Testing Algebraic Independence Of Polynomials Over Finite Fields

A thesis submitted
in partial fulfillment of the requirements
for the degree of
Master of Technology

by

Amit Kumar Sinhababu
Roll No: 12111010

under the guidance of

Dr. Manindra Agrawal

Department of Computer Science and Engineering

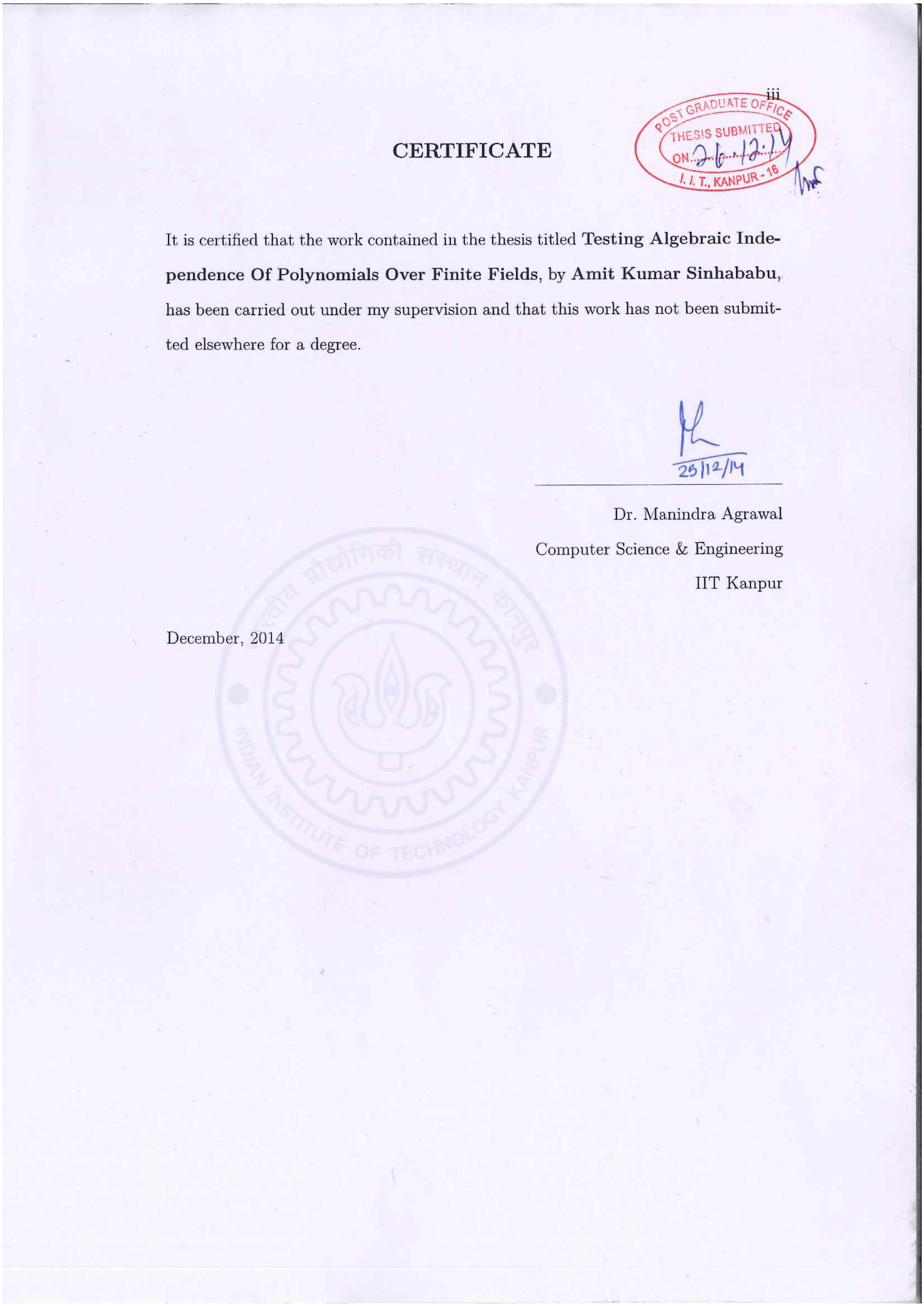
Indian Institute of Technology Kanpur

December, 2014

Abstract

We consider the problem of testing algebraic independence of a set of polynomials over finite fields of small characteristic. Algebraic independence of polynomials is a nonlinear generalization of linear independence of polynomials. Over fields of zero characteristic, a set of polynomials is algebraically independent if and only if the Jacobian matrix of the polynomials has full rank, and this can be tested in randomized polynomial time. But over fields of small characteristic, Jacobian criterion does not work and designing an efficient criterion to test algebraic independence is an open problem till now. In this thesis, we explore new approaches towards finding such a criterion.
Over fields of small characteristic, if Jacobian of a set of polynomials is nonzero, then we conclude that they are algebraically independent. If the Jacobian is zero, the polynomials need not be algebraically dependent. We try to transform the algebraically independent polynomials for which the Jacobian is zero such that the Jacobian of the transformed polynomials is nonzero. Using this approach, we solve the special case of efficiently testing algebraic independence of two bivariate binomials over $\mathbb{F}_p$.

Pursuing a different approach, we come up with a new characterization of algebraic independence over $\mathbb{F}_p$. We lift the polynomials by adding polynomials whose coefficients are multiples of p. We prove that if the two polynomials are algebraically dependent, then the p-adic valuation of the Jacobian of these polynomials can be arbitrarily increased by suitable lifting of the polynomials, but if the polynomials are algebraically independent then the p-adic valuation of the Jacobian cannot be increased by lifting beyond a fixed bound. One part of the proof uses Witt Jacobian [MSS12] criterion, the other part uses the observation that the annihilating polynomial's p-adic valuation can be arbitrarily increased by lifting the polynomials.



CERTIFICATE

It is certified that the work contained in the thesis titled **Testing Algebraic Independence Of Polynomials Over Finite Fields**, by **Amit Kumar Sinhababu**, has been carried out under my supervision and that this work has not been submitted elsewhere for a degree.

25/12/14

Dr. Manindra Agrawal
Computer Science & Engineering
IIT Kanpur

December, 2014

Dedicated to my Brother and my Parents.

Acknowledgements

I am greatly indebted to my advisor Prof. Manindra Agrawal, for his guidance and teaching, for his generous help and encouragement in difficult times. I consider myself fortunate to work under his guidance and he will always remain as a source of great inspiration. I am equally indebted to Dr. Nitin Saxena for his valuable guidance and constant support. His wealth of knowledge and enthusiasm for solving problems with students is greatly motivating. Special thanks to my friend and co-worker Anurag Pandey. Some of the results presented in this thesis came from joint work with him. Special thanks to Rohit Gurjar and Arpita Korwar, for patiently answering many doubts. I owe a lot to Prof. Sumit Ganguly, Prof. Piyush Kurur, Prof. Anil Seth, Prof. Raghunath Tewari as their teaching helped me to get understanding of various subjects in theoretical computer science. I want to take this opportunity to express my gratitude to the Computer Science and Engineering Department at IIT Kanpur for fostering a creative academic environment.

Amit Sinhababu

Contents

Chapter 1

Introduction

1.1 Motivation

The concept of algebraic dependence of polynomials is a nonlinear generalization of the concept of linear dependence of polynomials. Linear dependence of polynomials can only capture linear relationship among the polynomials, whereas algebraic dependence of polynomials can capture even nonlinear or higher degree relationship among the polynomials. Algebraic independence is a fundamental notion in mathematics, an important tool in commutative algebra and algebraic geometry. It has several applications in computer science, in polynomial identity testing algorithms [BMS13, ASSS12], proving formula lower bound for determinant [Kal85], construction of deterministic randomness extractors for polynomial sources [DGW09], computing program invariants of arithmetic straight line programs [L'v84].

Deciding whether a given set of polynomials are algebraically dependent or not and computing the relationship of the dependent polynomials are two natural computational problems. It is known that, although computing the dependency relationship of algebraically dependent polynomials is computationally hard, checking whether the polynomials are algebraically dependent or not can be done efficiently, in randomized polynomial time if the polynomials are over fields of characteristic zero (like the field $\mathbb{Q}$), or has large enough characteristic (compared to the product of the degrees of the input polynomials).

In this case, testing algebraic independence of polynomials reduces to computing the rank of the Jacobian matrix of $f_1, \ldots, f_m \in k[x_1, \ldots, x_n]$. If the Jacobian is of full rank, the polynomials are independent, otherwise the polynomials are dependent. Even if the polynomials are succinctly encoded as arithmetic circuits, using [BS83] we can efficiently construct the circuits computing partial derivatives. Now we can plug in random constants from the field in place of the variables and compute the rank of the Jacobian Matrix. Using Schwartz-Zippel lemma, we can show that, with high probability, the rank of the this matrix (with random values plugged in) equals the rank of the Jacobian with polynomial entries. So in this case, testing algebraic independence reduces to (the complement of) Polynomial Identity Testing (PIT) and can be done in randomized polynomial time (in terms of bit-size of the input).

Whereas the case of zero or large characteristic has efficient solution, the scenario is different if the polynomials are over finite fields of small positive characteristic. In this case, the Jacobian criterion fails. If we get nonzero Jacobian over $\mathbb{F}_p$, we can surely conclude that the given polynomials are algebraically independent over $\mathbb{F}_p$. If we get zero Jacobian, the polynomials need not be dependent, they can be independent as well. For example, let us take the polynomials x^p, y^p over the field $\mathbb{F}_p$. Their Jacobian with respect to x, y is zero, but clearly they are algebraically independent.

1.2 Problems

The absence of a criterion analogous to Jacobian leads to the following interesting question.

Problem 1.1 (Algebraic Independence Testing over $\mathbb{F}_p$)**.** *Given a set of m (n-variate) polynomials (encoded as Arithmetic Circuits) over $\mathbb{F}_p$, decide whether they are Algebraically Independent or not. Can we decide this in randomized polynomial time?*

We identify a few special cases of this general problem, which should be easier, but all these cases are nontrivial in the sense that current methods cannot decide independence over $\mathbb{F}_p$ efficiently (in randomized or deterministic polynomial time) even for these cases. In our thesis, we mainly focus on the following three special cases.

- We have two bivariate polynomials of high degree (exponential in terms of bit size) with constantly many monomials.
- We have two bivariate polynomials, both are supersparse or lacunary (sparse polynomials with exponential degree).
- We have two arithmetic circuits of bivariate polynomials.

1.3 Previous Work

[DGW09] asked whether algebraic independence testing of polynomials over $\mathbb{F}_p$ is in **RP**. [Kay09, ASSS12] also mentioned this as an open problem. [MSS12] gave a generalization of Jacobian, named Witt Jacobian which works for polynomials over $\mathbb{F}_p$. They improved the complexity of the independence testing over $\mathbb{F}_p$ from **PSPACE** to $\mathbf{NP}^{\#\mathbf{P}}$. So, in terms of complexity, there is a huge gap between the best known upper bound $\mathbf{NP}^{\#\mathbf{P}}$ and **RP**.

1.4 Contribution of the thesis

In this thesis, we explore new directions to this problem. The first approach we try is transforming the input polynomials (preserving their transcendence degree) so that Jacobian works correctly for the transformed polynomials, although Jacobian was wrongly zero for the original polynomials. The following example illustrates the idea: Let us take the polynomials x^p, y^p over the field $\mathbb{F}_p$. By taking p^{th} root, we transform these two polynomials into x and y. This transformation preserves the transcendence degree of the original set of polynomials. Now we get nonzero Jacobian (of x and y) and conclude that x^p and y^p are independent. We give evidence that Jacobian can be corrected even when the polynomials are not prime powered using natural transformations like applying polynomial map. We come up with a monomial map correcting Jacobian of algebraically independent monomials. Using these ideas, we resolve a special case of two exponential degree bivariate binomials, where direct application of known techniques do not give efficient solution. Pursuing a different approach, we give a new characterization of algebraic independence over finite fields. We prove that p-adic valuation of the

Jacobian of two polynomials can be arbitrarily increased if and only if the two polynomials are algebraically dependent.

1.5 Organization of the thesis

In chapter two, we describe the preliminary concepts and survey some of the key results. In chapter three and four, we present the main results of the thesis. In chapter five, we conclude, giving a summary and directions to future work.

Chapter 2

Background

2.1 Basic Definitions

We begin with the definition of algebraic independence of polynomials.

Definition 2.1 (Algebraic Independence)**.** Polynomials $f_1, \ldots, f_m \in k[x_1, \ldots, x_n]$ are called *algebraically independent* over a field k, if there is no nonzero m-variate polynomial $A \in k[y_1, \ldots, y_m]$ such that $A(f_1, \ldots, f_m) = 0$. If such a nonzero polynomial A exists, $f_1, \ldots, f_m$ are called *algebraically dependent* and the polynomial A is called an *annihilating* polynomial.

Examples: $f_1 = x + y$ and $f_2 = x^2 + 2xy + y^2$ are two algebraically dependent polynomials. Their annihilating polynomial is $f_1^2 - f_2$.
$f_1 = x$ and $f_2 = y$ over $F[x, y]$ are two algebraically independent polynomials. The general definition of algebraic dependence comes from field theory[Coh03]. Given any field extension F/k (where F is an extension of k), let $p_1, \ldots, p_m, q \in F$. Now, q is *algebraically dependent* on $p_1, \ldots p_m$ over k if q is *algebraic* over the field $k(p_1, \ldots, p_m)$ that is if q satisfies an equation with coefficients in $k(p_1, \ldots, p_m)$. If we multiply the equation by a common denominator, we get the equation for q as $a_0 q^d + a_1 q^{d-1} + \ldots + a_d = 0$ where a_0 is not zero and $a_i \in k[p_1, \ldots, p_m]$.

Now, a subset X of F is algebraically independent over k if no element of X is algebraically dependent on the rest of the elements in X. Otherwise, it is algebraically dependent.

Definition 2.2 (Transcendence Basis)**.** A subset B of F which is algebraically independent and every element of F is algebraically dependent on B over k is called a *transcendence basis* or *transcendence base* of F over k.

Example: If $K = k(x, y)$, $\{x^2, y^2\}$ is a transcendence basis for K. We note that, $k(x^2, y^2) \neq k(x, y)$.

Definition 2.3 (Algebraic Extension)**.** A field extension F/k is *algebraic* if every element of F is algebraic over k.

Example: All finite extensions are algebraic but the converse is not true. For example, field of all algebraic numbers is an infinite algebraic extension of field of rational numbers. An extension which is not algebraic is called a *transcendental extension.*

Definition 2.4 (Purely Transcendental Extension)**.** A field extension F/k is *purely transcendental* if there is an algebraically independent subset X of F such that $F = k(X)$.

Example: $k(x_1, ..., x_n)/k$

2.2 Properties of Algebraic Independence

2.2.0.1 Combinatorial Properties

It is evident from the definition of algebraic dependence that it is a generalization of linear dependence. If some polynomials are linearly dependent then obviously they are algebraically dependent. But the converse is not true, unless the polynomials are all linear. Analogous to linear dependence, algebraic dependence satisfies the defining properties of Matroid, a combinatorial structure unifying and generalizing the abstraction of dependence.[VdWAN31] Here, we prove two common properties of algebraic independence and linear independence.

- If $f_1, \ldots, f_m$ are algebraically independent polynomials, any subset of them are also algebraically independent.

Proof. Let us assume a subset S of the polynomials $f_i, \dots, f_j$ which are algebraically dependent and there is a nonzero A such that $A(f_i, \dots, f_j) = 0$. Now, the same annihilating polynomial annihilates $f_1, \dots f_m$ because if $f_k \notin S$ we can have $c_k.f_k$ as a term in the annihilating polynomial where $c_k = 0$. □

- If a polynomial f is algebraically dependent on $g_1, \dots, g_m$ but not on $g_1, \dots, g_{m-1}$, then g_m is algebraically dependent on $f, g_1, \dots, g_{m-1}$.

Proof. Let us write the annihilating polynomial of $f, g_1, \dots, g_m$ as a polynomial in g_m: $a_0{g_m}^d + a_1{g_m}^{d-1} + \dots + a_d = 0$, here $a_i \in k[f, g_1, \dots, g_{m-1}]$. Now, if $a_0, a_1, \dots a_{d-1}$ are all zero, then a_d equals to 0. Now, $a_d = 0$ implies that there is a nonzero polynomial relation between $f, g_1, \dots, g_{m-1}$ contradicting the hypothesis that they were independent. So, $a_0, a_1, \dots, a_{d-1}$ are not all 0. From the equation, we get g_m is algebraically dependent on $f, g_1, \dots, g_{m-1}$ □

Definition 2.5 (Transcendence Degree)**.** Maximal number of algebraically independent polynomials in a set of polynomials is known as the transcendence degree of the polynomials. Transcendence degree of a field extension, written as $tr.deg(F/k)$ is the cardinality of its transcendence base.

Using the exchange property of matroid, it can be proved that all transcendence bases have same degree. So, transcendence degree is well defined.

Algebraic extensions have transcendence degree zero.

Transcendence degree of $k(x_1, \dots, x_n)/k = n$ as $x_1, \dots, x_n$ forms transcendence basis.

We present the analogy between algebraic independence and linear independence in the following table.

Linear Independence	Algebraic Independence
Basis	Transcendence Basis
Dimension	Transcendence Degree
S Spans L	L is algebraic over $k(S)$

We mention here two basic facts. The proofs of these facts can be found in most textbooks on algebra and fields. [Coh03]

- Transitivity Property of algebraic dependence:

  If f is algebraically dependent on $g_1, \ldots, g_n$, and each g_i is algebraically dependent on $h_1, \ldots h_m$, then f is algebraically dependent on $h_1, \ldots, h_m$

- tr.deg(F/k)=tr.deg(F/E)+tr.deg(E/k)

2.2.1 Algebraic properties

The set of all annihilating polynomials of $f_1, \ldots, f_n$ forms an ideal of the polynomial ring $k[y_1, \ldots, y_n]$.

Lemma 2.6. *[Kay09] Let $f_1, \ldots, f_m \in F[x_1, \ldots, x_n]$ be a set of algebraically dependent polynomials over field F, such that no proper subset of them is algebraically dependent, equivalently the transcendence degree of the polynomials is $n-1$. Then the ideal of the annihilating polynomials is generated by a unique irreducible (up to constant) polynomial A. So in this case, the ideal of the annihilating polynomials is a principal ideal.*

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

$$A(y_1, \ldots, y_m) = A_1(y_1, \ldots, y_m) \cdot A_2(y_1, \ldots, y_m).$$

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

Now, the uniqueness of the minimal irreducible annihilating polynomial can be proved using properties of resultant. Let $B(y_1, \ldots, y_m)$ be another irreducible annihilating polynomial of $f_1, \ldots, f_m$. We have to prove $A = c{\cdot}B$ for some constant c. As, no proper subset of $f_1, \ldots, f_m$ are algebraically dependent, $f_2, \ldots, f_m$ are not algebraically dependent. So, both A and B has y_1. Now, let

$$p(y_2, \ldots, y_m) = RESULTANT_{y_1}(A(y_1, \ldots, y_m), B(y_1, \ldots, y_m)).$$

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

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

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

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

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

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

Now, resultant of A and B is zero implies that A and B share a common factor. As A is irreducible, this implies $A = c \cdot B$.

Remark 2.7. This lemma can be sometimes useful in testing algebraic independence in the following way. Let us suppose that the $f(x, y)$ and $g(x, y)$ are two algebraically dependent polynomials and $A(f(x, y), g(x, y))$ is an annihilating polynomial of them. Now, we substitute y with a constant c from the base field (or suitable field extension of the base field), such that none of $f(x, c), g(x, c)$ becomes constant. If no such substitution is possible, then we keep y as it is and replace x by a constant c. Let U be the ideal of annihilating polynomials of $f(x, y), g(x, y)$ and V be the ideal of annihilating polynomials of $f(x, c), g(x, c)$. As none of f, g is constant, the ideal U is a principal ideal. Now, if $A(f(x, y), g(x, y)) = 0$, then $A(f(x, c), g(x, c) = 0$. As the transcendence degree of $f(x, c), g(x, c)$ is 1, V is also a principal ideal, generated by a single absolutely irreducible polynomial. This implies, $U = V$. We use this idea to test algebraic independence in this special case. Let us assume, polynomials f and g are of the form such that $f_1 = f(0, c) = c_1 y^a$ and $f_2 = g(0, c) = c_2 y^b$. In this case if f and g are dependent, their minimal annihilating polynomial would be just the minimal annihilating polynomial of y^a and y^b. Let us suppose, minimal annihilating polynomial of f_1, f_2 is $f_1^d = f_2^e$. So, in this case, f and g are algebraically independent if and only if $f^d = g^e$.

□

The following lemma is very useful, it says if number of polynomials is more than number of variables in the polynomials, then those polynomials are always algebraically dependent.

Lemma 2.8. *[For92] The polynomials $f_1, \ldots, f_m \in k[x_1, \ldots, x_n]$ are algebraically dependent over k if $m > n$.*

Proof. We prove this by contradiction. Let us assume $f_1, \ldots, f_m$ are algebraically independent. Then, $f_1, \ldots, f_m$ forms a transcendence basis for $k(x_1, \ldots, x_n)$. Now, $Tr.degk(x_1, \ldots, x_n)/k = n$ as $x_1, \ldots, x_n$ forms a transcendence basis. But $m > n$. As we know that any two transcendence bases for K/k have the same cardinality, we get a contradiction. □

2.3 Computing the Annihilating Polynomial

2.3.1 Degree bound of Annihilating Polynomial

Let $f_1, \ldots, f_m \in k[x_1, \ldots, x_n]$ be polynomials of degree at most $\delta \geq 1$ and r is the transcendence degree of $f_1, \ldots, f_m$. If the polynomials are algebraically dependent, then there exists a non zero annihilating polynomial $A \in k[y_1, \ldots, y_m]$ such that degree of $A \leq \delta^r$. [Mit13] contains detailed proof of this degree upper bound. This bound is tight, there are algebraically dependent polynomials whose minimal annihilating polynomial's degree matches this bound.[Mit13]. $x_1, x_2 - {x_1}^d, x_3 - {x_2}^d, \ldots, x_n - {x_{n-1}}^d, x_n^d$ has transcendence degree n and it's minimal annihilating polynomial has degree d^n

The upper bound on the degree of annihilating polynomial gives a simple but inefficient method to compute the annihilating polynomial or test if they are algebraically independent. If $f_1, \ldots, f_m \in K[x_1, \ldots, x_n]$ are polynomials of degree at most $\delta \geq 1$, then $f_1, \ldots, f_m \in K[x_1, \ldots, x_n]$ are algebraically independent over k if and only if $\{f_1^{d_1} \cdot f_2^{d_2} \cdots f_m^{d_m} | \sum_{i=1}^{m} d_i \leq \delta^m\}$ is K-linearly independent. This exponential sized system of linear equations can be solved in **PSPACE**. In case of constantly many sparse polynomials with low (polynomially bounded) degree, as the degree bound of the annihilating polynomial is polynomial, we can test algebraic independence in polynomial time. But for constantly many polynomials with high (exponential) degree, the degree bound is exponential.

2.3.2 Hardness of computing Annihilating Polynomial

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

2.3.3 Special cases of algebraic dependence

2.3.3.1 Linear polynomials

If all the polynomials are linear, they are algebraically dependent if and only if they are linearly dependent. As, Jacobian matrix of linear polynomials is just the matrix of their coefficients, we can show this using Jacobian Criterion (proved later) for algebraic independence.

2.3.3.2 Monomials

Lemma 2.9. *[Mit13] A set of monomials are algebraically independent if and only if their exponent vectors are linearly independent over $\mathbb{Z}$.*

Proof. If $m_i = {x_1}^{\alpha_{i1}} \ldots {x_n}^{\alpha_{in}}$, then (α_i)=$(\alpha_{i1}, \alpha_{i2}, \ldots, \alpha_{in})$ is called the exponent vector of the monomial m_i. Now, let us assume that the exponent vectors of the monomials are $\mathbb{Z}$-linearly dependent and

$$\lambda_1.\alpha_1 + ... + \lambda_n.\alpha_n = 0$$

From this, we can easily show,

$${m_1}^{\lambda_1}{m_2}^{\lambda_2}\ldots{m_n}^{\lambda_n} = 1$$

This shows $m_1, \ldots, m_n$ are algebraically dependent.

Conversely, let $m_1, \ldots, m_n$ be algebraically dependent. If $t_1, \ldots, t_r$ are the terms of the annihilating polynomial, then $t_i(m_1, \ldots, m_n)$ is a monomial for all t_i. As all these monomials cancel, there are two distinct terms $t_1 = {y_1}^{\lambda_1}{y_2}^{\lambda_2}...{y_n}^{\lambda_n}$ and $t_2 = {y_1}^{\mu_1}{y_2}^{\mu_2}...{y_n}^{\mu_n}$ such that $t_1(m_1, ..., m_n) = t_2(m_1, ..., m_n)$.

Plugging in $m_1, ..., m_n$ in t_1 and t_2, we will get
$(\lambda_1 - \mu_1)\alpha_1 + \cdots + (\lambda_n - \mu_n)\alpha_n = 0$. 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.

□

2.4 A Sufficient condition for Algebraic Independence

Lemma 2.10. *[KR05] Let $f_1, \ldots, f_n \in k[x_1, \ldots, x_n]$ be non-zero polynomials. If under some lexicographic ordering σ, leading monomials of $f_1, \ldots, f_n$ are algebraically independent over K, then $f_1, \ldots, f_n$ are algebraically independent over K.*

Proof. Let us assume according to a lexicographic ordering σ, leading monomials of $f_1, \ldots, f_n$ are respectively $LM(f_1), \ldots, LM(f_n)$. Take any nonzero polynomial $g(f_1, \ldots, f_n)$. Let us suppose that m is the monomial in the support of g, such that $m(LM(f_1), \ldots, g(LM(f_n))$ is leading with respect to σ. Hence, for any monomial m' in the support of g, and any monomial k_i in the support of f_i,

$$m'(k_1, \ldots, k_n) \preceq m'(LM(f_1, \ldots f_n)) \preceq m(LM(f_1), \ldots, LM(f_n))$$

In this case the last inequality cannot be equality, unless $m' = m$. Otherwise, $m' - m$ is the annihilating polynomial of leading monomials, contradicting the assumption. So, this proves, the monomial $m(LM(f_1), \ldots, g(LM(f_n))$ cannot cancel with other monomials. This implies that there is no nonzero annihilating polynomial for $f_1, \ldots, f_n$. □

This condition on leading terms is not a necessary condition for algebraic independence as there are algebraically independent polynomials such that under all possible lexicographic orderings, their leading terms are algebraically dependent. For example, $x + y$ and $x^3 + y^3$ are algebraically independent over $\mathbb{Q}$ and under both orderings $x \prec y$ and $y \prec x$, leading terms are dependent.
As a corollary of this condition, we can show if in a set of n-variate polynomials, each polynomial has a variable, which is not present in the other polynomials, then

they are algebraically independent, because we can pick a lexicographic ordering such that the leading terms would be the terms containing the unique variables.

2.5 Jacobian Criterion

[ER93, For92] Jacobian converts the nonlinear problem of testing algebraic independence to linear algebra. We define Jacobian matrix as

$$Jac_{x_1,\ldots,x_n}(f_1,\ldots,f_n) = \begin{bmatrix} \frac{\partial f_1}{\partial x_1} & \frac{\partial f_2}{\partial x_1} & \cdots & \frac{\partial f_n}{\partial x_1} \\ \frac{\partial f_1}{\partial x_2} & \frac{\partial f_2}{\partial x_2} & \cdots & \frac{\partial f_n}{\partial x_2} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{\partial f_1}{\partial x_n} & \frac{\partial f_2}{\partial x_n} & \cdots & \frac{\partial f_n}{\partial x_n} \end{bmatrix}$$

Jacobian follows Chain Rule.

$$Jac_x(f(g)) = Jac_{g(x)}(f)Jac_x(g)$$

Theorem 2.11. *Over fields of characteristic zero, the transcendence degree of the polynomials $f_1,\ldots,f_n$ in$[x_1,\ldots,x_m]$ equals to the rank of the Jacobian matrix $Jac_{x_1,\ldots,x_m}(f_1,\ldots,f_n)$.*

We prove the case, when $m = n$.

Proof. Let us suppose that the f_i are algebraically dependent and $A \in k[y_1,\ldots,y_n]$ is a minimal degree annihilating polynomial that is $A(f_1,\ldots,f_n) \equiv 0$.

Differentiating the annihilating polynomial with respect to x_i and applying the chain rule, we get

$$\frac{\partial}{\partial x_i}A(f_1,\ldots,f_n) = \frac{\partial A}{\partial y_1}\frac{\partial f_1}{\partial x_i} + \cdots + \frac{\partial A}{\partial y_n}\frac{\partial f_n}{\partial x_i} \equiv 0$$

Arranging all the equations, we get

$$Jac(f_1,\ldots,f_n)\begin{bmatrix} \frac{\partial A}{\partial y_1} \\ \vdots \\ \frac{\partial A}{\partial y_n} \end{bmatrix} = \begin{bmatrix} 0 \\ \vdots \\ 0 \end{bmatrix}$$

Over characteristic zero, we can always find y_i such that $\frac{\partial A}{\partial y_i}$ is not zero. Over characteristic p, if for all i, $\frac{\partial A}{\partial y_i}$ is zero, then A is p^{th} power of some polynomial. So, it will contradict the fact that A was the minimal annihilating polynomial.

After fixing such a y_i, $\frac{\partial A}{\partial y_i}|_{y_j=f_j}$ should be nonzero. As derivative decreases the degree, if $\frac{\partial A}{\partial y_i}|_{y_j=f_j}$ is zero, it would become an annihilating polynomial of $f_1, \ldots, f_n$ with lesser degree than A. This contradicts the assumption that A is the minimal annihilating polynomial of $f_1, \ldots, f_n$.

Thus, $\frac{\partial A}{\partial y_i}$ cannot be all zero. So, determinant of Jacobian matrix must be zero.

Converse: Let us assume that the f_i are algebraically independent. Now, we know if number of polynomials are greater than the number of variables, then the polynomials are always algebraically dependent, so for each i there is a minimal degree annihilating polynomial $A_i \in k[y_0, \ldots, y_n]$ such that

$$A_i(x_i, f_1, \ldots, f_n) \equiv 0$$

As $f_1, \ldots, f_n$ are not algebraically dependent, the annihilating polynomial A_i should have y_0. As the field has characteristic zero,

$$\forall i : \frac{\partial A_i}{\partial y_0} \neq 0$$

We note, over small characteristic, this is the step, where proof of this direction of Jacobian criterion breaks down. Because, derivative of a p^{th} power is zero, over characteristic p, we cannot say $\forall i : \frac{\partial A_i}{\partial y_0} \neq 0$. If the field has characteristic larger than the degree bound of this annihilating polynomials, then only this step would be correct over characteristic p. Now, If $\frac{\partial A_i}{\partial y_0}$ evaluated at $x_i, f_1, \ldots, f_n$ is zero, that would contradict the fact that A_i is the minimal degree annihilating polynomial of $x_i, f_1, \ldots, f_n$, because derivative decreases the degree.

For all i,

$$\frac{\partial A_i}{\partial x_i} = \frac{\partial A_i}{\partial y_0} + \frac{\partial A_i}{\partial y_1}\frac{\partial f_1}{\partial x_i} + \cdots + \frac{\partial A_i}{\partial y_n}\frac{\partial f_n}{\partial x_i} \equiv 0$$

$$j \neq i \Rightarrow \frac{\partial A_i}{\partial x_j} = \frac{\partial A_i}{\partial y_1}\frac{\partial f_1}{\partial x_j} + \cdots + \frac{\partial A_i}{\partial y_n}\frac{\partial f_n}{\partial x_j} \equiv 0$$

$$Jac(f_1,\ldots,f_n)\begin{bmatrix}\frac{\partial A_i}{\partial y_1}\\ \frac{\partial A_i}{\partial y_2}\\ \vdots\\ \frac{\partial A_i}{\partial y_n}\end{bmatrix} = \begin{bmatrix}0\\ \vdots\\ -\frac{\partial A_i}{\partial y_0}\\ \vdots\\ 0\end{bmatrix} \leftarrow i^{th} position$$

$$Jac(f_1,\ldots,f_n)\begin{bmatrix}\frac{\partial A_1}{\partial y_1} & \frac{\partial A_2}{\partial y_1} & \cdots & \frac{\partial A_n}{\partial y_1}\\ \frac{\partial A_1}{\partial y_2} & \frac{\partial A_2}{\partial y_2} & \cdots & \frac{\partial A_n}{\partial y_2}\\ \vdots & \vdots & \ddots & \vdots\\ \frac{\partial A_1}{\partial y_n} & \frac{\partial A_2}{\partial y_n} & \cdots & \frac{\partial A_n}{\partial y_n}\end{bmatrix} = -\begin{bmatrix}\frac{\partial A_1}{\partial y_0} & 0 & \cdots & 0\\ 0 & \frac{\partial A_2}{\partial y_0} & \cdots & 0\\ \vdots & \vdots & \ddots & \vdots\\ 0 & 0 & \cdots & \frac{\partial A_n}{\partial y_0}\end{bmatrix}$$

As the matrix at right hand side is a diagonal matrix with all diagonal entries nonzero, Jacobian must have full rank. □

We note that the same proof works for rational functions as well. For an abstract proof of Jacobian criterion, we refer [MSS12] For the proof of the general case, that transcendence degree equals the rank of the Jacobian, we refer [BMS13].

Here, we give an alternate representation of Jacobian. Let R be a ring, and A be a R-algebra. Differentials are objects following these two rules $d(ra+sb) = r\ da+s\ db$ and $d(ab) = a\ db + b\ da$. Wedge products or exterior products are antisymmetric product. $du \wedge dv = -dv \wedge du$. Ω denotes the universal module of differentials of the polynomial ring $k[x_1,\ldots,x_n]$ over k.

$$df_1 \wedge \cdots \wedge df_2 = Jac_{x_1,\ldots,x_n}(f_1,\ldots,f_n)dx_1 \wedge \cdots \wedge\ dx_n$$

2.6 Algebraic Independence over positive characteristic

There are polynomials over $\mathbb{F}_p$ which are algebraically dependent over $\mathbb{F}_p$ but independent if viewed over $\mathbb{Q}$. For example, $f = x+y$ and $g = x^p+y^p$ are two such polynomials because in $\mathbb{F}_p$, $(x+y)^p = x^p+y^p$. Now, if $f_1,\ldots,f_n$ are algebraically dependent over $\mathbb{F}_p$, then we know that Jacobian of $f_1,\ldots,f_n$ would be zero over $\mathbb{F}_p$, because while proving the Jacobian criterion, we saw that even over positive characteristic, this direction of Jacobian criterion holds true. So, nonzero Jacobian over $\mathbb{F}_p$ proves that the polynomials are algebraically independent. But the other direction is false over fields of positive characteristic unless the characteristic of the field is greater than the product of the degrees of the polynomials (equivalently degree bound of annihilating polynomial).[Mit13]

2.6.1 Witt-Jacobian Criterion

[MSS12] introduced a new generalization of Jacobian, which they named Witt-Jacobian, that works over all finite fields. Unlike Jacobian criterion's proof, Witt-Jacobian Criterion's proof is not elementary, it uses technical results from algebraic geometry like De Rahm Complex. One key idea of Witt-Jacobian is it lifts the coefficients of polynomials from $\mathbb{F}_p$ to $\widehat{\mathbb{Z}}_p$(p-adics), thereby changing the characteristic from p to zero.

For $\ell \geq 1$, the ℓ^{th} Witt-Jacobian is defined as,

$$WJP_\ell(F) = (\widehat{f_1}\dots\widehat{f_n})^{p^{\ell-1}-1}(x_1\dots x_n).detJac(\widehat{f_1}\dots\widehat{f_n})$$

Witt-Jacobian f is called $(\ell{+}1)$-**degenerate** if the coefficient of $\mathbf{x}^\alpha$ in f is divisible by $p^{min[v_p(\alpha),\ell]+1}$ for all $\alpha \in \mathbb{N}^n$. $v_p(\alpha)$ is the highest power of p dividing all α_n.

Now, the explicit Witt-Jacobian criterion of algebraic independence is:

Theorem 2.12. *$f_1,\dots,f_n$ are algebraically independent if and only if $\ell+1th$ Witt Jacobian polynomial $WJP_{\ell+1} = (\widehat{f_1}\dots\widehat{f_n})^{p^\ell-1}.Jac(\widehat{f_1},\dots,\widehat{f_n}).x_1\dots x_n$ is not $(\ell+1)$ degenerate for $\ell \geq \log_p[\mathbb{F}(x_1,\dots x_n):\mathbb{F}(f_1,\dots f_n)]_{insep}$*

Here, $[\mathbb{F}(x_1,\dots x_n):\mathbb{F}(f_1,\dots f_n)]_{insep}$ is the inseparable degree of the finitely generated field extension. We refer to [MSS12] for the definition. This degree is bounded by product of the degrees of the polynomials.

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

where r is the transcendence degree of the polynomials and δ is the maximum degree.

As degeneracy testing is computationally hard in general, and Witt-Jacobian may have exponential sparsity, it is difficult to test this criterion efficiently. This criterion can be tested in $\mathbf{NP}^{\mathbf{\#P}}$ complexity, that means by a nondeterministic polynomial time Turing machine with a $\#\mathbf{P}$ oracle.

Chapter 3

Correcting Jacobian's failure in special cases

3.1 Jacobian Correcting Transformations

We have seen that there are algebraically independent polynomials $f_1, \ldots, f_n$ over $\mathbb{F}_p$, such that their Jacobian is zero. In this case, we say that Jacobian is *failing.* A natural question is whether we can always transform the polynomials $f_1, \ldots, f_n$ (preserving their transcendence degree) to $g_1, \ldots, g_n$ such that $Jac(g_1, \ldots, g_n)$ is non-zero. We know if Jacobian of $g_1, \ldots, g_n$ is nonzero over $\mathbb{F}_p$, then $g_1, \ldots, g_n$ are algebraically independent over $\mathbb{F}_p$. As the transformation is transcendence degree preserving, we can conclude that $f_1, \ldots, f_m$ are algebraically independent over $\mathbb{F}_p$. We call $g_1, \ldots, g_m$ as *algebraic independence certifying polynomials* for $f_1, \ldots, f_m$ and the transformation as *Jacobian correcting transformation* and transcendence degree preserving transformation as *faithful transformation.*
Faithful transformations like applying algebraically independent polynomial map cannot correct Jacobian because chain rule shows that Jacobian of the transformed polynomials is multiple of the Jacobian of the original polynomials. But one faithful transformation can correct the Jacobian, if the polynomials are p^{th} powered, we can take the highest possible p^{th} root of them and then take the Jacobian. This sometimes corrects the Jacobian. For example: Jacobian fails for x^p, y^p. After taking p^{th} root of them, the Jacobian becomes nonzero.

But there are algebraically independent polynomials f, g over $\mathbb{F}_p$, none of them p^{th} powered, yet their Jacobian is zero. For example, $x^{p-1}y$ and xy^{p-1}. We give evidence to show that in some of these cases, we can apply faithful transformations like applying polynomial map and make them p^{th} powered.

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

3.1.1 Taking p^{th} root of polynomials

Lemma 3.1. *$f_1^{p^\alpha}, \ldots, f_m^{p^\alpha}$ are algebraically dependent over $\mathbb{F}_p$ if and only if $f_1, \ldots, f_m$ are algebraically dependent over $\mathbb{F}_p$.*

Proof. If $f_1^{p^\alpha}, \ldots, f_m^{p^\alpha}$ are algebraically dependent over $\mathbb{F}_p$, then there exists a nonzero annihilating polynomial $A(f_1^{p^\alpha}, \ldots, f_m^{p^\alpha}) = 0$. Clearly this same polynomial also annihilates $f_1, \ldots, f_m$.

If $f_1, \ldots, f_m$ are algebraically dependent over $\mathbb{F}_p$, then there exists a nonzero annihilating polynomial $A(f_1, \ldots, f_m) = 0$. Over $\mathbb{F}_p$: $(a+b)^{p^\alpha} = a^{p^\alpha} + b^{p^\alpha}$. If we take p^α power of A, we get

$$A^{p^\alpha}(f_1, \ldots, f_m) = A(f_1^{p^\alpha}, \ldots, f_m^{p^\alpha}) = 0.$$

Thus, A^{p^α} works as an annihilating polynomial for $f_1^{p^\alpha}, \ldots, f_m^{p^\alpha}$. □

We note that this proof can easily be generalized to the polynomials $f_1^{p^{\alpha_1}}, \ldots, f_n^{p^{\alpha_n}}$. The first part of the proof is just the same and in the second part, we simply take A^m as the annihilating polynomial where m is $p^{lcm(\alpha_1, \ldots, \alpha_n)}$.

3.1.2 Applying polynomial map

A polynomial map φ is :

$$(x_1, x_2, \ldots, x_n) \mapsto (g_1, g_2, \ldots, g_n)$$

where $g_i \in k[x_1, \ldots, x_n]$

So, a polynomial $f \in k[x_1, ..., x_n]$ gets mapped to $f(g_1, \ldots, g_n)$, we denote this by $\varphi(f)$

Lemma 3.2. *If $f_1, \dots, f_n$ are algebraically dependent then $\varphi(f_1), \varphi(f_2), \dots, \varphi(f_n)$ are algebraically dependent. If $g_1(x_1, \dots, x_n), \dots, g_n(x_1, \dots, x_n)$ are algebraically independent polynomials, then 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 φ as a homomorphism from $k[x_1, \dots, x_n] \to k[g_1, \dots, g_n]$. As $g_1, \dots, g_n$ are algebraically independent, φ is injective. For the sake of contradiction, assume that $f_1, \dots, f_n$ be algebraically independent but $\varphi(f_1), \varphi(f_2), \dots, \varphi(f_n)$ are algebraically dependent. So, there is a nonzero annihilating polynomial A such that $A(\varphi(f_1), \varphi(f_2), \dots, \varphi(f_n)) = 0$. As φ is homomorphism, $\varphi(A(f_1, \dots, f_n)) = 0$. As φ is injective, this means $A(f_1, \dots, f_n) = 0$. So, we get a contradiction. □

Now, we show how monomial maps and more generally, polynomial maps may help to transform a non p^{th}-powered polynomial to a p^{th}-powered polynomial. Let us assume, we have two bivariate polynomials f and g such that none of them is p^{th} powered and all occurrences of x in both the polynomials are p^{th}-powered, but not all of the occurrences of y are p^{th}-powered. In this case, this monomial map, $x \mapsto x$, and $y \mapsto y^p$ makes both f and g, p^{th}-powered and if we take highest possible p^{th} root, the occurrence of x which had minimum p^{th} power, becomes p^{th} power free.

Polynomial maps are more general than monomial maps. We show how polynomial maps can help to correct Jacobian with two examples.

- $f = x^2 + x^3 + y$ and $g = x^3 + y$ over $\mathbb{F}_2$ Now, applying the polynomial map,

  $$x \mapsto x$$

  $$y \mapsto x^3 + y^2$$

  We get, x^2 and y^2. After taking square root of both, we get x and y. This proves the independence of f and g.

- $f = x + y$, $g = xy^2 + y^3$ over $\mathbb{F}_2$ Now, applying the polynomial map

  $$x \mapsto x^2 - y$$

$$y \mapsto y$$

We get, x^2 and x^2y^2. After taking square root of both the polynomials, we get x and xy. Jacobian of x, y is clearly nonzero.

3.1.3 Taking polynomials from the ring or function field of original polynomials

We know that, transcendence degree of polynomials f, g over field k = transcendence degree of $k(f, g)$. As $k[f, g]$ is contained in the function field $k(f, g)$, this implies that if f and g are two algebraically dependent polynomials, then any two polynomials $p_1, p_2 \in k[f, g]$ should be also be algebraically dependent. So, if we take two polynomials from $k[f, g]$ and prove them to be algebraically independent, it proves f and g must be algebraically independent. The converse is obviously not true. Now, going to ring can help in getting algebraic independence certifying polynomials.

- Even if none of the original polynomials are p powered, we may find p^{th} powered polynomial in the ring generated by them, and after taking p^{th} root, Jacobian can be corrected sometimes. For example,take these two polynomials over $\mathbb{F}_2$, $f = x^2 + x^3 + y$ and $g = x^3 + y$. None of them are square. But, if we take $f - g$, it is just x^2. If we take the Jacobian of the square root of $f - g$ and g, the Jacobian would be non zero. This proves f and g are independent.

- For example, $f = u^{p-1}v^p$ and $g = u$ over $\mathbb{F}_p$. Now, taking product of f and g, we get $f' = u^pv^p$, which is p^{th}-powered. If $Jac(uv, u)$ is nonzero, we get algebraic independence certifying polynomial

3.2 Correction of the Jacobian in special cases

3.2.1 Monomials

In chapter two, we saw the characterization of algebraic independence of monomials. As algebraic independence of monomials is equivalent to $\mathbb{Z}$-linear independence of the exponent vectors of them, $M_1, \dots, M_n$ are algebraically independent over $\mathbb{F}_p$ if and only if they are algebraically independent over $\mathbb{Q}$. So testing independence of monomials is easy, we just have to check if their Jacobian over $\mathbb{Q}$ is nonzero or if the exponent vectors are $\mathbb{Z}$-linear dependent. But, there are algebraically independent monomials whose Jacobian over $\mathbb{F}_p$ is zero. Obviously, if one or both of the monomials are p-powered, Jacobian of them would be zero over $\mathbb{F}_p$. In this case, by taking p^{th} root, we can easily get algebraic independence certifying monomials. But it is not necessary that one or both of the failing monomials have to be p^{th} powered, we saw the example of failure of Jacobian for monomials like $x^{p-1}y, xy^{p-1}$. Here, we show we can also transform these kinds of monomials to p^{th} powered monomials.

Lemma 3.3. *Independence certifying polynomials exists for every set of n algebraically independent n-variate monomials over $\mathbb{F}_p$.*

Proof. Let us assume that we have n monomials, $M_1, \dots, M_n$, where

$$M_i = c_i \cdot x_1^{a_{i1}} x_2^{a_{i2}} \dots, x_n^{a_{in}}$$

Exponent vector for M_i is $(a_{i1}, ..., a_{in})$.
We denote the matrix of the exponent vectors of the monomials by

$$A_{n,n} = \begin{array}{c} \\ M_1 \\ M_2 \\ \vdots \\ M_n \end{array} \begin{array}{c} \begin{array}{cccc} x_1 & x_2 & \cdots & x_n \end{array} \\ \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix} \end{array}$$

Calculating the Jacobian using the definition we get

$$Jac(m_1, \dots, m_n) = (\prod_{i=1}^{n} c_i) \cdot det\ A \cdot \frac{\prod_{i=1}^{n} M_i}{\prod_{i=1}^{n} x_i}$$

Now, the monomials are algebraically dependent over any field if and only if $det\ A$ is zero over $\mathbb{Q}$. But Jacobian over $\mathbb{F}_p$ can be zero if $det\ A$ is divisible by p.

We show that we can correct the Jacobian by applying a monomial map, each variable is mapped to algebraically independent monomials.

$$(x_1, x_2, \ldots, x_n) \mapsto (N_1, N_2, \ldots, N_n)$$

We illustrate this with an example. If $m_1 = x^a y^b, m_2 = x^c y^d$ and if

$$x \mapsto x^e y^f$$

$$y \mapsto x^g y^h$$

Then the transformed monomials become $m_1' = x^{ae+bg} y^{af+bh}$ $m_2' = x^{ce+dg} y^{cf+bh}$ We represent this with exponent matrix.

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} e & f \\ g & h \end{pmatrix} = \begin{pmatrix} ae + bg & af + bh \\ ce + dg & cf + bh \end{pmatrix}$$

Now, let us suppose B is the matrix of the exponent vectors of the monomials $N_1, \ldots, N_n$. It is easy to see that the matrix of the exponent vectors of the transformed monomials would be the product of the two exponent matrices $A \cdot B$.

So, we have to find a suitable B. We show that if we take B as the Adjoint of A (denoted by $Adj\ A$), we get algebraic independence certifying monomials.

We know that, $Adj\ A \cdot A = det\ A \cdot I_n$

Now, the exponent matrix of the transformed monomials would be

$$Adj\ A \cdot A = det\ A \cdot I_n$$

So, monomials would be transformed to

$$(M_1, M_2, \ldots, M_n) \mapsto (x_1^{detA}, x_2^{detA}, \ldots, x_n^{detA})$$

.

This transformation makes every monomial p^{th} powered as $det\ A = c \cdot p^k$.

After taking p^kth root, the monomials get transformed to $x_1^c, \ldots, x_n^c$, where c is not divisible by p.

Now, Jacobian of $x_1^c, \ldots, x_n^c$ is clearly non-zero.

□

3.2.2 Two bivariate binomials

Let us assume the given binomials over $\mathbb{F}_p$ (ignoring the constant terms) are

$$f_1(x,y) = m_1 + m_2$$

$$f_2(x,y) = n_1 + n_2$$

Here, $m_1 = \alpha_1 x^{a_1} y^{b_1}$, $m_2 = \alpha_2 x^{a_2} y^{b_2}$, $n_1 = \beta_1 x^{c_1} y^{d_1}$, $n_2 = \beta_2 x^{c_2} y^{d_2}$

Now,

$$Jac(f_1, f_2) = Jac(m_1, n_1) + Jac(m_1, n_2) + Jac(m_2, n_1) + Jac(m_2, n_2)$$

Let us assume, according to the lexicographic ordering $y \prec x$, $\{m_1, n_1\}$ are pair of leading monomials and $\{m_2, n_2\}$ are pair of least monomials.

ALGORITHM:

First, we test if the Jacobian of the two binomials is nonzero. If yes, the two polynomials are algebraically independent. Else, we go to Case 1.

- **Case 1:** We check if $\{m_1, n_1\}$ or $\{m_2, n_2\}$ are algebraically independent. If yes, then f_1 and f_2 are algebraically independent using the lemma from 2.10 Else, we go to case 2.

- **Case 2:** If both $\{m_1, n_1\}$ and $\{m_2, n_2\}$ are dependent, we check if $\{m_1, m_2\}$ are dependent. If yes, then f_1 and f_2 are dependent.

  Proof. If $\{m_1, n_1\}$ are algebraically dependent and $\{m_1, m_2\}$ are algebraically dependent, then $\{m_2, n_1\}$ are also algebraically dependent. This follows from 2.2.0.1 transitive property of algebraic dependence. In case of monomials, we can also directly verify this easily. Now $\{m_1, n_1\}$ are dependent and $\{n_1, n_2\}$ are dependent, so $\{m_1, n_2\}$ are dependent. As all pairs are dependent over $\mathbb{Q}$, $Jac(m_1, n_1) + Jac(m_1, n_2) + Jac(m_2, n_1) + Jac(m_2, n_2)$ is 0 if viewed over $\mathbb{Q}$. Thus, the two binomials will be dependent over $\mathbb{F}_p$ as well. □

Else, we go to case 3.

- **Case 3:** In this case, we apply the following monomial map on both the binomials. The exponent matrix of the monomial map is the adjoint matrix of the exponent matrix of m_1, m_2. As m_1, m_2 are independent, adjoint of their exponent matrix exists. Now, as we have seen in 3.2.1, the monomial map m_1 will be transformed to $\alpha_1 x^a$ and m_2 will be transformed to $\alpha_2 y^a$ where a is the determinant of the exponent matrix of m_1, m_2. As monomial map preserves transcendence degree, transformed m_1 and transformed n_1 should continue to be dependent. This implies that the map transforms n_1 to $\beta_1 x^c$. For the same reason, n_2 gets transformed to $\beta_2 y^d$. Now, the transformed binomials become

$$\alpha_1 x^a + \alpha_2 y^a$$

and

$$\beta_1 x^c + \beta_2 y^d$$

As $Jac(\alpha_1 x^a, \beta_1 x^c) = 0$ and $Jac(\alpha_2 y^a, \beta_2 y^d) = 0$

$$Jac(\alpha_1 x^a + \alpha_2 y^a, \beta_1 x^c + \beta_2 y^d) = Jac(\alpha_1 x^a, \beta_2 y^d) + Jac(\alpha_2 y^a, \beta_1 x^c)$$

We also use the fact that $Jac(c_1 x^a, c_2 y^b)$ is $abc_1c_2.x^{a-1}y^{b-1}$. So, it would be zero if and only if either a is divisible by p or b is divisible by p.

  - **Case A:** If none of a, c, d is divisible by p and $Jac(f_1, f_2)$ is zero, then the binomials are algebraically dependent.

    Proof. In this case, from the condition $Jac(f_1, f_2) = 0$, we get $c_1 x^{a-1} y^{d-1} = c_2 x^{c-1} y^{a-1}$ where $c_1 = ad\alpha_1\beta_2$ and $c_2 = ac\alpha_2\beta_1$. This implies $c_1 = c_2$ and $a = c = d$. From $c_1 = c_2$ and $c = d$, we get $\frac{\alpha_1}{\beta_1} = \frac{\alpha_2}{\beta_2}$ So, in this case the two binomials are constant multiples of each other. □

  - **Case B:** If a is divisible by p, remain in this case. else go to case C

    If the highest power of p dividing a is k. We take p^kth root from the first binomial. Now the first binomial is not p^{th} power anymore. We take Jacobian of the transformed binomials again. If Jacobian is nonzero, the binomials are independent. If Jacobian is zero, then go to next case.

- **Case C:** If a is not divisible by p, and c is divisible by p, but d is not divisible by p.

  Proof. If only c is divisible by p, then $Jac(\alpha_2 y^a, \beta_1 x^c)$ is zero. But $Jac(\alpha_1 x^a, \beta_2 y^d)$ is nonzero. So, Jacobian of the two binomials is nonzero in this case. □

  If a is not divisible by p and d is divisible by p, but c is not divisible by p, the same proof works and Jacobian is nonzero.

- **Case D:** In this case, p divides both c, d. We take highest possible p^{th} root from c, d. Now, if p does not divide both c, d, this will lead to case A, so we know the binomials are algebraically dependent in this case. The other possible case is p does not divide one of c or d. In this case, as the Jacobian is nonzero, the binomials are algebraically independent.

Time complexity:

Each case involves only checking if the highest power of p dividing the exponents and checking if Jacobian of the two binomials is zero. Even if the exponents are exponential in terms of bitsize, these operations can be done in polynomial time in the size of the input. So, this algorithm decides algebraic independence of two binomials in polynomial time in the size of input.

Chapter 4

Lifting the Jacobian

Let $f(x, y)$, $g(x, y)$ be two polynomials over $\mathbb{F}_p$, whose Jacobian is zero over $\mathbb{F}_p$ but when f and g are viewed as polynomials over $\mathbb{Q}$, the Jacobian is nonzero. It implies that all the coefficients of the Jacobian polynomial are divisible by p. The highest power of p dividing the Jacobian is called valuation (or p-adic order) of the Jacobian. If the Jacobian is zero over $\mathbb{Q}$, it's p-adic valuation would be infinity, because any power of p divides the Jacobian. A lift of a polynomial over $\mathbb{F}_p$ is adding a polynomial whose all coefficients are divisible by p. For example, $x^p + px$ is a lifted polynomial of x^p. Clearly, f and g are algebraically dependent over $\mathbb{F}_p$ if and only if $f + p\mu$ and $g + p\delta$ are algebraically dependent.

Let us take two algebraically dependent polynomials over $\mathbb{F}_p$, $x + y$ and $x^p + y^p$. If we lift the second polynomial by adding $(x + y)^p - (x + y)$ to $(x + y)^p$, the p-adic valuation of the Jacobian gets increased, in this case it goes up to infinity. We show that for any two algebraically dependent polynomials, p-adic valuation of the Jacobian can be arbitrarily increased by lifting. We also prove the converse, if they are independent, p-adic valuation of the Jacobian cannot be increased arbitrarily. This gives a characterization of algebraic dependence over finite fields based on classical Jacobian, though we do not know if it is computationally efficient.

Theorem 4.1. *p-adic valuation of $Jac(f, g)$ can be increased arbitrarily if and only if f, g are algebraically dependent.*

Proof. $\Rightarrow$ To prove this direction, we first prove the following lemma.

Lemma 4.2. *p-adic valuation of evaluated Annihilating Polynomial can be increased arbitrarily .*

Proof. Let us take two bivariate polynomials $f(x, y), g(x, y)$ which are dependent over $\mathbb{F}_p$, but independent over $\mathbb{Q}$. Let $A(x, y)$ be the minimal annihilating polynomial of f and g. Here, $A(f(x, y), g(x, y))$ is a zero polynomial over $\mathbb{F}_p$, that is, if we view $A(f(x, y), g(x, y))$ as a polynomial over $\mathbb{Q}$, all its coefficients are divisible by p. The highest power of p dividing all its coefficients is called the p-adic valuation of the annihilating polynomial evaluated at $f(x, y), g(x, y)$.

$$A(x, y) = \sum c_i x^{d_i} y^{e_i}$$

$$A(f, g) = \sum c_i f^{d_i} g^{e_i} \equiv 0\ (mod\ p)$$

Now, polynomials are lifted.

$$f \mapsto f + p\delta$$

$$g \mapsto g + p\mu$$

We want δ and μ such that,

$$A(f + p\delta, g + p\mu) \equiv 0\ (mod\ p^2)$$

$$\sum c_i (f + p\delta)^{d_i} (g + p\mu)^{e_i} \equiv 0\ (mod\ p^2)$$

Here we note that the same annihilating polynomial would work for the lifted polynomials as well.

Expanding the expression using binomial theorem and removing the terms with coefficients divisible by p^2, we get the following congruence equation.

$$\sum c_i f^{d_i} g^{e_i} + p\delta \sum c_i f^{d_i - 1} e_i g^{e_i} + p\mu \sum c_i f^{d_i} e_i g^{e_i - 1} \equiv 0\ (mod\ p^2)$$

As $p|A(f, g)$, we can write $p^{-1}A(f, g)$, and the above congruence equation is equivalent to

$$p^{-1}(\sum_i f^{d_i} g^{e_i}) + \delta \sum c_i f^{d_i - 1} e_i g^{e_i} + \mu \sum c_i f^{d_i} d_i g^{e_i - 1} \equiv 0\ (mod\ p)$$

The above equation can be re-written as,

$$p^{-1}A(f, g) + (\partial_x A)|_{(f,g)}\delta + (\partial_y A)|_{(f,g)}\mu \equiv 0\ (mod\ p)$$

Now, this equation has two unknowns δ and μ, we set one of them zero, and find the other. If

$$(\partial_x A)|_{(f,g)} \not\equiv 0 \ (mod\ p)$$

then we get the solution as,

$$\delta = \frac{-p^{-1}A(f,g)}{(\partial_x A)|_{(f,g)}}$$

$$\mu = 0$$

Similarly if

$$(\partial_x A)|_{(f,g)} \equiv 0 \ (mod\ p) \text{ but } (\partial_y A)|_{(f,g)} \not\equiv 0 \ (mod\ p)$$

we have the following solution,

$$\delta = 0$$

$$\mu = \frac{-p^{-1}A(f,g)}{(\partial_y A)|_{(f,g)}}$$

Now, if

$$(\partial_x A)|_{(f,g)} \equiv 0 \ (mod\ p) \text{ and } (\partial_y A)|_{(f,g)} \equiv 0 \ (mod\ p)$$

then, $A(x,y)$ is p^{th} power of some polynomial. In this case, $A^{1/p}$ will also be an annihilating polynomial. This contradicts the fact that A was the minimal annihilating polynomial.

Now, we have

$$A(f + p\delta, g + p\mu) \equiv 0 \ (mod\ p^2).$$

If we write $f + p\delta$ as f_1 and $g + p\mu$ as g_1 we can again repeat the same argument by lifting f_1 to $f_1 + p^2\delta_1$ and g_1 to $g_1 + p^2\delta_2$. Then we can get

$$A(f + p\delta + p^2\delta_1, g + p\mu + p^2\mu_1) \equiv 0 \ (mod\ p^4).$$

Iterating this process i times, we will get

$$A(f + p.\delta_{i'}, g + p.\mu_{i'}) \equiv 0 \ (mod\ p^{2^i}).$$

Here $\delta_{i'} = \sum_{j=1}^{i} p^{2^{j-1}}\delta_j$ and $\mu_{i'} = \sum_{j=1}^{i} p^{2^{j-1}}\delta_j$

□

Now, using this lemma, we can prove that $Jac(f, g)$'s p-adic valuation can be arbitrarily increased if f, g are algebraically dependent. The proof is exactly similar to the approach of proving that if f and g are algebraically dependent, then Jacobian of f and g is zero. We are using the same technique, presented here using the language of differentials and wedge product.

Let $A(f, g)$ be a minimal annihilating polynomial of f and g such that $A(f, g) \equiv 0\ (mod\ p)$.

After lifting f to f_1 and g to g_1, we get,

$$A(f_1, g_1) \equiv 0\ (mod\ p^2).$$

Applying the differential operator on A, we get

$$dA(f_1, g_1) \equiv 0\ (mod\ p^2).$$

Taking wedge product (or exterior product) with dg_1, we get,

$$dA(f_1, g_1) \wedge dg_1 \equiv 0\ (mod\ p^2).$$

Now,

$$(\partial_{f_1} A(f_1, g_1) df_1 + \partial_{g_1} A(f_1, g_1) dg_1) \wedge dg_1 \equiv 0\ (mod\ p^2).$$

We get,

$$\partial_{f_1} A(f_1, g_1)(df_1 \wedge dg_1) \equiv 0\ (mod\ p^2).$$

Now if $\partial_{f_1} A(f_1, g_1) \equiv 0\ (mod\ p)$, we take $dA(f_1, g_1) \wedge df_1$.

Repeating the previous steps, we'll get

$$\partial_{g_1} A(f_1, g_1)(dg_1 \wedge df_1) \equiv 0\ (mod\ p^2).$$

Now, both $\partial_{f_1} A(f_1, g_1)$ and $\partial_{g_1} A(f_1, g_1)$ cannot vanish $mod\ p$, because that implies that the annihilating polynomial is p^{th} power of some polynomial, contradicting the fact that A was the minimal annihilating polynomial. So, we get

$$(df_1 \wedge dg_1) \equiv 0 \ (mod \ p^2).$$

So, the lifts which increased the p-adic valuation of the annihilating polynomial would also increase the p-adic valuation of the Jacobian.

$\Leftarrow$ Now, we prove the converse using the non-degeneracy condition of algebraic independence from [MSS12].

$Jac(f, g)$ cannot be lifted arbitrarily if f and g are algebraically independent. The number of steps of lifting is upper bounded by $\log_2(\log_p[\mathbb{F}(x, y) : \mathbb{F}(f, g)]_{insep} + 1)$

Proof. We prove this by contradiction. Let us assume that Jacobian's p-adic valuation can be arbitrarily lifted even when f and g are algebraically independent. So, after the ith lifting, f and g can be lifted to f_i and g_i such that

$$Jac(f_i, g_i) \equiv 0 \ (mod \ p^{2^i}).$$

After $i = \log_2(\log_p[\mathbb{F}(x, y) : \mathbb{F}(f, g)]_{insep} + 1)$ many steps, we get

$$Jac(f_i, g_i) \equiv 0 \ (mod \ p^{m+1}).$$

where $m = log_p[\mathbb{F}(x, y) : \mathbb{F}(f, g)]_{insep}$

Now, from the explicit definition of Witt-Jacobian 2.6.1, Witt-Jacobian is a multiple of the p-adic Jacobian. So we get,

$$WJP_{m+1}(f_i, g_i) \equiv 0 \ (mod \ p^{m+1})$$

That means, $WJP_{m+1}(f_i, g_i)$ is $m + 1$ degenerate.

But as $m + 1^{th}$ Witt-Jacobian polynomial's degeneracy cannot be increased by lifting, we get $WJP_{m+1}(f, g)$ is also $m + 1$ degenerate.

This contradicts with $m + 1^{th}$ Witt-Jacobian's non-degeneracy condition. □

□

This theorem can be potentially used to design an algorithm for testing algebraic independence over positive characteristic, but currently we do not know if it is computationally feasible. Let us assume that the input polynomials are f_0 and g_0 and

$$df_0 \wedge dg_0 \equiv 0 \ mod \ (p).$$

We search for rational functions δ_1 and μ_1 over characteristic p such that

$$d(f_0 + p \cdot \delta_1) \wedge d(g_0 + p \cdot \mu_1) \equiv 0 \ mod \ (p^2).$$

If we can solve this equation, we iterate this process again $i = \log_2(\log_p[\mathbb{F}(x, y) : \mathbb{F}(f, g)]_{insep} + 1)$ many steps. If in that step, Jacobian can be lifted, then the polynomials are algebraically dependent. Otherwise, the polynomial are algebraically independent. We note that in the special case of purely inseparable extensions of exponent 1, that means if $[\mathbb{F}(x, y) : \mathbb{F}(f, g)]_{insep} = p$, then we need to just check for the existence of δ_1 and μ_1, this could be easier than the general case. We end this chapter with the following conjecture.

Conjecture 4.3. *If two polynomials are algebraically dependent over $\mathbb{F}_p$, then we can lift those polynomials so that they become algebraically dependent over $\mathbb{Q}$.*

Chapter 5

Conclusion and Future Directions

5.1 Summary

We have pursued two approaches to efficiently test algebraic independence of polynomials over positive characteristic. Both the approaches are around the classical Jacobian criterion. The first approach we have tried is transforming polynomials such that Jacobian works correctly for the transformed polynomials. We could find such transformations for special cases like monomials and two binomials. The main difficulty in this approach, is transforming a polynomial to a p^{th} power. Although, we can probably resolve a few more cases with this technique, new tools are needed to make this approach work for the general case of two high degree polynomial's algebraic independence testing. The second approach we have tried is lifting the polynomials and it's effect on Jacobian's p-adic valuation. We have come up with a characterization, which is closer to classical Jacobian than Witt-Jacobian. Though we do not know how to test this criterion effectively, pursuing this approach may lead to new insights on the problem.

5.2 Future Directions

We would try to extend the proof of two binomial's algebraic independence testing to two bivariate trinomials and if possible to the case of two bivariate polynomials with constantly many monomials. We would also like to prove or disprove the following conjecture.

Conjecture 5.1. *If f and g are two algebraically independent polynomials over $\mathbb{F}_p$ such that their Jacobian polynomial is zero, we can always get algebraic independence certifying polynomials for them by applying suitable polynomial map and and taking p^{th} root.*

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.

[BMS13] Malte Beecken, Johannes Mittmann, and Nitin Saxena. Algebraic independence and blackbox identity testing. *Inf. Comput.*, 222:2–19, 2013.

[BS83] Walter Baur and Volker Strassen. The complexity of partial derivatives. *Theoretical computer science*, 22(3):317–330, 1983.

[Coh03] Paul M Cohn. *Basic algebra: groups, rings, and fields.* Springer, 2003.

[DGW09] Zeev Dvir, Ariel Gabizon, and Avi Wigderson. Extractors and rank extractors for polynomial sources. *Computational Complexity*, 18(1):1–58, 2009.

[ER93] Richard Ehrenborg and Gian-Carlo Rota. Apolarity and canonical forms for homogeneous polynomials. *European Journal of Combinatorics*, 14(3):157–181, 1993.

[For92] Krister Forsman. Two themes in commutative algebra: Algebraic dependence and k ahler differentials. 1992.

[Kal85] KA Kalorkoti. A lower bound for the formula size of rational functions. *SIAM Journal on Computing*, 14(3):678–687, 1985.

[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.

[KR05] M. Kreuzer and L. Robbiano. *Computational Commutative Algebra 2*. Number v. 1 in Computational commutative algebra. Springer, 2005.

[L'v84] MS L'vov. Calculation of invariants of programs interpreted over an integrality domain. *Cybernetics and Systems Analysis*, 20(4):492–499, 1984.

[Mit13] Johannes Mittmann. *Independence in Algebraic Complexity Theory*. PhD thesis, Universitäts-und Landesbibliothek Bonn, 2013.

[MSS12] Johannes Mittmann, Nitin Saxena, and Peter Scheiblechner. Algebraic independence in positive characteristic–a p-adic calculus. *arXiv preprint arXiv:1202.4301*, 2012.

[VdWAN31] Bartel Leendert Van der Waerden, Emil Artin, and Emmy Noether. *Moderne algebra*, volume 31950. Springer, 1931.