, \dots, f_n)) \equiv 0 \pmod{p^{2^j}}$ . From the Witt Jacobian criterion, we have the Witt Jacobian polynomial:

$WJP_{\ell+1}(f_1, \dots, f_n) = (\hat{f}_1, \dots, \hat{f}_n)^{p^{\ell-1}-1} \cdot \det(J(\hat{f}_1, \dots, \hat{f}_n)) \cdot \prod_{i=1}^n x_i$ . So, we also get that after  $j$  lifting steps,  $WJP_{\ell+1}(f_1, \dots, f_n) \equiv 0 \pmod{p^{2^j}}$  i.e.  $p^{2^j}$  divides all the coefficients of  $WJP(f_1, \dots, f_n)$ , so we call it  $2^j$  degenerate.

This happens for arbitrary  $j$ . Thus, we pick  $j$  to be  $\log_2(\log_p[\mathbb{F}(x, y) : \mathbb{F}(f_1, f_2)]_{insep} + 1)$  such that after  $j$  lifting steps, the Witt Jacobian polynomial is  $\log_p[\mathbb{F}(x, y) : \mathbb{F}(f_1, f_2)]_{insep} +$

1 degenerate. This contradicts Theorem 5.3 when  $f_1, \dots, f_n$  are algebraically independent which states that the Witt Jacobian polynomial cannot be  $(\ell + 1)$  degenerate for  $\ell \geq \log_p[\mathbb{F}(x, y) : \mathbb{F}(f_1, f_2)]_{insep}$ .  $\square$

This finishes the proof of the theorem.  $\square$

Now, using Theorem 5.9, we introduce a criterion for independence testing. We demonstrate this in the two-polynomials case. So, we start with input  $f_0$  and  $g_0$  such that  $df_0 \wedge dg_0 \equiv 0 \pmod{p}$ . If not, we are done already and  $f_0$  and  $g_0$  are independent. Now, we try to find rational functions  $\delta_1$  and  $\mu_1$  such that

$$d(f_0 + p \cdot \delta_1) \wedge d(g_0 + p \cdot \mu_1) \equiv 0 \pmod{p^2}$$

equivalently, it becomes

$$p^{-1}d(f_0 \wedge dg_0) + df_0 \wedge d\mu_1 + d\delta_1 \wedge dg_0 \equiv 0 \pmod{p}$$

If such a solution exists, we find  $f_1 := f_0 + p \cdot \delta_1$  and  $g_1 := g_0 + p \cdot \mu_1$ .

Now,  $df_1 \wedge dg_1 \equiv 0 \pmod{p^2}$ . As the theorem suggests, we repeat the process  $i = m := \log_2(\log_p[\mathbb{F}(x, y) : \mathbb{F}(f, g)]_{insep} + 1)$  many times. At this stage if  $f_i$  and  $g_i$  can be further lifted, we deduce that  $f_0$  and  $g_0$  are algebraically independent over  $\mathbb{F}_p$ . Non-existence of such lifts will imply algebraic independence of the two polynomials  $f_0$  and  $g_0$ . In terms of the above differential equations, it is similar to finding  $\delta = \sum_1^m p^{2^{i-1}} \delta_i$  and  $\mu = \sum_1^m p^{2^{i-1}} \mu_i$  where  $\delta_i, \mu_i \in (\mathbb{Z}/p^{2^{i-1}}\mathbb{Z})(x, y)$  such that

$$d(f_0 + \delta) \wedge d(g_0 + \mu) \equiv 0 \pmod{p^{2^m}} \tag{5.20}$$

**Criterion :** Solution to the above differential equation exists if and only if  $f$  and  $g$  are algebraically dependent.

For algorithms to find rational function solutions to a linear first order partial differential equations, we refer to [BCW05].

**Conjecture 1 :** If  $f$  and  $g$  are algebraically independent,  $J(f, g)$  can be lifted exactly  $\log_2(\log_p[\mathbb{F}(x, y) : \mathbb{F}(f, g)]_{insep} + 1)$  many times.

**Conjecture 2 :**  $\delta_i, \mu_i \in (\mathbb{Z}/p^{2^{i-1}}\mathbb{Z})[x, y]$  suffice i.e. non-existence of polynomial solutions  $(\delta, \mu)$  to the above equation (5.20) is sufficient to establish independence.

### 5.3.2 Proof of theorem 5.10: Lifting to Rationals

We now use Theorem 5.8 (Extended Lüroth's theorem) to prove that for two algebraically dependent polynomials  $f_1$  and  $f_2$  over  $\mathbb{F}_p$ , their dependence can be lifted to dependence over  $\mathbb{Q}$ .

*Proof.* If  $f_1, f_2 \in \mathbb{F}_p[x_1, x_2]$  are algebraically dependent over  $\mathbb{F}_p$ , then we can apply Theorem 5.2 and 5.3 where  $\mathbb{K} = \mathbb{F}_p(f_1, f_2)$ . which implies that there exists  $h \in \mathbb{F}_p[x_1, x_2]$  such that  $f_1 = g_1(h)$  and  $f_2 = g_2(h)$ , where  $g \in \mathbb{F}_p(t)$  Also note that from Lemma 5.8, univariates  $g_1(t)$  and  $g_2(t)$  are algebraically dependent over  $\mathbb{Q}$  as well. Thus, the evaluated  $g_1(t), g_2(t)$  at  $t = h(x_1, x_2)$  when the evaluations are seen over  $\mathbb{Q}$  are also algebraically dependent over  $\mathbb{Q}$ . Let us called these evaluated  $g_1(t)$  and  $g_2(t)$  as  $\tilde{f}_1$  and  $\tilde{f}_2$  respectively. Thus  $\tilde{f}_1$  and  $\tilde{f}_2$  are the lifted  $f_1$  and  $f_2$  which are dependent over  $\mathbb{Q}$  since:

$\tilde{f}_1 \equiv f_1 \pmod{p}$  and  $\tilde{f}_2 \equiv f_2 \pmod{p}$ . We also get the desired lifts as:

$\delta_i = p^{-1}(f_i - g_i(h(x_1, x_2)))$  seen over  $\mathbb{Q}$ . □

## 5.4 Lifting to rationals: Independence testing criteria

The above theorem offers two directions to get an algebraic independence testing algorithm.

- Computing the Lüroth generator which by itself is a certificate for dependence. Algorithms are known to compute Lüroth generator, for instance refer to [Chè10]. However, no algorithm is known with time complexity polynomial in terms of log of the degrees of the polynomials.

- The above lifting of dependence to dependence over  $\mathbb{Q}$  implies that zero Jacobian determinant over  $\mathbb{F}_p$  can be lifted to zero Jacobian determinant over  $\mathbb{Q}$  if and only if  $f_1$  and  $f_2$  are algebraically dependent over  $\mathbb{F}_p$ . We therefore set up the differential equation capturing this property and claim that a rational function solution to the differential equation exists if and only if  $f_1$  and  $f_2$  are algebraically dependent.

$$d(f_1 + p\delta_1) \wedge d(f_2 + p\delta_2) = 0. \quad (5.21)$$



## Chapter 6

# Alternative Criterion over Zero

## Characteristic: Supersparse

### Polynomials

Lüroth's theorem (see section 5.1.2) relates algebraic independence of given two polynomials to their decomposition. It asserts that they have a common generator if they are algebraically dependent. We use this property to prove results in the supersparse model of computation. We show in 6.3 that the minimal annihilating polynomial of two algebraically dependent supersparse polynomials over  $\mathbb{Q}$  is sparse in most of the cases (and exactly characterize those cases as well). We further give an alternative randomized polynomial time algorithm for testing algebraic independence of two supersparse polynomials over  $\mathbb{Q}$  in 6.4. We finally prove in 6.5, a result about two algebraically dependent homogeneous polynomials.

#### 6.1 Preliminaries

**Definition 6.1.** [KK05] **Supersparse polynomial.** A supersparse (lacunary) polynomial

$$f(x_1, \dots, x_n) = \sum_{i=0}^t a_i x_1^{\alpha_{i,1}} \cdots x_n^{\alpha_{i,n}} \quad (6.1)$$

is input by a list of its coefficients and corresponding term degree vectors in binary.

One cannot evaluate a supersparse polynomial at algebraic numbers in polynomial-time in its size, because the value of the polynomial can have exponential size, say  $2^{100}$  digits. Important exceptions are evaluating at roots of unity. A supersparse polynomial can be represented by a straight-line program of size  $O(\text{size } f)$  via evaluating its terms with repeated squaring [Kal88].

## 6.2 Main Results

### 6.2.1 Degree bound on annihilating polynomial

We prove the following theorem about the annihilating polynomial of two supersparse polynomials.

**Theorem 6.2.** *If two supersparse polynomials,  $f_1$  and  $f_2 \in \mathbb{Q}[x, y]$  which do not decompose as  $f_i(x, y) = g_i(h_i(x, y))$ , where  $h_i(x, y) = x^m y^n + c$ ,  $m, n \in \mathbb{N}$ ,  $c \in \mathbb{Q}$  are algebraically dependent, their minimal annihilating polynomial,  $A$  is sparse.*

*Let  $t_i$  be the number of non-zero monomials in the supersparse representation of  $f_i$  and  $t := \max(t_1, t_2)$ , then  $\deg(A) \leq 5t^2$ .*

### 6.2.2 Algebraic independence testing algorithm

Using the above result, we also give an alternative randomized polynomial time algorithm for testing algebraic independence of two supersparse polynomials over  $\mathbb{Q}$ .

### 6.2.3 Annihilating polynomial of homogeneous polynomials

We give an alternative proof to a known result on homogeneous polynomials. Most of the references use Lüroth's theorem to prove it.

**Theorem 6.3.** *Let  $f, g \in \mathbb{F}[x, y]$  be two non-constant homogeneous polynomials of degree at most  $\delta \geq 1$ . Then  $f, g$  are algebraically dependent over  $\mathbb{F}$  if and only if  $f^m = c \cdot g^n$  for some field constant  $c$ .*



### 6.3 Proof of Theorem 6.2

We first state a key theorem (without proof) which we'll be using to prove Theorem 6.2. For the proof, see [Zan07].

**Theorem 6.4.** (Zannier'07) *If  $f \in \mathbb{K}[x]$  where  $\mathbb{K}$  is a field of zero characteristic such that  $f = g(h)$ ,  $h \neq ax^m + b$  and  $f$  is sparse with number of non-zero terms being  $l$ , then  $\deg(g) \leq l(2l + 1)$ .*

We now prove the lemmas which are also required to prove the theorem.

**Lemma 6.5.** *If polynomials  $f_1(x, y)$  and  $f_2(x, y)$  are algebraically dependent over a field  $\mathbb{F}$ , there exists a polynomial  $h \in \mathbb{F}[x, y]$  such that  $f_1$  and  $f_2$  decompose respectively as  $f_1 = g_1(h)$  and  $f_2 = g_2(h)$ , where  $g_1, g_2 \in \mathbb{K}[t]$ .*

*Proof.* This is a direct consequence of Lüroth's theorem (Theorem 5.5). The Lüroth generator  $h$ , given by the theorem serves the purpose of the lemma.  $\square$

Note that the  $h$  obtained in Lüroth's theorem satisfies a stronger property than what is required for the above lemma. The Lüroth generator  $h$ , for  $f$  and  $g$  lives in  $\mathbb{F}(f, g)$  which is not required by the above lemma.

**Lemma 6.6.** [Kay09] *Let  $f_1, \dots, f_m \in \mathbb{F}[x_1, \dots, x_n]$  be a set of algebraically dependent polynomials over the field  $\mathbb{F}$ , such that none of its proper subset is algebraically dependent, equivalently the transcendence degree of the set of polynomials is  $n - 1$ . Then the ideal of the annihilating polynomials is generated by a unique irreducible (up to a constant multiple) polynomial  $A$ . So in this case, the ideal of the annihilating polynomials is a principal ideal.*

*Proof.* Let  $A \in \mathbb{F}[y_1, \dots, y_m]$  be a minimal degree annihilating polynomial of  $f_1, \dots, f_m$ . First, we prove that it is an  $\mathbb{F}$ -irreducible polynomial. If it is reducible, it is the product of two polynomials with smaller degree. Let us assume,

$$A(y_1, \dots, y_m) = A_1(y_1, \dots, y_m) \cdot A_2(y_1, \dots, y_m) \quad (6.2)$$

Now, as  $A(f_1, \dots, f_m) = 0$ , either  $A_1(f_1, \dots, f_m) = 0$  or  $A_2(f_1, \dots, f_m) = 0$ . In both the cases, we get an annihilating polynomial of smaller degree, this contradicts the assumption that  $A$  was the minimal degree annihilating polynomial of  $f_1, \dots, f_m$ .

Now, the uniqueness of the minimal irreducible annihilating polynomial can be proved using resultant. Let  $B(y_1, \dots, y_m)$  be another irreducible annihilating polynomial of  $f_1, \dots, f_m$ . We have to prove that  $A = c \cdot B$  for some field constant  $c$ . Since no proper subset of  $f_1, \dots, f_m$  are algebraically dependent,  $f_2, \dots, f_m$  are algebraically independent. So, both  $A$  and  $B$  has  $y_1$ . Now, let

$$p(y_2, \dots, y_m) = \text{RESULTANT}_{y_1}(A(y_1, \dots, y_m), B(y_1, \dots, y_m)). \quad (6.3)$$

We use  $\mathbf{y}$  to denote  $y_1, \dots, y_m$ .

From a standard property of resultant, we can find  $A'(\mathbf{y})$  and  $B'(\mathbf{y})$  such that

$$p(y_2, \dots, y_m) = A'(\mathbf{y}) \cdot A(\mathbf{y}) + B'(\mathbf{y}) \cdot B(\mathbf{y}). \quad (6.4)$$

Plugging in  $f_1, \dots, f_m$  in place of  $y_1, \dots, y_m$ , we get

$$p(f_2, \dots, f_m) = A'(f_1, \dots, f_m) \cdot A(f_1, \dots, f_m) + B'(f_1, \dots, f_m) \cdot B(f_1, \dots, f_m). \quad (6.5)$$

This implies  $p(f_2, \dots, f_m) = 0$ . But as  $f_2, \dots, f_m$  are algebraically independent,  $p$  must be zero.

now, resultant of  $A$  and  $B$  is zero implies that they share a common factor. But  $A$  is irreducible as already established. Hence  $A = c \cdot B$ .  $\square$

**Lemma 6.7.** *If  $A$  is the minimal annihilating polynomial of  $f_1(x_1, x_2)$  and  $f_2(x_1, x_2)$  over a field  $k$ , then  $A$  is also the minimal annihilating polynomial (up to a constant multiple) of the non-constant polynomials  $f_1(x_1, c)$  and  $f_2(x_1, c)$  obtained after fixing  $x_2 = c \in k(x_1)$ .*

*Proof.* Let us call  $B$  the minimal annihilating polynomial of  $f_1(x_1, c)$  and  $f_2(x, c)$ . Now by using the above Lemma 6.6, the set of annihilating polynomials of  $f_1(x, c)$  and  $f_2(x, c)$  form a principal ideal  $U$  generated by  $B$ . Now since  $A(f_1(x_1, x_2), f_2(x_1, x_2)) = 0$ , we also have  $A(f_1(x, c), f_2(x, c)) = 0$ . Thus  $A \subset U$  implying that  $B$  divides  $A$ . But  $A$  is irreducible, hence  $A = \alpha \cdot B$ , where  $\alpha$  is a field constant.  $\square$

**Lemma 6.8.** *Let  $f_1 = g_1(h)$  and  $f_2 = g_2(h)$  be two algebraically dependent bivariate polynomials over a field  $k$ . Then minimal annihilating polynomial of  $f_1$  and  $f_2$  is same as the minimal annihilating polynomial of  $g_1(t)$  and  $g_2(t)$  (up to a constant multiple).*

*Proof.* Let us call  $A$  the minimal annihilating polynomial of  $g_1(t)$  and  $g_2(t)$  and  $B$  the minimal annihilating polynomial of  $f_1$  and  $f_2$ . Now since  $A(g_1(t), g_2(t)) = 0$  and  $t$  is an indeterminate, replacing it with any element  $h \in k(X)$  preserves the dependence. Hence  $A(g_1(h), g_2(h)) = A(f_1, f_2) = 0$ . Thus  $A$  annihilates  $f_1$  and  $f_2$ . Now invoking the irreducibility on  $A$  and  $B$ , we get the desired result.  $\square$

#### **Proof Idea of Theorem 6.2:**

1. Theorem 6.1 relates the problem of algebraic dependence of two polynomials to the problem of polynomial decomposition. It asserts the existence of  $g_1$ ,  $g_2$  and  $h$  for the dependent polynomials  $f_1$  and  $f_2$ .
2. Lemma 6.6 implies that it suffices to work with  $g_1$  and  $g_2$  for studying the annihilating polynomial of  $f_1$  and  $f_2$ .
3. Theorem 6.4 suggests degree bounds on  $g_1$  and  $g_2$  in terms of the sparsity of  $f_1$  and  $f_2$  when  $h$  is univariate. Lemma 6.5 implies that annihilating polynomial does not change if we fix one of the variables in  $h(x, y)$  to a constant to get a univariate  $h$ .
4. Invoke Perron's bound to get a degree bound on the annihilating polynomial.

*Proof.* If  $f$  and  $g$  are algebraically dependent, then by a Corollary to the Extended Lüroth's theorem (Theorem 5.4), we get that there exists an  $h \in \mathbb{Q}[x, y]$  such that  $f_1 = g_1(h)$  and  $f_2 = g_2(h)$ . Now by Lemma 6.6, to get a degree bound on the minimal annihilating polynomial of  $f_1$  and  $f_2$ , getting the degree bounds of  $g_1$  and  $g_2$  would be sufficient.

We fix one of the variables to get two univariate non-constant polynomials  $f'_1$  and  $f'_2$  which gives the decomposition  $f'_1 = g_1(h')$  and  $f'_2 = g_2(h')$  where  $h'$  is just the evaluated  $h$  obtained by fixing the variable. Indeed Lemma 6.5 guarantees that the above operation preserves the minimal annihilating polynomial.

We are now set to apply Theorem 6.4 on univariates  $f'_1$  and  $f'_2$ . Note that in Theorem 6.4, we get the bound only if  $h$  is not of the form  $ax^m + b$ . Hence, in the bivariate case, we get the bound in the cases in which we can fix one of the variables in a way that the evaluated  $h$  is not of the above form i.e. we get the bounds in the cases when  $h' \neq ax^m + b$  or  $h' \neq ay^m + b$ ;  $a, b \in \mathbb{Q}$ .

**Case 1:** Sparsity of  $h(x, y) - h(0, 0) \geq 3$ .

Clearly in this case, at least one of the variable will have distinct non-zero exponents in two distinct monomials, allowing us to set the other variable to a field constant  $\alpha$  such that  $h'$  is not of the form  $ax^m + b$ .

**Case 2:**  $h(x, y) - h(0, 0)$  is a binomial.

Again if one of the variables will have distinct non-zero exponents in two distinct monomials, we can easily get the bound. This leaves us with two interesting cases - when  $h(x, y) - h(0, 0)$  is either of the form (i)  $ax^m y^n + bx^m$  or (ii)  $ax^m + by^n$ . In (i), we plugin  $y = x$  and in (ii), we plugin  $y = x$  (if  $m \neq n$ ), or  $y = x^2$  (if  $m = n$ ), to get an  $h'$  not of the form  $ax^m + b$ .

**Case 3:**  $h(x, y) - h(0, 0)$  is a monomial  $ax^m y^n$ . Here, we cannot apply the theorem.

Thus in the cases (1) and (2), we can apply the Theorem to get the desired bound on  $g_1$  and  $g_2$ . i.e.  $\deg(g_1) \leq t_1(2t_1 + 1)$  and  $\deg(g_2) \leq t_2(2t_2 + 1)$ .

Applying Perron's bound on  $g_1$  and  $g_2$ , we get  $\deg(A) \leq \deg(g_1) \cdot \deg(g_2) \leq 5t^2$ .  $\square$

## 6.4 Independence Testing Algorithm:

---

### ALGORITHM 1:

**Input :** 2 supersparse polynomials  $f_1, f_2 \in \mathbb{Q}[x, y]$ ,  
 $\ell_i :=$  number of non-zero terms in  $f_i$ ;  $\ell := \max(\ell_1, \ell_2)$ .

**Output :** One of the three:

- dependent; (their annihilating polynomial)  $A(y_1, y_2)$ .
- dependent; (their decomposition)  $f_1 = g_1(h)$  and  $f_2 = g_2(h)$ .
- independent.

**Step 1 (Checking for linear dependence):**

- **if** ( $k_1f_1 + k_2f_2 + k_3 = 0$ , for some  $k_1, k_2, k_3 \in \mathbb{Q}$ )  
output “dependent”.
- **else**, proceed to Step 2.

**Step 2 (Checking for decomposition into a monomial):**

- $\text{gcd}_i :=$  GCD of the exponent vectors of the monomials in  $f_i(x, y) - f_i(0, 0)$ .
- **if** ( $\text{gcd}_1$  exists &&  $\text{gcd}_2$  exists &&  $\text{gcd}(\text{gcd}_1, \text{gcd}_2)$  exists)  
let  $(m, n) := \text{gcd}(\text{gcd}_1, \text{gcd}_2)$ , then  $h = x^m y^n$ ;  
compute the decompositions  $f_1 = g_1(h)$  and  $f_2 = g_2(h)$ ;  
output “dependent”; output  $h, g_1, g_2$ .
  - **else, if** ( $\text{gcd}_1$  does not exist &&  $\text{gcd}_2$  does not exist)  
proceed to Step 3.
  - **else**, output “independent”.

**Step 3 (Finding the Annihilating Polynomial):**

- **if** ( $A(y_1, y_2)$  exists such that  $A(f_1, f_2) = 0$ ,  $\deg(A) \leq 5\ell^2$ )  
output “dependent”; output  $A(y_1, y_2)$ .
  - **else**, output “independent”.
- 

### 6.4.1 Proof of Correctness

*Proof.* Here we have two cases

**Case 1:** At least one of  $f_1$  and  $f_2$  is indecomposable.

In this case, there will be no Lüroth generator for  $f_1$  and  $f_2$ . So,  $f_1$  and  $f_2$  are algebraically independent.

Indeed if any of  $f_1$  and  $f_2$  is indecomposable, no corresponding GCD exists in Step 1, and the algorithm outputs  $f_1$  and  $f_2$  as algebraically independent polynomials.

**Case 2:**  $f_1$  and  $f_2$  are both decomposable. There are three cases:

2 (a). Exactly one of  $f_1$  and  $f_2$  decomposes as  $f_i = g_i(x^m y^n)$ .

By Lüroth’s theorem,  $f_1$  and  $f_2$  will be algebraically independent. Indeed if one of the

polynomials does not decompose as  $g_i(x^m y^n)$ , no corresponding GCD exists in Step 1 and the algorithm outputs  $f_1$  and  $f_2$  as algebraically independent polynomials.

2 (b). Both  $f_1$  and  $f_2$  decompose as  $f_i = g_i(x_i^m y_i^n)$ .

If gcd of  $((m_1, n_1), (m_2, n_2))$  exists and is equal to  $x^m y^n$ , then  $f_1 = g'_1(h)$  and  $f_2 = g'_2(h)$ , where  $h = x^m y^n$  which implies by Lüroth's theorem that  $f_1$  and  $f_2$  are dependent. Step 2 of the algorithm asserts that the algorithm outputs the same.

2 (c). Neither of  $f_1$  and  $f_2$  decompose as  $f_i = g_i(x^m y^n)$ .

By Theorem 6.3, when they are dependent, the minimal annihilating polynomial will have a degree  $\leq 5l^2$ . Step 3 of the algorithm searches for an annihilating polynomial of degree  $\leq 5l^2$  and outputs it if one exists. Also, clearly it will not find the annihilating polynomial if  $f_1$  and  $f_2$  are independent.  $\square$

Note that the algorithm use the following three subroutines:

- 1) Finding the GCD of the exponent vectors of the monomials of a given polynomial.
- ii) Finding decomposition in Step 2.
- iii) Finding the annihilating polynomial with a given degree bound.

We conjecture that Theorem 6.2 and the above algorithm works for polynomials over fields of positive characteristic as well. However, to prove it, one needs to generalize Theorem 6.4 to fields of positive characteristic as well..

## 6.5 Homogeneous Polynomials

We use Lemma 6.6 to give an alternative proof to a known result on homogeneous polynomials. Most of the references (for example, see [Mit13]) use Lüroth's theorem to prove it.

**Theorem 6.9.** *Let  $f, g \in \mathbb{F}[x, y]$  be two non-constant homogeneous polynomials of degree at most  $\delta \geq 1$ . Then  $f, g$  are algebraically dependent over  $\mathbb{F}$  if and only if  $f^m = c \cdot g^n$  for some field constant  $c$ .*

*Proof.* We have:

$$f = \alpha_1 x^{a_1} y^{b_1} + \cdots + \alpha_n x^{a_n} y^{b_n} \quad (6.6)$$

with  $a$  being the total degree of each monomial; and

$$g = \beta_1 x^{c_1} y^{d_1} + \cdots + \beta_m x^{c_m} y^{d_m} \quad (6.7)$$

with  $c$  being the total degree of each monomial.

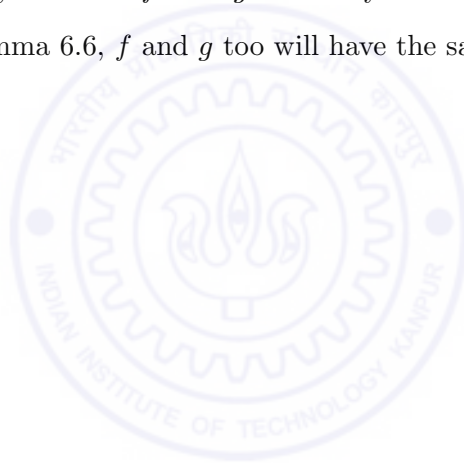
Now, we apply the map  $x \mapsto x$  and  $y \mapsto kx$  where  $k$  is chosen such that the polynomials do not vanish. So, the polynomials get transformed to:

$$f' = \left( \sum_{i=1}^n \alpha_i k^{b_i} \right) x^a \quad (6.8)$$

$$g' = \left( \sum_{i=1}^m \beta_i k^{d_i} \right) x^c. \quad (6.9)$$

The annihilating polynomial of  $f'$  and  $g'$  is clearly of the form  $(f')^c = \alpha(g')^a$ . Now, as a consequence of Lemma 6.6,  $f$  and  $g$  too will have the same annihilating polynomial.

□



## Chapter 7

# Higher Derivatives

In Chapter 3, we saw that checking linear independence of the first order derivatives of the input polynomials is not sufficient to test their algebraic independence over  $\mathbb{F}_p$ . Naturally, one could ask whether higher derivatives come to rescue in such cases. In this chapter, we give a higher derivatives based method which gives a criterion relating algebraic independence of polynomials to linear independence of their derivatives, similar to the Jacobian criterion. The operators we use are inspired by the Hasse-Schmidt derivatives which over positive characteristic are well behaved relative to the usual higher derivatives (see [Tra98]). With our proof technique, we first show the correctness of the Jacobian Criterion for separable extensions  $\mathbb{F}_2(x, y)/\mathbb{F}_2(f, g)$  in 7.2.1. Finally, using the operator defined in 7.1.1, we give an efficient independence testing criterion for the extensions of inseparable degree 2 over  $\mathbb{F}_2$  in 7.2.2.

### 7.1 Preliminaries

#### 7.1.1 Separability

We first give some basic definitions and properties of separable and inseparable extensions. For the proofs, one can refer to any standard textbook on field theory, for example: [Nag77].



**Definition 7.1.** (Separable Polynomial). A nonzero polynomial  $f(X) \in \mathbb{F}[X]$  is called separable when it has distinct roots in the algebraic closure of  $\mathbb{F}$ . That is, each root of  $f(X)$  has multiplicity 1. If  $f(X)$  has a multiple root then  $f(X)$  is called inseparable.

**Example 7.1.** In  $\mathbb{C}[X]$ , the polynomial  $X^2 - 4X$  is separable, since its roots are 0 and 4. In  $\mathbb{F}_3[X]$ , the polynomial  $X^3 - 2$  is inseparable since  $X^3 - 2 = X^3 + 1 = (X + 1)^3$ , implying that it has a multiple root at  $X = 1$ .

**Definition 7.2.** (Separable Element). An element  $\alpha$ , algebraic over  $\mathbb{F}$  is called separable over  $\mathbb{F}$  if its minimal polynomial in  $\mathbb{F}[X]$  is separable.

**Theorem 7.3.** For any field  $\mathbb{F}$ , an irreducible polynomial in  $\mathbb{F}[X]$  is separable if and only if it has a non-zero derivative.

**Corollary 7.4.** Every irreducible polynomial in  $\mathbb{F}[X]$  is separable, when  $\mathbb{F}$  has characteristic 0, whereas for  $\mathbb{F}$  with characteristic  $p$ , an irreducible polynomial in  $\mathbb{F}[X]$  is separable if and only if it is not a polynomial in  $X^p$ .

**Definition 7.5.** (Separable Extension). A finite extension  $\mathbb{E}/\mathbb{F}$  is called *separable* if every element of  $\mathbb{E}$  is separable over  $\mathbb{F}$ . When  $\mathbb{E}/\mathbb{F}$  is not separable, it is called *inseparable*.

More generally, a finite extension  $\mathbb{E}/\mathbb{F}$  is separable if it has a transcendence basis  $B \subset \mathbb{E}$  such that the finite extension  $\mathbb{E}/\mathbb{F}(B)$  is separable.

**Theorem 7.6.** Let  $\mathbb{E}/\mathbb{F}$  be a finite extension and write  $\mathbb{E} = \mathbb{F}(\alpha_1, \dots, \alpha_r)$ . Then,  $\mathbb{E}/\mathbb{F}$  is separable if and only if each  $\alpha_i$  is separable over  $\mathbb{F}$ .

**Proposition 7.7.** For a field  $\mathbb{F}$  of zero characteristic, the field extension  $\mathbb{F}(x, y)/\mathbb{F}(f, g)$  is always separable for algebraically independent polynomials  $f, g \in \mathbb{F}[x, y]$ .

*Proof.* We can write  $\mathbb{F}(x, y)$  as  $\mathbb{F}(f, g, x, y)$  or  $\mathbb{F}(f, g)(x, y)$  since  $\mathbb{F}(f, g) \subseteq \mathbb{F}(x, y)$ .

Now both  $x$  and  $y$  are algebraic over  $\mathbb{F}(f, g)$  since  $f$  and  $g$  are algebraically independent. Also by the definition, minimality implies irreducibility as well. So the minimal annihilating polynomials of  $x$  and  $y$  over  $\mathbb{F}(f, g)$  would be irreducible and hence separable (by Corollary 7.4). Thus, both  $x$  and  $y$  are separable over  $\mathbb{F}(f, g)$ . Finally, applying Theorem 7.6 on  $\mathbb{F}(f, g)(x, y)$  gives the desired result.  $\square$

More generally, it is true that every algebraic extension of a field of zero characteristic is separable.

**Definition 7.8.** (Inseparable degree) For an inseparable extension  $\mathbb{E}/\mathbb{F}$ , it is defined as the minimum  $d$  such that for every element  $\alpha \in \mathbb{E}$ ,  $\alpha^d$  is separable over  $\mathbb{F}$ .

**Proposition 7.9.** Over fields of characteristic  $p$ , the inseparable degree  $d$  of a field extension  $\mathbb{E}/\mathbb{F}$  is always of the form  $p^n$  for some  $n$ . We call  $n$  the inseparable index of the extension.

### 7.1.2 The Operator $\mathcal{H}_2$

We define the operators we would be using as

$$H_1(f) := df = \frac{\partial f}{\partial x}(dx) + \frac{\partial f}{\partial y}(dy), \quad \text{and} \quad (7.1)$$

$$H_2(f) := \frac{1}{2!} \frac{\partial^2 f}{\partial x^2}(dx)^2 + \frac{1}{2!} \frac{\partial^2 f}{\partial y^2}(dy)^2 + \frac{\partial^2 f}{\partial x \partial y}(dx \cdot dy). \quad (7.2)$$

We now define our main operator  $\mathcal{H}_2$  as:

$$\mathcal{H}_2(f) := H_1(f) + H_2(f). \quad (7.3)$$

**Proposition 7.10.**  $\mathcal{H}_2(f) = 0$  if and only if  $f \in \mathbb{F}_2[x^4, y^4]$ .

*Proof.* Clearly if  $f \in \mathbb{F}_2[x^4, y^4]$ , by (7.1), we get  $H_1(f) = 0$  and (7.2) gives  $H_2(f) = 0$ .

So, we have  $\mathcal{H}_2(f) = 0$ .

For the converse, note that  $\mathcal{H}_2(f) = 0$  implies that  $H_2(f) = 0$  which gives

$$\frac{1}{2!} \frac{\partial^2 f}{\partial x^2} = \frac{1}{2!} \frac{\partial^2 f}{\partial y^2} = \frac{\partial^2 f}{\partial x \partial y} = 0. \quad (7.4)$$

$\frac{1}{2!} \frac{\partial^2 f}{\partial x^2} = 0$  implies that every monomial in  $f$  has the exponent of  $x$  of the form  $4k$  or  $4k + 1$ . Similarly, for  $y$ , we get that every monomial in  $f$  has the exponent of  $y$  of the form  $4k$  or  $4k + 1$ . However,  $\frac{\partial^2 f}{\partial x \partial y} = 0$  implies that  $f \in \mathbb{F}_2[x^2, y^2]$ . The three conditions, together give that  $f \in \mathbb{F}_2[x^4, y^4]$ .  $\square$

**The Product Rule:**

It is easy to verify that the following product rules hold:

$$H_1(fg) = fH_1(g) + gH_1(f). \quad (7.5)$$

$$H_2(fg) = fH_2(g) + gH_2(f) + H_1(f)H_1(g). \quad (7.6)$$

$$\mathcal{H}_2(fg) = H_1(fg) + H_2(fg) = f\mathcal{H}_2(g) + g\mathcal{H}_2(f) + H_1(f)H_1(g). \quad (7.7)$$

Over  $\mathbb{F}_2$ , one can also verify the following:

$$\mathcal{H}_2(f^i) = if^{i-1}\mathcal{H}_2(f) + \frac{i(i-1)}{2}f^{i-2}(H_1(f))^2. \quad (7.8)$$

**7.2 Main Results**

We give an efficient criterion to test algebraic independence of two polynomials over  $\mathbb{F}_2$  when the inseparable degree of the field extension  $[\mathbb{F}(x, y) : \mathbb{F}(f, g)]_{insep} = 2$  i.e the inseparable index is 1.

As a warm up, we give the proof that the Jacobian criterion works when the field extension  $\mathbb{F}_2(x, y)/\mathbb{F}_2(f, g)$  is separable.

**7.2.1 Separable Extension: Jacobian Criterion**

**Theorem 7.11.** *Let  $f, g \in \mathbb{F}_2[x, y]$  be such, that the extension  $\mathbb{F}_2(f, g)/\mathbb{F}_2(x, y)$  is separable. Then  $f$  and  $g$  are algebraically dependent if and only if  $H_1(f) \wedge H_1(g) = 0$ .*

*Proof.*  $\Rightarrow$  If  $f$  and  $g$  are algebraically dependent, then there exists a minimal  $A \in \mathbb{F}_2[y_1, y_2]$  such that  $A(f, g) = 0 = \sum_{j,k} \alpha_{j,k} f^j g^k = 0$ . Applying  $H_1$  on the equation gives

$$d(A(f, g)) = \sum_{j,k} \alpha_{j,k} f^j \cdot k g^{k-1} d(g) + \sum_{j,k} \alpha_{j,k} g^k \cdot j f^{j-1} d(f) = 0. \quad (7.9)$$

Now because of the minimality of  $A$ , we  $\sum_{j,k} \alpha_{j,k} f^j \cdot k g^{k-1}$  cannot be zero unless all the  $k$ 's are even. But all the  $k$ 's and  $j$ 's cannot be both simultaneously even, else  $A$  becomes

a square contradicting the minimality. So, coefficient of at least one of  $H_1(f)$  and  $H_1(g)$  is non-zero in the above equation. So,  $H_1(f)$  and  $H_1(g)$  are linearly dependent over  $\mathbb{F}_2(x, y)$ . We define  $\mathcal{U}$  as the subspace generated by  $\mathbb{F}(x, y)\{H_1(f), H_1(g)\}$  over  $\mathbb{F}(x, y)$ . Thus we have  $\text{rank}\{\mathcal{U}\} < 2$  i.e.  $H_1(f) \wedge H_1(g) = 0$ . Degenerate cases also satisfy this since when one or both of  $H_1(f), H_1(g)$  is/are zero, we trivially get  $\text{rank}\{\mathcal{U}\}$  to be 1 and 0 respectively.

$\Leftarrow$  Let us say  $f$  and  $g$  are algebraically independent. Now, separability of the extension  $\mathbb{F}_2(x, y)/\mathbb{F}_2(f, g)$  implies that there exist minimal, separable  $A_1, A_2 \in \mathbb{F}_2[y_1, y_2, y_3]$  such that  $A_1(x, f, g) = 0$  and  $A_2(y, f, g) = 0$  satisfying  $\partial_{y_1} A_1, \partial_{y_1} A_2 \neq 0$ . We start with the equation

$$A_1(x, f, g) = \sum_{i,j,k} \alpha_{i,j,k} x^i f^j g^k = 0. \quad (7.10)$$

We apply the operator  $H_1$  as defined above on this equation to obtain

$$d(A_1(x, f, g)) = \sum_{i,j,k} \alpha_{i,j,k} \cdot i x^{i-1} \cdot dx \cdot f^j g^k + \sum_{i,j,k} \alpha_{i,j,k} x^i \cdot d(f^j g^k) = 0. \quad (7.11)$$

Note that separability implies the presence of atleast one odd  $i$  in  $A_1$ . So, we have atleast one non-zero term  $\sum_{i,j,k} \alpha_{i,j,k} \cdot i x^{i-1} \cdot dx \cdot f^j g^k$ . Now the overall sum too cannot be zero because of the minimality of  $A_1$ . Using this observation and the product rule on  $H_1(f^j g^k) = f^j \cdot k g^{k-1} H_1(g) + g^k \cdot j f^{j-1} H_1(f)$ , we deduce that

$$dx \in \mathcal{U}. \quad (7.12)$$

Similar operation on  $A_2$  gives

$$dy \in \mathcal{U}. \quad (7.13)$$

So, we have two linearly independent elements  $dx, dy \in \mathcal{U}$ . So  $\text{rank}\{\mathcal{U}\} = 2$  i.e.  $H_1(f) \wedge H_1(g) \neq 0$ .  $\square$

Now, we see a lemma which establishes that the failure of the Jacobian criterion is directly related to the inseparable nature of the field extension  $\mathbb{F}_p(f, g)/\mathbb{F}_p(x, y)$ .

**Lemma 7.12.** *For algebraically independent polynomials  $f, g \in \mathbb{F}_p[x, y]$ , the Jacobian criterion fails if the field extension  $\mathbb{F}_p(x, y)/\mathbb{F}_p(f, g)$  is inseparable.*

*Proof.* Since  $f$  and  $g$  are algebraically independent, the extension  $\mathbb{F}_p(x, y)/\mathbb{F}_p(f, g)$  is algebraic. So, there exist minimal polynomials for both  $x, y$  over  $\mathbb{F}_p(f, g)$ . Let us call them  $A_1$  and  $A_2$  respectively. Now, if the extension  $\mathbb{F}_p(x, y)/\mathbb{F}_p(f, g)$  is inseparable, by Theorem 7.6 at least one of  $x$  and  $y$  is inseparable over  $\mathbb{F}_p(f, g)$ . Let us assume that  $x$  is inseparable over  $\mathbb{F}_p(f, g)$ . Then by Corollary 7.4, the minimal annihilating polynomial,  $A_1$  of  $x$  over  $\mathbb{F}_p(f, g)$  is a polynomial in  $x^p$ . Thus, we have

$$A_1(x) = \sum \alpha_i(f, g)(x^p)^i = \sum \alpha_{i,j,k}(x^p)^i f^j g^k = 0 \quad (7.14)$$

where  $\alpha_i(f, g) \in \mathbb{F}_p(f, g)$ , and  $\alpha_{i,j,k} \in \mathbb{F}_p$ .

Applying  $H_1$  on the above equation, we get

$$d\left(\sum \alpha_{i,j,k}(x^p)^i f^j g^k\right) = \sum \alpha_{i,j,k}(x^p)^i \cdot d(f^j g^k) = 0. \quad (7.15)$$

This is similar to 7.9. By the arguments similar to the ones used there, we get  $H_1(f) \wedge H_1(g) = 0$  i.e.  $df \wedge dg = 0$ . Thus, the Jacobian criterion fails.  $\square$

We now use the operator  $\mathcal{H}_2$  to give a criterion which works in the inseparable index 1 case over  $\mathbb{F}_2$ .

### 7.2.2 Inseparable extension: inseparable index 1

Using Definition 7.8 and Proposition 7.9, we call the extension  $\mathbb{F}_2(f, g)/\mathbb{F}_2(x, y)$  to be of inseparable index 1 when the extension  $\mathbb{F}_2(f, g)/\mathbb{F}_2(x, y)$  is inseparable but the extension  $\mathbb{F}_2(f, g)/\mathbb{F}_2(x^2, y^2)$  is a separable one.

**Theorem 7.13.** *Let  $f, g \in \mathbb{F}_2[x, y]$  such that the extension  $\mathbb{F}_2(f, g)/\mathbb{F}_2(x, y)$  has inseparable index 1. Further let  $\mathcal{U}$  be the subspace generated by  $\{\mathcal{H}_2(f), \mathcal{H}_2(g), H_1(f)^2, H_1(g)^2\}$  over  $\mathbb{F}_2(x, y)$ . Then  $f$  and  $g$  are algebraically dependent if and only if  $\text{rank}\{\mathcal{U}\} < \min(r, 3)$  where  $r := \#$  non-zero elements in  $\{\mathcal{H}_2(f), \mathcal{H}_2(g), H_1(f)^2, H_1(g)^2\}$ .*

*Proof.*  $\Rightarrow$   $f$  and  $g$  are algebraically dependent:

If  $f$  and  $g$  are algebraically dependent, then there exists a minimal  $A$  such that  $A(f, g) = 0$ . We first apply  $H_1$  on the equation as in the previous theorem to get the same equation as (7.9) i.e.

$$H_1(A(f, g)) = \left( \sum_{j,k} \alpha_{j,k} g^k \cdot j f^{j-1} \right) \cdot H_1(f) + \left( \sum_{j,k} \alpha_{j,k} f^j \cdot k g^{k-1} \right) \cdot H_1(g) = 0. \quad (7.16)$$

We now apply the  $\mathcal{H}_2$  operator on the above equation to get

$$\sum_{j,k} \alpha_{j,k} \mathcal{H}_2(f^j g^k) = 0. \quad (7.17)$$

Applying the product rule, we get

$$\sum_{j,k} \alpha_{j,k} (f^j \mathcal{H}_2(g^k) + g^k \mathcal{H}_2(f^j) + H_1(f^j) \cdot H_1(g^k)) = 0. \quad (7.18)$$

which because of (7.7), becomes

$$\begin{aligned} & \sum_{j,k} \alpha_{j,k} g^k (j f^{j-1} \mathcal{H}_2(f) + \frac{j(j-1)}{2} f^{j-2} (H_1(f))^2) + \\ & \sum_{j,k} \alpha_{j,k} f^j (k g^{k-1} \mathcal{H}_2(g) + \frac{k(k-1)}{2} g^{k-2} (H_1(g))^2) + \\ & \sum_{j,k} \alpha_{j,k} j f^{j-1} k g^{k-1} H_1(f) H_1(g) = 0 \quad \text{or,} \end{aligned} \quad (7.19)$$

$$\begin{aligned} & \left( \sum_{j,k} \alpha_{j,k} j g^k f^{j-1} \right) \cdot \mathcal{H}_2(f) + \left( \sum_{j,k} \alpha_{j,k} \frac{j(j-1)}{2} f^{j-2} g^k \right) \cdot (H_1(f))^2 + \\ & \left( \sum_{j,k} \alpha_{j,k} k f^j g^{k-1} \right) \cdot \mathcal{H}_2(g) + \left( \sum_{j,k} \alpha_{j,k} \frac{k(k-1)}{2} g^{k-2} f^j \right) \cdot (H_1(g))^2 + \\ & \left( \sum_{j,k} \alpha_{j,k} j k f^{j-1} g^{k-1} \right) \cdot H_1(f) H_1(g) = 0. \end{aligned} \quad (7.20)$$

CASE 1:  $r = 4$ .

We observe that (7.12) implies linear dependence of  $H_1(f)^2, H_1(g)^2$  and  $H_1(f)H_1(g)$ . This reduces the basis of  $\mathcal{U}$  to  $\{\mathcal{H}_2(f), \mathcal{H}_2(g), H_1(f)^2\}$  and hence its rank 3. Further, note that coefficients of  $\mathcal{H}_2(g)$  and  $\mathcal{H}_2(f)$  in (7.20) cannot be both simultaneously zero as it contradicts the minimality of  $A$ . Thus (7.20) necessarily offers a non-trivial dependence

among the remaining basis elements of  $\mathcal{U}$  and we eventually get  $\text{rank}\{\mathcal{U}\} \leq 2$ .

CASE 2:  $r = 3$ .

Since by definition, zeroness of  $\mathcal{H}_2(f)$  also implies zeroness of  $H_1(f)$ ,  $r = 3$  corresponds to the case when exactly one of  $H_1(f), H_1(g)$  is zero. Let us say  $H_1(g) = 0$ . Again we are remained with three basis elements in  $\mathcal{U}$  i.e.  $\{\mathcal{H}_2(f), \mathcal{H}_2(g), H_1(f)^2\}$ . Now as argued in the previous case, (7.20) offers a non-trivial dependence among these, and we get  $\text{rank}\{\mathcal{U}\} \leq 2$ .

CASE 3:  $r = 2$ .

Here we have two cases:

Case 3a:  $H_1(f) = H_1(g) = 0$ .

The basis elements of  $\mathcal{U}$  get reduced to  $\{\mathcal{H}_2(f), \mathcal{H}_2(g)\}$ . Now (7.18) implies  $\text{rank}\{\mathcal{U}\} = 1$ .

Case 3b:  $\mathcal{H}_2(g) = H_1(g) = 0$  or the same case with  $f$  having the vanishing derivatives:  $\mathcal{H}_2(g) = 0$  implies that  $g$  is a fourth power. Thus Proposition 7.14 implies that we are no more in the case of inseparable index 1.

$\Leftarrow$   $f$  and  $g$  are algebraically independent:

inseparable index 1 implies that there exist minimal, separable  $A_1, A_2 \in \mathbb{F}_2[y_1, y_2, y_3]$  such that  $A_1(x^2, f, g) = A_2(y^2, f, g) = 0$ . We apply the operator  $\mathcal{H}_2$  on  $A_1$  to get

$$\mathcal{H}_2(A(x^2, f, g)) = \sum_{i,j,k} \mathcal{H}_2(\alpha_{i,j,k} x^{2i} f^j g^k) = 0. \quad (7.21)$$

The product rule of  $\mathcal{H}_2$  gives

$$\sum_{i,j,k} \alpha_{i,j,k} (f^j g^k \cdot \mathcal{H}_2(x^{2i}) + x^{2i} \mathcal{H}_2(f^j g^k) + H_1(x^{2i}) H_1(f^j g^k)) = 0. \quad (7.22)$$

Now  $H_1(x^{2i}) = 0$  and  $\mathcal{H}_2(x^{2i}) = i(2i - 1)x^{2i-1}(dx)^2$ . Using these, the above equation becomes

$$\sum_{i,j,k} i(2i - 1)x^{2i-2} f^j g^k (dx)^2 + \sum_{i,j,k} \alpha_{i,j,k} x^{2i} \mathcal{H}_2(f^j g^k) = 0. \quad (7.23)$$

Now we use the similar argument as in the case of previous theorem i.e. inseparable index 1 implies the presence of atleast one odd  $i$  in  $A_1$ . So, we have atleast one non-zero term  $\sum_{i,j,k} i(2i - 1)x^{2i-2} f^j g^k$ . Now the overall sum too cannot be zero because of the minimality of  $A_1$ . Using this observation and the product rule on  $\mathcal{H}_2(f^j g^k)$  as given by

(7.18) and (7.19), we deduce that

$$(dx)^2 \in \mathcal{U}. \quad (7.24)$$

Similar operation on  $A_2$  gives

$$(dy)^2 \in \mathcal{U}. \quad (7.25)$$

So we have  $\text{rank}\{\mathcal{U}\} \geq 2$ .

So for  $r = 2$ , independence implies  $\text{rank}\{\mathcal{U}\} = 2$ .

Note that from the definition, it follows that  $\mathcal{H}_2(f), \mathcal{H}_2(g), H_1(f)^2, H_1(g)^2$  can all be written as linear combinations of  $dx, dy, (dx)^2, (dy)^2, (dx \cdot dy)$  over  $\mathbb{F}_2(x, y)$ . Now given that  $(dx)^2, (dy)^2$  are already in  $\{\mathcal{U}\}$ , a non-zero coefficient corresponding to  $dx, dy$  or  $(dx \cdot dy)$  in the expansion of any of  $\mathcal{H}_2(f), \mathcal{H}_2(g), H_1(f)^2, H_1(g)^2$  gives  $\text{rank}\{\mathcal{U}\} = 3$ .

Thus independence implies  $\text{rank}\{\mathcal{U}\} = 3$  for  $r = 3$  and  $r = 4$  case. Observe that zero coefficients corresponding to each of  $dx, dy$  or  $(dx \cdot dy)$  imply  $H_1(f) = H_1(g) = 0$ , i.e.  $r = 2$  case.  $\square$

**Proposition 7.14.** *If one or both of  $\mathcal{H}_2(f), \mathcal{H}_2(g)$  is zero, then the inseparable index of the extension  $\mathbb{F}_2(x, y)/\mathbb{F}_2(f, g) > 1$ .*

*Proof.* For the sake of contradiction, let us assume that the inseparable index of the extension  $\mathbb{F}_2(x, y)/\mathbb{F}_2(f, g) \leq 1$ . Thus, the minimal polynomials of  $x^2$  and  $y^2$  over  $\mathbb{F}_2(f, g)$  must be separable. So, we also have separable polynomials  $A_1, A_2 \in \mathbb{F}_2[y_1, y_2, y_3]$  such that  $A_1(x^2, f, g) = A_2(y^2, f, g) = 0$ . Also, let us assume that  $\mathcal{H}_2(f) = 0$ .

Now, we first apply  $\mathcal{H}_2(f)$  on the evaluated  $A_1$  to get (using 7.23 and 7.20) that  $(dx)^2$  lives in the span of  $\{\mathcal{H}_2(f), \mathcal{H}_2(g), (H_1(f))^2, (H_1(g))^2\}$ . But since  $\mathcal{H}_2(f) = 0$ , we get that  $(dx)^2$  lives in the span of  $\{\mathcal{H}_2(g), (H_1(g))^2\}$ . Recalling that  $\mathcal{H}_2(g) = H_1(g) + H_2(g)$ , and that  $(H_1(g))^2$  does not have any first order  $(dx, dy)$  term, we get that  $H_1(g) = 0$ . So, we get that  $(dx)^2$  lives in the span of  $H_2(g)$ .

Similar operations on  $A_2$  gives that  $(dy)^2$  also lives in the span of  $H_2(g)$ . But both  $(dx)^2$  and  $(dy)^2$  cannot be spanned by a single element  $H_2(g)$ . Thus, we arrive at a contradiction.  $\square$



## Chapter 8

# Conclusions and Future

## Directions

### 8.1 Summary/Conclusion

We pursue four major approaches to find an algorithm to test algebraic independence of polynomials over finite fields.

- First is correcting the Jacobian by applying faithful transformations on the polynomials. This approach could provide efficient algorithms in some special cases. However stronger techniques are required to generalize it to solve more cases.
- Second approach is lifting the polynomials to increase the  $p$ -adic valuation of the Jacobian. This offers a new criterion for testing independence. It is not very clear if whether it also gives an efficient algorithm since there is limited work done on finding rational function solutions to differential equations.
- The third approach uses Lüroth's theorem to relate the problem of algebraic independence to the problem of polynomial decomposition. We have shown using the results on sparse polynomial decomposition that this connection helps in resolving algebraic independence for supersparse case. The result obtained is for fields

of zero characteristic which we believe can also be extended to fields of positive characteristic.

- The fourth approach is to come up with a higher-derivatives based Jacobian like criterion. We give a randomised polynomial time algorithm problem of testing algebraic independence of two circuits over  $\mathbb{F}_p$  with inseparable degree 2.

## 8.2 Future Directions

Based on our work, we propose the following directions of work to pursue in order to get efficient algorithms for testing algebraic independence over fields of positive characteristic:

- Generalizing the algorithm for two binomials to two trinomials and beyond.
- Generalizing the algorithm for two sum of univariates to constantly many sum of univariates.
- Exploring algorithms to test the existence of rational function solution to differential equations modulo a prime or over rationals. Solving special cases would resolve special cases of algebraic independence as well.
- Extending Zannier's degree bound result on sparse decomposition over fields of zero characteristic to fields of positive characteristic as well.
- Extending the Higher Derivatives based algorithm to get a randomized polynomial time algorithm for  $n$  arithmetic circuits.

# Bibliography

- [ASSS12] Manindra Agrawal, Chandan Saha, Ramprasad Saptharishi, and Nitin Saxena. Jacobian hits circuits: Hitting-sets, lower bounds for depth-D occur-k formulas & depth-3 transcendence degree-k circuits. In *Proceedings of the forty-fourth annual ACM symposium on Theory of computing*, pages 599–614. ACM, 2012.
- [Ax71] James Ax. On Schanuel’s conjectures. *Annals of Mathematics*, 93(2):pp. 252–268, 1971.
- [BCW05] Moulay A. Barkatou, Thomas Cluzeau, and Jacques-Arthur Weil. *Factoring partial differential systems in positive characteristic*, pages 213–238. Trends in Mathematics. Birkhäuser Basel, 2005.
- [Ben04] Michaël Bensimhoun. Another elementary proof of Lüroth’s theorem. May 2004.
- [BMS13] Malte Beecken, Johannes Mittmann, and Nitin Saxena. Algebraic independence and blackbox identity testing. *Inf. Comput.*, 222:2–19, 2013.
- [BT04] E.B. Burger and R. Tubbs. *Making transcendence transparent: An intuitive approach to classical transcendental number theory*. Springer, 2004.
- [Can92] Georg Cantor. Über eine elementare frage der mannigfaltigkeitslehre. *Jahresbericht der Deutschen Mathematiker-Vereinigung*, 1:75–78, 1892.
- [Chè10] Guillaume Chèze. Nearly optimal algorithms for the decomposition of multivariate rational functions and the extended Lüroth theorem. *Journal of Complexity*, 26(4):344–363, 2010.

- [DF93] E Delaleau and M Fliess. An algebraic interpretation of the structure algorithm with an application to feedback decoupling. In *IFAC SYMPOSIA SERIES*, pages 179–179. PERGAMON PRESS, 1993.
- [DGW09] Zeev Dvir, Ariel Gabizon, and Avi Wigderson. Extractors and rank extractors for polynomial sources. *Computational Complexity*, 18(1):1–58, 2009.
- [Duv10] D. Duverney. *Number theory: An elementary introduction through Diophantine problems*. Monographs in number theory. World Scientific, 2010.
- [Dvi12] Zeev Dvir. Extractors for varieties. *computational complexity*, 21(4):515–572, 2012.
- [For92] Krister Forsman. Two themes in commutative algebra: Algebraic dependence and Kähler differentials. 1992.
- [Gel34] A. Gelfond. Sur le septième problème de Hilbert. *Bull. Acad. Sci. URSS*, 1934(4):623–630, 1934.
- [Her74] Charles Hermite. Sur la fonction exponentielle. 1874.
- [Kal85] KA Kalorkoti. A lower bound for the formula size of rational functions. *SIAM Journal on Computing*, 14(3):678–687, 1985.
- [Kal88] Erich Kaltofen. Greatest common divisors of polynomials given by straight-line programs. *J. ACM*, 35:231–264, 1988.
- [Kay09] Neeraj Kayal. The complexity of the annihilating polynomial. In *Computational Complexity, 2009. CCC'09. 24th Annual IEEE Conference on*, pages 184–193. IEEE, 2009.
- [KK05] Erich Kaltofen and Pascal Koiran. On the complexity of factoring bivariate supersparse (lacunary) polynomials. In *Proceedings of the 2005 International Symposium on Symbolic and Algebraic Computation, ISSAC '05*, pages 208–215, New York, NY, USA, 2005. ACM.
- [KR08] Martin Kreuzer and Lorenzo Robbiano. *Computational commutative algebra 1*. Springer Publishing Company, Incorporated, 2008.

- [Lam98] JH Lambert. Mémoire sur quelques propriétés remarquables des quantités transcendentes circulaires et logarithmiques, Histoire de l'Académie de Berlin 1761 (publ. 1768), S. 265–322. *Vgl. hierzu Alfred Pringsheim, Über die ersten Beweise der Irrationalität von  $\pi$ , Sitzungsber. d. math.-phys. Kl. der bayer. Akad. d. Wiss.*, 28:325–337, 1898.
- [Lan66] S. Lang. *Introduction to transcendental numbers*. Addison-Wesley series in mathematics. Addison-Wesley Pub. Co., 1966.
- [Lin82] F. Lindemann. Ueber die Zahl  $\pi$ . *Mathematische Annalen*, 20(2):213–225, 1882.
- [L'v84] MS L'vov. Calculation of invariants of programs interpreted over an integrality domain. *Cybernetics and Systems Analysis*, 20(4):492–499, 1984.
- [Mil03] James S Milne. *Fields and Galois theory*. 2003.
- [Mit13] Johannes Mittmann. *Independence in algebraic complexity theory*. PhD thesis, Universitäts- und Landesbibliothek Bonn, 2013.
- [Mor51] L. J. Mordell. *The Mathematical Gazette*, 35(311):pp. 56–58, 1951.
- [MSS12] Johannes Mittmann, Nitin Saxena, and Peter Scheiblechner. Algebraic independence in positive characteristic—A  $p$ -Adic Calculus. *arXiv preprint arXiv:1202.4301*, 2012.
- [Nag77] Masayoshi Nagata. *Field theory*. 1977.
- [NoFRS09] Yu. V. Nesterenko, Tata Institute of Fundamental Research, and American Mathematical Society. *Algebraic independence*. Tata Institute of Fundamental Research lectures on mathematics. Narosa Publishing House, 2009.
- [Per27] O. Perron. *Algebra: die Grundlagen*. Number v. 1 in Göschens Lehrbücherei: Reine und angewandte Mathematik. de Gruyter, 1927.
- [Per32] Oskar Perron. *Algebra: Die Grundlagen*, volume 8. 1932.

- [Pło05] Arkadiusz Płoski. Algebraic dependence of polynomials after O. Perron and some applications. *Computational Commutative and Non-Commutative Algebraic Geometry*, pages 167–173, 2005.
- [Rot55] K. F. Roth. Rational approximations to algebraic numbers. *Mathematika*, 2:1–20, 6 1955.
- [Sax09] Nitin Saxena. Progress on polynomial identity testing. 2009.
- [Sch34] Theodor Schneider. Transzendenzuntersuchungen periodischer Funktionen. 2. *Journal für die reine und angewandte Mathematik*, pages 65–74, 1934.
- [Sch00] A. Schinzel. *Polynomials with special regard to reducibility*. Cambridge University Press, 2000. Cambridge Books Online.
- [Sie14] Carl L. Siegel. Über einige anwendungen diophantischer approximationen. In Umberto Zannier, editor, *On some applications of Diophantine approximations*, volume 2 of *Publications of the Scuola Normale Superiore*, pages 81–138. Scuola Normale Superiore, 2014.
- [Sin15] Amit Kumar Sinhababu. Testing algebraic independence of polynomials over finite fields. Master’s thesis, Indian Institute of Technology, Kanpur, 2015.
- [ŠKB89] A.B. Šidlovskii, N. Koblitz, and W.D. Brownawell. *Transcendental numbers*. De Gruyter studies in mathematics. Walter de Gruyter, 1989.
- [Ste10] E. Steinitz. Algebraische theorie der körper. *J. Reine Angew. Math.*, 137:167–309, 1910.
- [Tra98] William Nathaniel Traves. Differential operators and Nakai’s conjecture. 1998.
- [Wei04] K. Weierstrass. Zu Lindemann’s abhandlung: ”Über die Ludolph’sche zahl”. In *Pi: A Source Book*, pages 207–225. Springer New York, 2004.
- [Zan07] Umberto Zannier. On the number of terms of a composite polynomial. *Acta Arithmetica*, 127:157–167, 2007.