Towards Algebraic Independence based PITs over arbitrary Fields

Prerona Chatterjee

Tata Institute of Fundamental Research

School of Technology and Computer Science

Master's Project Report

Towards Algebraic Independence based PITs over arbitrary Fields

submitted by

18/12/2017

Prerona Chatterjee

Supervisor:

12/12/2017

Ramprasad Saptharishi

December, 2017

Abstract

The connection between Algebraic Independence and PITs was first studied by Beecken-Mittmann-Saxena [BMS11]. The ideas were then used to solve PITs for non-trivial circuit classes by Agrawal-Saha-Saptharishi-Saxena [ASSS12]. However, they required the field under consideration to have characteristic zero.

The reason was that their technique required constructing "faithful maps", for which they used the Jacobian Criterion, and this required the field to have characteristic zero. Recently however, Pandey-Saxena-Sinhababu [PSS16] gave a Jacobian-like criterion for fields of arbitrary characteristic.

In this thesis, we have used the [PSS16] criterion to construct "faithful maps" for fields of any characteristic. Further, this allowed us to extend the sparse polynomial PIT presented in [BMS11] to arbitrary fields in the case when a parameter called the "inseparable degree" is constant.

Acknowledgements

I would like to thank Ramprasad for believing in me and supporting me throughout these last six months. Everything that I have learnt in this period, right from how to read a paper to working independently and coming up with something non-trivial, is because of him. I wish that one day, I will be able to see and explain concepts as clearly as he does.

I would also like to thank the organisers of the NMI workshop on Arithmetic Circuits held at IMSc, since it was attending this workshop that made me realise my interest in this field.

Sagarmoy sir, it is you who had introduced me to theoretical computer science, to the algebraic techniques in this field and also to Ramprasad. For these, I will forever be grateful.

I had always wanted to do research since I was in class 6 because it seemed to be the only way I could keep studying and get paid for it. Clearly, to have such a dream and being able to reach a point where it doesn't seem too far-fetched requires a lot of "thank-you"s. One big reason for me being the person that I am is that I was fortunate enough to attend some of the best institutions in our country.

La Martiniere for Girls, Kolkata: I had the best childhood one could hope for because of the school I went to. To each and every teacher who taught there in the period 1999-2011, even those who did not teach me, I know for a fact that you loved me as your own daughter. I would like to thank you all for creating an ideal world hidden from the real world. It allowed me to dream big and made me believe that everything is possible. To my friends, thank you for making my school life so memorable.

St. Xavier's College, Kolkata: I would like to thank all the teachers and classmates for making me mentally stronger and making me realise how important it is to listen to one's own heart.

IIT Guwahati: Thank you for giving me everything and more than I ever asked for. To every teacher, thank you for making me believe that my dream was reachable and guiding me towards it. To my friends Pranali, Sayani, Shyam, and Shamik: I know that I have given higher priority to my studies most of the time, both during the IIT days and now. Yet you have never failed to support me whenever I needed you. Thank you for tolerating me. Thank you for everything.

TIFR, Mumbai: This place is everything and more than I could have ever imagined what a research institute could be like. I would like to thank Jaikumar for being a father figure to me, and for being a person I can only hope to become like. I would also like to thank Arkadev for his enthusiasm that got me interested in Complexity theory. To Shraddha and the "Outingphilic Group": Thank you for making life at TIFR enjoyable despite the huge pressure.

This would be incomplete if I do not thank a few other people I met academically. Kunal Sir, thank you for getting me interested in mathematics. Jayanta Sir, thank you for the sleepless nights I spent writing the Java programs you gave for homework. The only reason I realised that my real interest lied in CS and not pure math was your tuition classes. And finally, Apoorva: I know we haven't spoken properly in a long time, but I really dont know how the last two years of school would have been had we not met. Thankyou.

To my brother Prithu, thank you for always having my back. Thank you baba for working selflessly so that we could get the best of everything. And to my grandfather, thank you for being who you are, the more time I spend with my books the more I begin to understand you.

To the three women who had the biggest hand in making me the person I am. Thank you ma for teaching some of the most important virtues required to become anything non-trivial. Thank you Taua for perfectly complementing ma, thank you for introducing me to the world of reading and thank you for always believing in me. Thank you to Ma'am Peacock for being the perfect role model as I grew up, and teaching me how important it is to remain a child at heart.

Finally to the man I have never met, but has been the reason I have never given up irrespective of how many times I fail. Thank you Rahul Dravid for teaching me how important it is to work hard, stay stubborn, stay true to oneself and get up to fight every time one falls down. I really doubt I would have gotten anywhere close to the position I am in had it not been for Rahul Dravid, and it is to him I dedicate my first original work.

To Rahul Dravid

Contents

1 Introduction

The area of complexity theory tries to classify problems depending on the amount of resources it requires with respect to the size of its input. In Algebraic Complexity Theory one tries to, among other things, classify polynomials according to how "easy" it is to compute them. The "easy"ness of a polynomial is mostly described by the minimum number of operations required to compute it and this measure is written in terms of the number of variables it depends on and its degree.

An n-variate polynomial that requires $\text{poly}(n)$ many operations is considered to be efficiently computable. "Low degree" polynomials that are efficiently computable constitute the class VP — the algebraic counterpart of P, the class of efficiently solvable problems. Similarly VNP, the class of "explicit" polynomials, is the algebraic counterpart of the class NP. Both these classes were formally defined by Valiant in his seminal paper [Val79], where he also defined complete problems for these classes.

Further, these complete problems show that VP seems to have the computational powers equivalent to a class considered to be much smaller than P, while VNP seems of have computational powers much stronger than that of NP. Thus, it seems like solving the question of VP $\neq$ VNP must precede solving the question of P $\neq$ NP.

Another question that Algebraic Complexity tries to answer is that of Polynomial Identity Testing (or PIT). Given an algebraic circuit $\mathcal{C}$, we want to check whether the polynomial computed by it is identically zero or not. This is one of the simplest questions one would want to ask about a given circuit, and yet answering this deterministically turns out to be hard.

This was "justified" by providing strong connection between PITs and lower bounds in algebraic circuits, as shown by Kabanets-Impagliazzo [KI03], Heintz-Schnor [HS80], Agrawal [Agr05] and Dvir-Shpilka-Yehudayoff [DSY08]. In fact, Agrawal [Agr11] showed that under some structural assumptions on the PIT, a strong enough result will separate VP from VNP.

To understand the PIT question a little better, we first define what an algebraic circuit is. Suppose one wants to draw a pictorial representation of computing a polynomial. How would one do it? The picture that should come to your mind is exactly what an arithmetic circuit looks like. Formally,

Definition 1.0.1. *An arithmetic circuit is a DAG with the leaves being the input nodes labelled by either variables or field elements. Each edge is labelled by a field element and each non-leaf node is labelled by a "+" or a "×". Each gate and each edge computes a polynomial. The leaves compute the polynomial corresponding to its label. Each edge computes the polynomial equal to its label times the polynomial computed by the node it is coming out of. Each + gate computes the sum of the polynomials computed by the incoming edges, and each × computes the product of the polynomials computed by its incoming edges. The polynomials computed at the nodes with no out-going edges are the polynomials computed by the circuit.* ◊

There are two kinds of PIT questions that can arise depending on what kind of access we have to the circuit. If we are allowed to actually look at the circuit — more formally, if we are allowed to query how the nodes and wires are connected — then the task of checking whether the circuit outputs the identically zero polynomial is called "white-box" PIT. Note that one cannot afford to expand the entire polynomial computed by the circuit as there might be super-polynomially many monomials.

On the other hand, if we are only allowed evaluation access — that is, if we are only allowed to check whether the circuit evaluates to zero or not at points of our choice — then checking if the circuit outputs the identically zero polynomial is called "black-box" PIT. Note that in this case, all that one can essentially do is evaluate the circuit on a small set of points which is guaranteed to have the property that every non-zero circuit produces at least one non-zero evaluation in this set. Such a set of points is called a hitting set.

It is important to note that PIT has a trivial randomized algorithm because of the Schwartz-Zippel Lemma [Sch80], [Zip79], [DL78]. Thus, all of the research in PIT is basically about trying to de-randomise the Schwartz-Zippel test. We do not have a sub-exponential time PIT for general circuits yet. However, there have been progress for restricted classes like depth-2 circuits - [KS01], [AB99]; depth-3 powering circuits - [Kay10; Sax08], [ASS12], [FS13]; non-commutative ABPs - [FS13], [GKS16]; depth-3 circuits with constant top fan-in - [KS07], [DS05; SS09; KS09; SS10], [SS11]; depth-4 multilinear circuits with constant top fan-in - [SV11]; $\Sigma \wedge \Sigma\Pi$ - circuits with constant bottom fan-in - [Kay12].

Another important point to note is that, just like lowerbounds, PITs seem to be difficult for even general depth-3 and depth-4 circuits. The reason for this can be explained by the depth reduction results. Agrawal-Vinay (later simplified by Koiran, Tavenas) [AV08; Koi12; Tav15] show that polynomial time black-box PITs for structured depth-4 circuits will imply quasi-poly time PITs for general circuits. Similarly Gupta-Kamath-Kayal-Saptharishi [GKKS13] show that polynomial time black-box PITs for depth-3 circuits, over characteristic zero fields, will imply quasi-poly time PITs for general circuits.

1.1 Unifying PIT Approaches

Although progress has been made in the PIT question for various restricted classes of circuits, each result seems to depend on the restriction assumed. So, the natural question would be whether there is a unifying approach for most (if not all) of these PIT results. Agrawal-Saha-Saptharishi-Saxena [ASSS12] gave a unified approach to PITs for depth-2 circuits, depth-3 circuits with constant top fan-in, depth-4 multilinear circuits with constant top fan-in among others. They do so via the concepts of "algebraic independence" and the "Jacobian", which were introduced by Beecken-Mittman-Saxena [BMS11]. However, the approach works only over fields of characteristic zero.

To understand the reason, we must understand the heart of their technique. A set of polynomials $f_1, f_2, \ldots, f_m \in \mathbb{F}[x_1, x_2, \ldots, x_n]$ is said to be algebraically independent over $\mathbb{F}$ iff there is no non-zero polynomial $A \in \mathbb{F}[y_1, y_2, \ldots, y_m]$ such that $A(f_1, f_2, \ldots, f_m) = 0$. Now one can prove that the family of all algebraically independent subsets of $\{f_1, f_2, \ldots, f_m\}$ forms a matroid [Oxl06]. Hence the size of maximal algebraically independent subsets of $\{f_1, f_2, \ldots, f_m\}$ is well-defined and this quantity is called the *algebraic rank* of $\{f_1, f_2, \ldots, f_m\}$ (denoted by $\mathsf{algrank}(f_1, f_2, \ldots, f_m)$).

The connection between algebraic independence and PIT stems from the concept of faithful maps. Given a set of polynomials $\{f_1, f_2, \ldots, f_k\}$, a linear map

$$\varphi : \{x_1, x_2, \ldots, x_n\} \to \{y_1, y_2, \ldots, y_k\}$$

is said to be faithful if $\{\varphi(f_1), \varphi(f_2), \ldots, \varphi(f_k)\}$ has the same rank as $\{f_1, f_2, \ldots, f_m\}$. The connection is established in this crucial lemma.

Lemma 1.1.1. *Suppose $f_1, f_2, \ldots, f_m \in \mathbb{F}[x_1, x_2, \ldots, x_n]$ and φ is a faithful map. Then, for any circuit $C(z_1, \ldots, z_m)$,*

$$C(f_1, f_2, \ldots, f_m) = 0 \Leftrightarrow \varphi\left(C(f_1, f_2, \ldots, f_m)\right) = 0$$

Note that in this lemma, there is no assumption on the characteristic of the field and [BMS11] used it to show PIT results for some classes. For bounded degree circuits they gave a PIT over arbitrary fields. However, the dependency on the degree is huge. For the restricted case of sparse polynomials over characteristic zero fields, they were able to construct faithful maps using the Jacobian matrix to give much better PITs.

For the polynomials $f_1, f_2, \ldots, f_m \in \mathbb{F}[x_1, x_2, \ldots, x_n]$, the Jacobian matrix $\mathbf{J}_x(\mathbf{f})$, for $\mathbf{f} = (f_1, f_2, \ldots, f_m)$ is defined as follows.

$$\mathbf{J}_x(\mathbf{f}) = (\partial_{x_i}(f_j))_{i\in[n],j\in[m]} = \begin{bmatrix} \partial_{x_1}(f_1) & \partial_{x_1}(f_2) & \ldots & \partial_{x_1}(f_m) \\ \partial_{x_2}(f_1) & \partial_{x_2}(f_2) & \ldots & \partial_{x_2}(f_m) \\ \vdots & \vdots & \ddots & \vdots \\ \partial_{x_n}(f_1) & \partial_{x_n}(f_2) & \ldots & \partial_{x_n}(f_m) \end{bmatrix}$$

Given polynomials $f_1, f_2, \ldots, f_m \in \mathbb{F}[x_1, x_2, \ldots, x_n]$, suppose it is known that the algebraic rank of $\{f_1, f_2, \ldots, f_m\} = k$. Further, suppose $\mathbb{H}$ be a hitting set for $\tilde{\mathbf{J}}$, the set of all $k \times k$ minors in $\mathbf{J}$. If $\mathbb{F}$ has characteristic zero, then [BMS11] proved that at least one of the following maps will be faithful for $\{f_1, f_2, \ldots, f_m\}$.

$$\left\{ \varphi : x_i \to \sum_{j=1}^{k} t^{ij} y_k + a_i \ : \ \mathbf{a} = (a_1, a_2, \ldots, a_n) \in \mathbb{H} \right\}.$$

However, the proof depended heavily on the Jacobian Criterion which requires the field to have characteristic zero.

Theorem 1.1.2. *If $\mathbb{F}$ is a field of characteristic zero, then $f_1, f_2, \ldots, f_m \in \mathbb{F}[\mathbf{x}]$ are algebraically independent if and only if for $\mathbf{f} = f_1, f_2, \ldots, f_m$, $\mathbf{J}_x(\mathbf{f})$ has full rank.*

[ASSS12] then used this technique to give PITs for more general classes over characteristic zero fields. Recently however, Pandey-Saxena-Sinhababu [PSS16] came up with a Jacobian-like criterion over fields of abitrary characteristic.

Theorem 1.1.3. *Let $\{f_1, f_2, \ldots, f_m\}$ be a set of n-variate polynomials over a field $\mathbb{F}$. They are algebraically independent iff for a random $\mathbf{z} \in \mathbb{F}^n$, $\{\mathcal{H}_t(f_1), \ldots, \mathcal{H}_t(f_m)\}$ are linearly independent in $\frac{\mathbb{F}(\mathbf{z})[x_1,x_2,\ldots,x_n]}{\langle \mathcal{H}_t(f_1),\ldots,\mathcal{H}_t(f_m)\rangle^{\geq 2}_{\mathbb{F}(\mathbf{z})} + \langle x_1,x_2,\ldots,x_n\rangle^{t+1}}$, where t is the inseparable degree of $\{f_1, f_2, \ldots, f_m\}$.*

We will understand what this criterion says later, but intuitively it reduces the question of finding algebraic rank of a set of polynomials to finding the linear rank of a matrix. This is very similar to what the Jacobian Criterion says and so it motivated us to construct faithful maps even over fields that have finite characteristic.

1.2 Our Contribution and Future Directions

Extending the ideas from the zero characteristic case, we have been able to use the [PSS16] criterion to construct faithful maps over arbitrary fields. Formally, we prove the following theorem.

Theorem 1.2.1. *Given a set of polynomials* $\{f_1, f_2, \ldots, f_m\} \in \mathbb{F}[x_1, x_2, \ldots, x_n]$ *with constant inseparable degree, there exists a* $\mathrm{poly}(n)$ *sized family of linear maps* Φ *such that for some* $\varphi \in \Phi$,

$$\mathsf{algrank}(f_1, f_2, \ldots, f_m) = \mathsf{algrank}(f_1(\varphi, \ldots, f_m(\varphi))).$$

This allows us to extend the sparse polynomial PIT presented in [BMS11] to fields of arbitrary characteristic. Formally, we show that if $\{f_1, f_2, \ldots, f_m\} \in \mathbb{F}[x_1, x_2, \ldots, x_n]$ is a set of sparse polynomials with bounded transcendence degree, and bounded inseparable degree, then there is a $\mathrm{poly}(n)$ time PIT for $\mathcal{C}(f_1, f_2, \ldots, f_m)$.

Similarly, we hope to extend the PIT results in [ASSS12] to fields of arbitrary characteristic. Another question we would like to look into is whether the [PSS16] criterion can be made feasible even for unbounded inseparable degree.

1.3 Structure of the Thesis

We begin the thesis with the study of Algebraic Independence. The two main results in chapter 2 are that the set of algebraically independent subsets form a matroid, and that computing the annihilating polynomial for a given set of polynomials is "hard". Chapter 3 focuses on proving the Jacobian Criterion for fields of characteristic zero. Continuing this thread, chapter 4 presents the recent result of [PSS16] which proves a Jacobian-like criterion for fields of finite characteristic. Chapter 5 deals with the connection between algebraic independence and PITs. In this chapter, we also see how to construct "faithful maps" over fields of characteristic zero. Finally, chapter 6 is devoted to constructing faithful maps over fields of finite characteristic and extending the sparse polynomial PIT result in [BMS11] to arbitrary fields in the case that a parameter called "inseparable degree" is constant.

2 Algebraic Independence

The central concept that was used in [ASSS12] while trying to unify the PIT approaches, as we saw, was Algebraic Independence. Thus before going any further, we develop some intuition about algebraically independent polynomials and look at a few tools that will help us work with them.

2.1 The Definition and a few useful Properties

Let $\mathbb{F}$ be a field and $\mathbb{K}$ be an extension field of $\mathbb{F}$. Further, let $\{f_1, f_2, \ldots, f_m\} \subseteq \mathbb{K}$. Then, $g \in \mathbb{K}$ is said to be algebraically dependent on $\{f_1, f_2, \ldots, f_m\}$ over $\mathbb{F}$ if g is a root of some non-zero polynomial $A \in \mathbb{F}[f_1, f_2, \ldots, f_m][x]$.

That is, g is algebraically dependent on $\{f_1, f_2, \ldots, f_m\}$ over $\mathbb{F}$ if

$$a_0(f_1, f_2, \ldots, f_m)g^k + a_1(f_1, f_2, \ldots, f_m)g^{k-1} + \cdots + a_k(f_1, f_2, \ldots, f_m) = 0$$

where $a_i \in \mathbb{F}[f_1, f_2, \ldots, f_m]$ for every i and at least one a_i is non-zero. If this is not the case, then g is said to be algebraically independent of $\{f_1, f_2, \ldots, f_m\}$ over $\mathbb{F}$.

A finite subset T of $\mathbb{K}$ is algebraically independent over $\mathbb{F}$ if for every $t \in T$, the element t is algebraically independent of $T \setminus \{t\}$ over $\mathbb{F}$.

It can easily be shown that the above definition is equivalent to the following one in the special case of $\mathbb{K} = \mathbb{F}[x_1, x_2, \ldots, x_n]$, and it is this that we will be working with.

Definition 2.1.1. *A non-empty set $\{f_1, f_2, \ldots, f_m\} \subseteq \mathbb{F}[x_1, x_2, \ldots, x_n]$ is said to be algebraically independent over $\mathbb{F}$ if there is no non-zero polynomial $A \in \mathbb{F}[y_1, y_2, \ldots, y_m]$ such that $A(f_1, f_2, \ldots, f_m) = 0$.*

Otherwise, $\{f_1, f_2, \ldots, f_m\}$ is said to be algebraically dependent and the non-zero polynomial $A \in \mathbb{F}[y_1, y_2, \ldots, y_m]$ for which $A(f_1, f_2, \ldots, f_m) = 0$ is called the annihilating polynomial for $\{f_1, f_2, \ldots, f_m\}$. ◊

We will now look at a few properties, without proof, that will be used later. [Oxl06] is an excellent reference if one wants to see the proofs.

Lemma 2.1.2. *Let $g, f_1, f_2, \ldots, f_m \in \mathbb{F}[x_1, x_2, \ldots, x_n]$. If g is algebraically dependent on $\{f_1, f_2, \ldots, f_m\}$, but not on $\{f_1, f_2, \ldots, f_{m-1}\}$, then f_m is algebraically dependent on $\{f_1, f_2, \ldots, f_{m-1}, g\}$.*

Sketch of Proof. View the annihilating polynomial as a polynomial in f_m. □

Lemma 2.1.3. *Suppose g is algebraic over $\mathbb{F}(t)$ and t is algebraic over $\mathbb{F}$. Then g is algebraic over $\mathbb{F}$.*

Sketch of Proof. $\mathbb{F}(t)(g)$ over $\mathbb{F}(t)$ and $\mathbb{F}(t)$ over $\mathbb{F}$ are finite-dimensional. □

Lemma 2.1.4. *If g is algebraically dependent on $\{f_1, f_2, \ldots, f_n\}$ and each f_i is algebraically dependent on $\{u_1, u_2, \ldots, u_k\}$, then g is algebraically dependent on $\{u_1, u_2, \ldots, u_k\}$.*

Sketch of Proof. Induction and Lemma 2.1.3 □

Corollary 2.1.5. *Let T and U be finite subsets of polynomials over field $\mathbb{F}$ and further, let U be algebraically independent over $\mathbb{F}$. Then:*

1. *If every element of T is algebraic over $\mathbb{F}$, then U is algebraically independent over $\mathbb{F}(T)$.*
2. *$T \cup U$ is algebraically independent over $\mathbb{F}$ iff T is algebraically independent over $\mathbb{F}(U)$.*

2.2 The Matroid Property

Algebraic Independence and Linear Independence differ in many respects. One of the main points of difference is that if $\{l_1, l_2, \ldots, l_m\}$ are linearly dependent, then there is always some l_i which can be written as a linear combination of the others in the set. However, if $\{f_1, f_2, \ldots, f_m\}$ is a set of algebraically dependent polynomials, then there is no guarantee that there is some f_i which can be written as a polynomial combination of the other polynomials in the set.

However, they do have some property in common, namely the matroid property.

Definition 2.2.1. *$M = (E, \mathcal{I})$ is said to be a* matroid *if E is a finite set and $\mathcal{I}$ satisfies:*

- *Closure under subsets: $I \in \mathcal{I}$ and $J \subseteq I \Rightarrow J \in \mathcal{I}$*
- *Augmentation Property: $I, J \in \mathcal{I}$ and $|I| < |J| \Rightarrow \exists x \in J$ s.t. $I \cup \{x\} \in \mathcal{I}$*

◊

With this definition, we have the following theorem.

Theorem 2.2.2. *Suppose E is a finite subset of polynomials over some field $\mathbb{F}$. Then, $M = (E, \mathcal{I})$ is a matroid where $\mathcal{I}$ is the collection of subsets of E that are algebraically independent over $\mathbb{F}$.*

Before going into the proof, let us take inspiration from the concept of linear span of a set of vectors, and define the algebraic span of a set of polynomials.

Definition 2.2.3. *Let $\{f_1, f_2, \ldots, f_m\} \in \mathbb{F}[\mathbf{x}]$. The algebraic span of $\{f_1, f_2, \ldots, f_m\}$ denoted by $\mathsf{algspan}(f_1, f_2, \ldots, f_m)$ is the set of all $g \in \mathbb{F}[\mathbf{x}]$ that are algebraically dependent on $\{f_1, \ldots, f_m\}$* ◊

It is easy to see that the algebraic span shares a couple of simple properties with its linear algebraic counterpart.

Lemma 2.2.4. *Let $A \subseteq \mathbb{F}[\mathbf{x}]$. Then*

1. *clearly, $A \subseteq \mathsf{algspan}(A)$ and*
2. *by Lemma 2.1.4, if $A' \subseteq \mathsf{algspan}(A)$ and $B \subseteq \mathsf{algspan}(A')$, then, $B \subseteq \mathsf{algspan}(A)$.*

We are now ready to see the proof of why algebraic independence has the matroid property. As expected, it will closely follow the proof of why linear independence has the matroid property.

Proof of Theorem 2.2.2. We have to check whether $\mathcal{I}$ satisfies the two matroid properties.

1. Clearly from the definition of Algebraic Independence, if $I_1 \subseteq I_2$ and $I_2 \in \mathcal{I}$, then $I_1 \in \mathcal{I}$.
2. Let $I_1, I_2 \in \mathcal{I}$ and $|I_1| < |I_2|$. We need to find $a \in I_2 \setminus I_1$ such that $I_1 \cup \{a\} \in \mathcal{I}$.

   Assume that no such a exists. Then, for every $a \in I_2 \setminus I_1$, a is algebraically dependent on I_1. That is, $I_2 \setminus I_1 \subseteq \mathsf{algspan}(I_1)$.

   Let $I_1 = \{x_1, x_2, \ldots, x_n\}$, and $I_2 \setminus I_1 = \{y_1, \ldots, y_k\}$. Note that $I_2 \setminus I_1$ or any subset of it will be algebraically independent. However, $\{y_1, x_1, x_2, \ldots, x_n\}$ is dependent and in fact, there is a $j_1 \in [n]$ such that x_{j_1} is dependent on $\{y_1, x_1, \ldots, x_{j_1-1}\}$ (start with $\{y_1\}$ and keep adding x_is into the set in order, till you find x_{j_1} with the required property).

   Let $A_1 = \{y_1\} \cup \left(I_1 \setminus \{x_{j_1}\}\right)$. Then, $I_1 \subseteq \mathsf{algspan}(A_1)$ and so by Lemma 2.2.4, $I_2 \setminus I_1 \subseteq \mathsf{algspan}(A_1)$. Thus, $\{y_2, y_1, x_1, \ldots, x_{j_1-1}, x_{j_1+1}, \ldots, x_n\}$ is algebraically dependent. Now, as $\{y_2, y_1\}$ is algebraically independent, by the same procedure as before we will get a j_2 such that x_{j_2} is dependent on the previous terms and we can define A_2 as $\{y_1, y_2\} \cup \left(I_1 \setminus \{x_{j_1}, x_{j_2}\}\right)$ with $I_2 \setminus I_1 \subseteq \mathsf{algspan}(A_2)$.

   Continuing like this, if we have $A_{k-1} = \{y_1, y_2, \ldots, y_{k-1}\}$, then we get $I_2 \setminus I_1 \subseteq \mathsf{algspan}(A_{k-1})$ which contradicts the fact that $I_2 \setminus I_1$ is algebraically independent. Thus, our assumption must be wrong and there must exist $a \in I_2 \setminus I_1$ such that $I_1 \cup \{a\} \in \mathcal{I}$, completing the proof. □

Before we conclude this section, it would be good to note that due to the matroid property, any maximal algebraically independent subset of $\{f_1, f_2, \ldots, f_m\}$ must have the same size. Thus we can define the algebraic rank and algebraic basis of a set of polynomials.

Definition 2.2.5. *For any set of polynomials $\{f_1, f_2, \ldots, f_m\} \subseteq \mathbb{F}[\mathbf{x}]$, its algebraic rank or transcendence rank denoted by $\mathsf{algrank}(f_1, f_2, \ldots, f_m)$ is the size of a maximal algebraically independent subset.*

Any maximal algebraically independent subset of $\{f_1, f_2, \ldots, f_m\}$ is said to be a transcendence basis for it. ◊

2.3 Computing the Annihilating polynomial is Hard

One natural question that comes to mind after one learns about Algebraic Independence is, "How does one check if a given set of polynomials is algebraically independent?". The most natural answer would be to try and find, if there exists one, an annihilating polynomial for the given set of polynomials. However, it was shown by Kayal [Kay09] that this is hard.

Definition 2.3.1. *Let* ANNIHILATING-AT-ZERO *denote the following decision problem: Given a set of polynomials $\{f_1, f_2, \ldots, f_m\} \subseteq \mathbb{F}[x_1, x_2, \ldots, x_n]$ of algebraic rank $m-1$, that has a minimal annihilating polynomial $A(y_1, y_2, \ldots, y_m)$, determine if $A(0, \ldots, 0) = 0$.* ◊

Definition 2.3.2. *Let* ANNIHILATING-EVALUATION *denote the functional problem of evaluating the annihilating polynomial at a given point. The input consists of a set of polynomials $\{f_1, f_2, \ldots, f_m\} \in \mathbb{Z}[x_1, x_2, \ldots, x_n]$ with its minimal monic annihilating polynomial as $A(y_1, y_2, \ldots, y_m) \in \mathbb{Z}[y_1, y_2, \ldots, y_m]$, and a prime p. The output is the integer $A(0, \ldots, 0) \pmod p$.* ◊

Theorem 2.3.3. *Following the above definitions,*

1. ANNIHILATING-AT-ZERO *is* NP*-hard*
2. ANNIHILATING-EVALUATION *is* #P*-hard*

Although we will not see the proof of Theorem 2.3.3 here, we will see a proof of the surprising theorem that it crucially depends on. Before that however, we will state a few properties of the annihilating polynomial without proof. All of these were observed in [Kay09], and the interested reader may find the proofs in the same.

Definition 2.3.4. *Let $f_1, f_2, \ldots, f_m \in \mathbb{F}[x_1, x_2, \ldots, x_n]$. $A \in \mathbb{F}[y_1, y_2, \ldots, y_m]$ is said to be an* **f***-annihilating polynomial if $A(y_1, y_2, \ldots, y_m) \neq 0$ but $A(f_1, f_2, \ldots, f_m) = 0$.* ◊

Theorem 2.3.5. *Let $f_1, f_2, \ldots, f_m \in \mathbb{F}[x_1, x_2, \ldots, x_n]$ be a set of algebraically dependent polynomials, no proper subset of which is algebraically dependent. Then, the ideal of* **f***-annihilating polynomials is generated by a single irreducible polynomial $A(\mathbf{y})$ that continues to remain irreducible over $\overline{\mathbb{F}}$. Further, $A(\mathbf{y})$ remains the minimal annihiating polynomial of $\{f_1, f_2, \ldots, f_m\}$ when they are viewed as polynomials over $\overline{\mathbb{F}}$.*

Theorem 2.3.6. *Let $\mathbf{f} = \{f_1, f_2, \ldots, f_m\}$ be a set of degree d polynomials over n variables. Then there is an* **f***-annihilating polynomial of degree $\leq D = (r+1)d^r$.*

Theorem 2.3.7. *If $\mathbb{F}$ has characteristic zero, and $d \in \mathbb{N}$, then there is a set of polynomials $\{f_1, \ldots, f_n, g\} \in \mathbb{F}[x_1, x_2, \ldots, x_n]$ of degree $\leq d$ and algebraic rank n such that the minimal annihilating polynomial has degree $\geq d^n$.*

We will now work our way towards the theorem that is used in the proof of Theorem 2.3.3, namely Theorem 2.3.11. It says that under some restrictions on the polynomials $f_1, f_2, \ldots, f_m \in \mathbb{F}[x_1, x_2, \ldots, x_n]$, the characteristic polynomial of some linear operator is always a power of the annihilating polynomial for $\{f_1, f_2, \ldots, f_m, g\}$ where g can be any polynomial in $\mathbb{F}[x_1, x_2, \ldots, x_n]$.

Before going into that however, we state the useful Hilbert's Nullstellensatz theorem. Its proof can be found in any basic algebraic geometry text (eg. [CLO97]).

Lemma 2.3.8. *(Hilbert's Nullstellensatz) Let $f, g \in \overline{\mathbb{F}}^n[x_1, x_2, \ldots, x_n]$ and g be $\overline{\mathbb{F}}$-irreducible. If every root of $f(x_1, x_2, \ldots, x_n)$ in $\overline{\mathbb{F}}^n$ is also a root of $g(x_1, x_2, \ldots, x_n)$, then $\exists t \in \mathbb{N}$ such that $f(x_1, x_2, \ldots, x_n) = g(x_1, x_2, \ldots, x_n)^t$.*

We are now ready to state and prove Theorem 2.3.11. The proof of its second part as presented here, is different from that in [Kay09].

Definition 2.3.9. *Let $R \supseteq \mathbb{F}$ be a ring whose elements form a finite-dimensional vector space over $\mathbb{F}$. Then, for every $\alpha \in R$, $\varphi_\alpha : R \to R$ defined by $\varphi_\alpha(r) = r.\alpha$, is a linear transformation on this vector space. Define*

$$\mathsf{charpoly}_\alpha(z) \in \mathbb{F}[z]$$

to be the characteristic polynomial of φ_α. ◊

Lemma 2.3.10. *Let $f_1, f_2, \ldots, f_m \in \mathbb{F}[x_1, x_2, \ldots, x_n]$ be a set of algebraically dependent polynomials with annihilating polynomial $A \in \mathbb{F}[y_1, y_2, \ldots, y_m]$. If they have a common root in $\overline{F}^n$, then $A(0, 0, \ldots, 0) = 0$.*

Proof. Let the common root of $f_1, f_2, \ldots, f_m$ be $\mathbf{a} \in \mathbb{F}^n$. As A is the annihilating polynomial, $A(0, 0, \ldots, 0) = A(\mathbf{f}(\mathbf{a})) = A(\mathbf{f}(a_1, a_2, \ldots, a_n)) = 0$. □

Theorem 2.3.11. *For each $i \in [n]$, let $f_i(x_1, \ldots, x_i) \in \mathbb{F}[x_1, \ldots, x_i]$. Suppose further that f_i when viewed as a member of $\mathbb{F}(x_1, \ldots, x_{i-1})[x_i]$ is monic. Then, for any $g \in \mathbb{F}[x_1, x_2, \ldots, x_n]$, if $r \in \mathbb{F}(v_1, \ldots, v_n)[u]$ is defined as*

$$r(v_1, \ldots, v_n, u) = \mathsf{charpoly}_{g(x) \bmod (f_1 - v_1, f_2 - v_2, \ldots, f_n - v_n)}(u),$$

then:

- $\mathsf{algrank}(f_1, \ldots, f_n, g) = n$
- $r(v_1, \ldots, v_n, u)$ *is a power of annihilating polynomial for* $\{f_1, f_2, \ldots, f_n, g\}$.

Proof. First, we show that $\{f_1, f_2, \ldots, f_n, g\}$ has algebraic rank n by showing that $\{f_1, f_2, \ldots, f_n\}$ is an algebraically independent set. Note that showing this would be enough as this proves $\mathsf{algrank}(f_1, f_2, \ldots, f_n, g) \geq n$ which together with the fact that $\{f_1, f_2, \ldots, f_n, g\} \in \mathbb{F}[x_1, x_2, \ldots, x_n]$ proves that $\mathsf{algrank}(f_1, f_2, \ldots, f_n, g) = n$.

We prove that $\{f_1, f_2, \ldots, f_n\}$ is algebraically independent using induction. Clearly $\{f_1\}$ is an algebraically independent set. So for the induction hypothesis, assume that $\{f_1, \ldots, f_i\}$ is an algebraically independent set. Now, if we assume that the set $\{f_1, f_2, \ldots, f_{i+1}\}$ is algebraically dependent, we have:

Case 1: f_{i+1} **is algebraically dependent on** $\{f_1, \ldots, f_i\}$

Let $A \in \mathbb{F}(f_1, \ldots, f_i)[x]$ be the annihilating polynomial. Then, $A[x] \neq 0$ but $A(f_{i+1}) = 0$. Thus, for every $j \in \{0, 1, \ldots, k\}$, $A_j = 0$ where

$$A(f_{i+1}) = \sum_{j=0}^{k} A_j x_{i+1}^j \text{ and } k \text{ is the highest power of } x_{i+1} \text{ in } A(f_{i+1}).$$

Now, note that $A_k \in \mathbb{F}(f_1, \ldots, f_i)$ and thus $A_k = 0$ contradicts the fact that $\{f_1, \ldots, f_i\}$ is an algebraically independent set.

Case 2: f_j **is algebraically dependent on** $\{f_1, \ldots, f_{j-1}, f_{j+1}, \ldots, f_{i+1}\}$ **for** $j \neq i+1$

We note that by the induction hypothesis, f_j is algebraically dependent on $\{f_1, \ldots, f_{j-1}, f_{j+1}, \ldots, f_{i+1}\}$ but not on $\{f_1, \ldots, f_{j-1}, f_{j+1}, \ldots, f_i\}$. Thus, we are in Case 1 by Lemma 2.1.2.

Thus, the assumption that $\{f_1, f_2, \ldots, f_{i+1}\}$ is an algebraically dependent is wrong and so by the Principle of Mathematical Induction, $\{f_1, f_2, \ldots, f_n\}$ is an algebraically independent set.

Next, we show that $r(v_1, v_2, \ldots, v_n, u)$ is a power of the annihilating polynomial for $\{f_1, f_2, \ldots, f_n, g\}$, say $A(v_1, v_2, \ldots, v_n, u)$. Note that by Theorem 2.3.5, we can assume that $\mathbb{F} = \overline{\mathbb{F}}$ and thus, by Lemma 2.3.8, it is enough to show the following:

Claim 2.3.12. *If* $(b_1, b_2, \ldots, b_n, a) \in \mathbb{F}^{n+1}$ *is a root of* $r(v_1, v_2, \ldots, v_n, u)$*, then it is also a root of* $A(v_1, v_2, \ldots, v_n, u)$.

Indeed, $A(v_1, v_2, \ldots, v_n, u)$ is the annihilating polynomial for $\{f_1, f_2, \ldots, f_n, g\}$ iff $A(v_1 + b_1, \ldots, v_n + b_n, u + a)$ is the same for $\{f_1 - b_1, \ldots, f_n - b_n, g - a\}$. Thus, without loss of generality we can assume $(b_1, b_2, \ldots, b_n, a) = (0, 0, \ldots, 0, 0)$.

Now by Lemma 2.3.10, it is enough to show that $\{f_1, f_2, \ldots, f_n, g\}$ have a common root. So, let us assume that this is not true.

Then,

$$\begin{aligned}
&\{f_1, f_2, \ldots, f_n, g\} \text{ does not have a common root} \\
&\Rightarrow \langle f_1, f_2, \ldots, f_n, g\rangle = \mathbb{F}[x_1, x_2, \ldots, x_n] \\
&\Rightarrow 1 \in \langle f_1, f_2, \ldots, f_n, g\rangle \\
&\Rightarrow f \in \langle f_1 f, f_2 f, \ldots, f_n f, gf\rangle \text{ for every } f \\
&\Rightarrow f \in \langle f_1, f_2, \ldots, f_n, gf\rangle \text{ for every } f
\end{aligned}$$

where $\langle f_1, f_2, \ldots, f_k\rangle$ denotes the ideal generated by $f_1, f_2, \ldots, f_k$.

Note that we are working in the ring $R = \frac{\mathbb{F}[x_1, x_2, \ldots, x_n]}{\langle f_1, f_2, \ldots, f_n\rangle}$, where for the given g, we are looking at the linear operator

$$\Phi_g : R \to R \text{ given by } \Phi_g(p) = gp \bmod (f_1, f_2, \ldots, f_n)$$

and defining r to be the characteristic polynomial of this operator. Further, we are assuming that $r(0, 0, \ldots, 0, 0) = 0$ and so, 0 is an eigen value of Φ_g which would mean that $\exists f \notin \langle f_1, f_2, \ldots, f_n\rangle$ such that $gf \in \langle f_1, f_2, \ldots, f_n\rangle$, say f_0.

However, by our assumption, for every f, $f \in \langle f_1, f_2, \ldots, f_n, gf\rangle$ and so for f_0,

$$f_0 \in \langle f_1, f_2, \ldots, f_n, gf_0\rangle \subseteq \langle f_1, f_2, \ldots, f_n\rangle .$$

This is a contradiction and thus, $\{f_1, f_2, \ldots, f_n, g\}$ must have a common root. □

Since now we know that computing the annihilating polynomial is hard, we are back to the question of how one can check whether a given set of polynomials is algebraically independent. This was answered a long time back by Jacobi [Jac41] for fields that have characteristic zero.

3 The Jacobian Criterion

Given polynomials $f_1, f_2, \ldots, f_m \in \mathbb{F}[x_1, x_2, \ldots, x_n]$, we want to check whether they are algebraically independent. As we have already seen, trying to compute its annihilating polynomial is hard. However, over fields of characteristic zero, Jacobi had shown that there is an equivalent criterion that is easy to check. Before going into the criterion though, we need to go over a few preliminary definitions.

3.1 Partial Derivatives and the Jacobian

First we define partial derivatives for polynomials and see a few of their properties. Note that these are to be treated as syntactic definitions.

Partial Derivative of Univariate Polynomials

If $f \in \mathbb{F}[x]$ can be written as

$$f = a_m x^m + a_{m-1} x^{m-1} + \ldots + a_1 x + a_0$$

then

$$\frac{\partial f}{\partial x} = (m a_m) x^{m-1} + ((m-1) a_{m-1}) x^{m-2} + \ldots + (2a_2) x + a_1.$$

Partial Derivative of Multivariate Polynomials

Let $f \in \mathbb{F}[x_1, x_2, \ldots, x_n]$ be written as:

$$f = g_m x_i^m + a_{m-1} x_i^{m-1} + \ldots + a_1 x_i + a_0$$

where $g_i \in \mathbb{F}[x_1, \ldots, x_{i-1}, x_{i+1}, \ldots x_n]$ for all $0 \leq i \leq m$. Then,

$$\frac{\partial f}{\partial x_i} = (m g_m) x_i^{m-1} + ((m-1) g_{m-1}) x_i^{m-2} + \ldots + (2g_2) x_i + g_1$$

The Chain Rule

Let $F \in \mathbb{F}[y_1, y_2, \ldots, y_m]$ and $f_1, f_2, \ldots, f_m \in \mathbb{F}[x_1, x_2, \ldots, x_n]$. Then,

$$\frac{\partial F}{\partial x_i} = \sum_{j=1}^{m} \frac{\partial F}{\partial y_j}(f_1(\mathbf{x}), f_2(\mathbf{x}), \ldots, f_m(\mathbf{x})).\frac{\partial f_j(\mathbf{x})}{\partial x_i} = \sum_{j=1}^{m} \frac{\partial F}{\partial y_j}(\mathbf{f}(\mathbf{x})).\frac{\partial f_j(\mathbf{x})}{\partial x_i}$$

where $\mathbf{f} = (f_1, f_2, \ldots, f_m)$ and $\mathbf{x} = (x_1, x_2, \ldots, x_n)$.

Partial Derivatives being zero

Let $f \in \mathbb{F}[x_1, x_2, \ldots, x_n]$. If $\mathbb{F}$ has characteristic zero, then

$$\forall i \in [n], \partial_{x_i} f = 0 \Leftrightarrow f \in \mathbb{F}[x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n]$$

and so

$$\forall i \in [n], \partial_{x_i} f = 0 \Leftrightarrow f \text{ is a constant function.}$$

However, if $\mathbb{F}$ has characteristic p, then

$$\forall i \in [n], \partial_{x_i} f = 0 \Leftrightarrow f \in \mathbb{F}[x_1, \ldots, x_{i-1}, x_i^p, x_{i+1}, \ldots, x_n]$$

and so

$$\forall i \in [n], \partial_{x_i} f = 0 \Leftrightarrow f \in \mathbb{F}[x_1^p, x_2^p, \ldots, x_n^p].$$

Thus, if $\mathbb{F}$ is a finite field with characteristic p, then

$$\forall i \in [n], \partial_{x_i} f = 0 \Leftrightarrow f = g^p \text{ for some } g \in \mathbb{F}[x_1, x_2, \ldots, x_n].$$

Next, we define the Jacobian and its property.

The Jacobian

If $f_1, f_2, \ldots, f_m \in \mathbb{F}[x_1, x_2, \ldots, x_n]$ and $\mathbf{f} = (f_1, f_2, \ldots, f_m)$, then the Jacobian matrix of $\mathbf{f}$ is given by

$$\mathbf{J_x}(\mathbf{f}) = (\partial_{x_i}(f_j))_{i\in[n], j\in[m]} = \begin{bmatrix} \partial_{x_1}(f_1) & \partial_{x_1}(f_2) & \ldots & \partial_{x_1}(f_m) \\ \partial_{x_2}(f_1) & \partial_{x_2}(f_2) & \ldots & \partial_{x_2}(f_m) \\ \vdots & \vdots & \ddots & \vdots \\ \partial_{x_n}(f_1) & \partial_{x_n}(f_2) & \ldots & \partial_{x_n}(f_m) \end{bmatrix}$$

Chain Rule for the Jacobian

If $f_1, f_2, \ldots, f_m \in \mathbb{F}[x_1, x_2, \ldots, x_n]$ and $F_1, F_2, \ldots, F_k \in \mathbb{F}[y_1, y_2, \ldots, y_m]$, then

$$\mathbf{J_x}(\mathbf{F}(\mathbf{f})) = (\mathbf{J_y}(\mathbf{F}))(\mathbf{f}).\mathbf{J_x}(\mathbf{f})$$

where $\mathbf{F} = (F_1, F_2, \ldots F_k)$ and $\mathbf{f} = (f_1, f_2, \ldots, f_m)$.

We are now ready to state and prove the Jacobian criterion.

3.2 The Criterion over Fields of Characteristic Zero

The criterion reduces the problem of checking algebraic independence of a set of polynomials to checking linear independence of a set of vectors, namely checking whether the Jacobian matrix has full rank. Formally the criterion is stated as follows.

Theorem 3.2.1. *If $\mathbb{F}$ is a field of characteristic zero, then $f_1, f_2, \ldots, f_m \in \mathbb{F}[x_1, x_2, \ldots, x_n]$ are algebraically independent if and only if $\mathbf{J}_{\mathbf{x}}(\mathbf{f})$ has full rank.*

We will prove the above theorem in two parts.

Theorem 3.2.2. *Let $\mathbb{F}$ be a field of characteristic zero and $\mathbf{J}_x(\mathbf{f})$ have full rank where $\mathbf{f} = (f_1, f_2, \ldots, f_m)$ and $f_1, f_2, \ldots, f_m \in \mathbb{F}[x_1, x_2, \ldots, x_n]$. Then, $\{f_1, f_2, \ldots, f_m\}$ are algebraically independent over $\mathbb{F}$.*

Proof. Assume $\{f_1, f_2, \ldots, f_m\}$ are algebraically dependent over $\mathbb{F}$. Then, there is a non-zero polynomial of minimum degree, say $A \in \mathbb{F}[y]$ such that $A(\mathbf{f}) = 0$. Taking partial derivative with respect to the x_is, we get for every i,

$$\frac{\partial A}{\partial x_i} = \sum_{j=1}^{m} \frac{\partial A}{\partial y_j}(\mathbf{f}(\mathbf{x})).\frac{\partial f_j}{\partial x_i} = 0$$

where $\mathbf{x} = (x_1, x_2, \ldots, x_n)$. Expanding it out, we get

$$\begin{bmatrix} \partial_{x_1}(f_1) & \partial_{x_1}(f_2) & \ldots & \partial_{x_1}(f_m) \\ \partial_{x_2}(f_1) & \partial_{x_2}(f_2) & \ldots & \partial_{x_2}(f_m) \\ \vdots & \vdots & \ddots & \vdots \\ \partial_{x_n}(f_1) & \partial_{x_n}(f_2) & \ldots & \partial_{x_n}(f_m) \end{bmatrix} \begin{bmatrix} \partial_{y_1} A(\mathbf{f}(\mathbf{x})) \\ \partial_{y_2} A(\mathbf{f}(\mathbf{x})) \\ \vdots \\ \partial_{y_m} A(\mathbf{f}(\mathbf{x})) \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}.$$

Now as $\mathbf{J}_{\mathbf{x}}(\mathbf{f})$ is full rank,

$$\begin{bmatrix} \partial_{y_1} A(\mathbf{f}(\mathbf{x})) \\ \partial_{y_2} A(\mathbf{f}(\mathbf{x})) \\ \vdots \\ \partial_{y_m} A(\mathbf{f}(\mathbf{x})) \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix},$$

and thus for every i, $\partial_{y_i} A(\mathbf{f}(\mathbf{x})) = 0$. However this would then imply that for every i, $\partial_{y_i} A = 0$ as otherwise we will contradict the fact that A is the minimum degree nonzero polynomial over $\mathbb{F}$ such that $A(\mathbf{f}(\mathbf{x})) = 0$.

Thus, for every i, $\partial_{y_i} A = 0$ and so, A is a constant function. However, as $A(\mathbf{f}) = 0$, it must be the case that $A \equiv 0$, which contradicts the fact that we started with A being a non-zero polynomial. Hence, our assumption must be wrong and $\{f_1, f_2, \ldots, f_m\}$ must be algebraically independent over $\mathbb{F}$. □

Note. The above proof goes through even if $\mathbb{F}$ is a finite field. As

$$\forall i \in [m], \partial_{y_i} A = 0 \Leftrightarrow A = F^p \text{ for some } F \in \mathbb{F}[y_1, y_2, \ldots, y_m],$$

if $A \neq 0$, then $F \neq 0$. If we denote $(f_1, f_2, \ldots, f_m)$ by $\mathbf{f}$ and $(y_1, y_2, \ldots, y_m)$ as $\mathbf{y}$, we have $F(\mathbf{y}) \neq 0$ but $F(\mathbf{f}) = 0$ which contradicts the fact that A is the minimum degree non-zero polynomial over $\mathbb{F}$ such that $A(\mathbf{f}) = 0$.

The opposite direction is given by the following theorem.

Theorem 3.2.3. *Let $\mathbb{F}$ be a characteristic zero field and $\{f_1, f_2, \ldots, f_m\} \subseteq \mathbb{F}[x_1, x_2, \ldots, x_n]$ be algebraically independent over $\mathbb{F}$. Then, $\mathbf{J}_{\mathbf{x}}(f_1, f_2, \ldots, f_m)$ has full rank.*

Proof. Let $\{f_1, f_2, \ldots, f_m\} \subseteq \mathbb{F}[x_1, x_2, \ldots, x_n]$ be algebraically independent. Then, by Theorem 2.2.2, we can assume that $\{f_1, f_2, \ldots, f_m, x_{m+1}, \ldots, x_n\}$ is algebraically independent over $\mathbb{F}$ (by reordering the x_is as required).

Define $f_k = x_k$ for $k \in \{m+1, \ldots, n\}$. Then, for every $i \in [n]$, $\{x_i, f_1, f_2, \ldots, f_n\}$ becomes dependent over $\mathbb{F}$ and so there will exist a non-zero polynomial $A_i \in \mathbb{F}[y_0, y_1, \ldots, y_n]$ such that $A_i(x_i, f_1, f_2, \ldots, f_n) = 0$. Note that $\deg_{y_0}(A_i) \neq 0$ and as $\mathbb{F}$ has characteristic zero, $\partial_{y_0}(A_i) \neq 0$.

Now for every j in $[n]$, if we differentiate A_i with respect to x_j, we get

$$\partial_{y_0}(A_i)(\mathbf{f}_i).\delta_{i,j} + \sum_{k=1}^{n} \partial_{y_k}(A_i)(\mathbf{f}_i).\partial_{x_j} f_k = 0$$

where $\mathbf{f}_i = (x_i, f_1, f_2, \ldots, f_n)$. Now as $\partial_{y_0}(A_i) \neq 0$ and A_i is the minimum degree annihilating polynomial for $\{\mathbf{f}_i\}$, $\partial_{y_0}(A_i)(\mathbf{f}_i) \neq 0$. Thus,

$$\sum_{k=1}^{n} \frac{-\partial_{y_k}(A_i)(\mathbf{f}_i)}{\partial_{y_0}(A_i)(\mathbf{f}_i)} \partial_{x_j} f_k = \delta_{i,j}.$$

In other words, there exists a matrix M such that

$$\mathbf{J}_{\mathbf{x}}(\mathbf{f})M = \mathbf{I}_n$$

where $\mathbf{f} = (f_1, f_2, \ldots, f_n)$ and

$$M_{i,j} = \frac{-\partial_{y_i}(A_j)(\mathbf{f}_j)}{\partial_{y_0}(A_j)(\mathbf{f}_j)}.$$

Thus, $\mathbf{J}_{\mathbf{x}}(\mathbf{f})$ has full rank and so in particular, $\mathbf{J}_x(f_1, f_2, \ldots, f_m)$ has full rank. □

Clearly, Theorem 3.2.2 and Theorem 3.2.3 together prove the Jacobian Criterion.

4 A Jacobian-like Criterion over Arbitrary fields

As we saw earlier, the Jacobian Criterion requires the field to have characteristic zero. A trivial example where the criterion fails would be $f = x^p \in \mathbb{F}_p[x]$. Clearly, $\{f\}$ is algebraically independent, but $\partial_x(f) = 0$. It is important to note however, that the criterion might fail even if polynomials are not from $\mathbb{F}[x_1^p, x_2^p, \ldots, x_n^p]$. For example, consider $f_1 = x^2y + x^3$, $f_2 = xy^2 + xy^5$ over $\mathbb{F}_3$. Then,

$$\mathbf{J}_{x,y} = \begin{bmatrix} 2xy + 3x^2 & x^2 \\ y^2 + y^5 & 2xy + 5xy^4 \end{bmatrix}.$$

Using the fact that $x^3 = x$ over $\mathbb{F}_3$, it is easy to see that $\mathbf{J}_{x,y}$ has rank 1 even though f_1, f_2 are algebraically independent over the said field.

Recently however, [PSS16] gave a criterion that will work over arbitrary fields. Before going into its statement, we require a few preliminary ideas.

4.1 The idea behind it

As noted before, Theorem 3.2.2 holds even when the field has finite characteristic. While trying to prove the other direction we used the fact that the characteristic was zero when we said that $\partial_{y_0} f \neq 0$ if $f \neq 0$. Clearly, this is not true if we work over finite characteristic fields. However, the next theorem says that we can make a similar statement even in this case if we work a little harder. This fact will be used crucially.

Theorem 4.1.1. *Let $\{f_1, f_2, \ldots, f_m\} \subseteq \mathbb{F}[x_1, x_2, \ldots, x_n]$ have algebraic rank k. If $\mathbb{F}$ is an algebraically closed field, then the f_is can be reordered in such a way that for every $i \in [m]$, the minimal annihilating polynomial of $\{f_i, f_1, f_2, \ldots, f_k\}$, say $A \in \mathbb{F}[y_0, y_1, y_2, \ldots, y_k]$, satisfies $\frac{\partial A}{\partial y_0} \neq 0$.*

We will not see the proof of this theorem here. The interested reader can take a look at [Kna07]. As mentioned before, the problem that we face while working with finite fields is that partial derivatives of non-zero polynomials might become zero. For this reason, we prefer to work with Hasse-derivatives instead.

Definition 4.1.2. *Hasse-derivative of f with respect to $x_1^{e_1}x_2^{e_2}\dots x_n^{e_n}$ is defined as*

$$\frac{1}{e_1!e_2!\dots e_n!}\times\frac{\partial^{\sum e_i}f}{\partial x_1^{e_1}\dots\partial x_n^{e_n}}$$

◊

To see how this is helpful, assume we are working over the field $\mathbb{F}_p$ and consider the polynomial $f = x^p$. It is clear that

$$\frac{\partial^i f}{\partial x^i} = 0 \text{ for every } i.$$

However, the p^{th} order Hasse-derivative is non zero as

$$\frac{1}{p!}\times\frac{\partial^p(x^p)}{\partial x^p} = \frac{1}{p!}\times p! = 1.$$

The idea behind the criterion in [PSS16], is simple. We want to do something very similar to what we did in the case of fields with characteristic zero. It is clear that taking a single partial derivative will not work any more. Instead, we need to take higher order Hasse-derivatives. Up to what order, is something we need to figure out, and that is exactly what they did.

Definition 4.1.3. *A polynomial $f \in \mathbb{F}[x]$ is said to be separable if it has no multiple roots in its splitting field.* ◊

Definition 4.1.4. *The inseparable degree of the extension $\mathbb{F}(\mathbf{x})/\mathbb{F}(\mathbf{f})$ is defined as the minimum p^k such that the minimal polynomial of $x_j^{p^k}$ over $\mathbb{F}(\mathbf{f})$ is separable, for all $j \in [n]$. Here $\mathbf{x} = (x_1, x_2, \dots, x_n)$, and $\mathbf{f} = (f_1, f_2, \dots, f_m)$.*

We define the inseparable degree of the extension $\mathbb{F}(\mathbf{x})/\mathbb{F}(\mathbf{f})$ to be the inseparable degree of $\{f_1, f_2, \dots, f_m\}$ over $\mathbb{F}$. ◊

They showed that if we take Hasse-derivatives up to the inseparable degree, then checking algebraic independence can be reduced to checking linear independence. Only this time, the vector space under consideration will be a quotient space.

We are now almost ready to state and prove the criterion. However before we end this section and go onto that, let us fix some notation.

Notation 4.1.5. *For any $f \in \mathbb{F}[x_1, x_2, \dots, x_n]$ let $\mathcal{H}_t(f)$ denote the non-constant terms of the Taylor expansion of f about an arbitrary point $\mathbf{z} \in \mathbb{F}^n$. That is,*

$$\mathcal{H}_t(f) = f(\mathbf{x}+\mathbf{z}) - f(\mathbf{z}) = \sum_{\sum e_i \le t}\frac{1}{e_1!\dots e_n!}\frac{\partial^{\sum e_i}f(\mathbf{z})}{\partial^{e_1}x_1\dots\partial^{e_n}x_n}x_1^{e_1}x_2^{e_2}\dots x_n^{e_n},$$

◊

4.2 The Criterion over Arbitrary Fields

We will now state the criterion for Algebraic independence over arbitrary fields.

Theorem 4.2.1. *Let $\{f_1, f_2, \ldots, f_m\}$ be a set of n-variate polynomials over a field $\mathbb{F}$. Then, they are algebraically independent iff for a random $\mathbf{z} \in \mathbb{F}^n$, $\{\mathcal{H}_t(f_1), \ldots, \mathcal{H}_t(f_m)\}$ are linearly independent in $\frac{\mathbb{F}(\mathbf{z})[\mathbf{x}]}{\langle \mathcal{H}_t(f_1), \ldots, \mathcal{H}_t(f_m)\rangle^{\geq 2}_{\mathbb{F}(\mathbf{z})} + \langle \mathbf{x}\rangle^{t+1}}$, where t is the inseparable degree of $\{f_1, f_2, \ldots, f_m\}$ and $\mathbf{x} = (x_1, x_2, \ldots, x_n)$.*

As before, we will prove the theorem in two parts. Here is the first direction.

Theorem 4.2.2. *Let $\{f_1, f_2, \ldots, f_m\}$ be a set of n-variate algebraically dependent polynomials over a field $\mathbb{F}$. Then, for a random $\mathbf{z} \in \mathbb{F}^n$ and any $t \in \mathbb{N}$, $\{\mathcal{H}_t(f_1), \ldots, \mathcal{H}_t(f_m)\}$ are linearly dependent in $\frac{\mathbb{F}(\mathbf{z})[\mathbf{x}]}{\langle \mathcal{H}_t(f_1), \ldots, \mathcal{H}_t(f_m)\rangle^{\geq 2}_{\mathbb{F}(\mathbf{z})} + \langle \mathbf{x}\rangle^{t+1}}$ where $\mathbf{x} = (x_1, x_2, \ldots, x_n)$.*

Sketch of Proof. The approach is very similar to the original Jacobian Criterion proof. However, this time one needs to work with higher order Hasse-derivatives and hence with Taylor expansions instead of a single partial derivative. When one considers the Taylor expansion though, it becomes evident that there are a lot of unwanted terms. Hence it is required to go modulo these. □

We have tried to simplify the notations and explanations of [PSS16] slightly. However, the idea is exactly the same as that in the paper.

Proof. Let $\{f_1, f_2, \ldots, f_m\}$ be a set of n-variate algebraically dependent polynomials over a field $\mathbb{F}$ with algebraic rank $k < m$. By Theorem 2.3.5, their annihilating polynomial will remain the same over $\overline{\mathbb{F}}$. Thus, without any loss, we can consider these polynomials to be over $\overline{\mathbb{F}}$ and reorder the f_is such that $\{f_1, f_2, \ldots, f_k\}$ satisfies the conditions of Theorem 4.1.1. Now, fix any $i \in [m]$ arbitrarily and define $\mathbf{f} = (f_i, f_1, f_2, \ldots, f_k)$. Then, $\{f_i, f_1, f_2, \ldots, f_k\}$ is algebraically dependent and so,

$$\exists A(\not\equiv 0) \in \mathbb{F}[y_0, y_1, y_2, \ldots, y_k] \text{ such that } A(\mathbf{f}(\mathbf{x})) = 0 \text{ and } \partial_{y_0}(A) \neq 0.$$

From this we can conclude that for a new variable $\mathbf{z} \in \mathbb{F}^n$, $A(\mathbf{f}(\mathbf{x} + \mathbf{z})) = 0$. Now for any $j \in \{i, 1, \ldots, k\}$, by Taylor expansion,

$$f_j^{\leq t}(\mathbf{x} + \mathbf{z}) = f_j(\mathbf{z}) + \mathcal{H}_t(f_j)$$

and so, $A(\mathbf{f}(\mathbf{z}) + \mathcal{H}_t(\mathbf{f})) = 0 \bmod \langle \mathbf{x}\rangle^{t+1}$. Thus, by Taylor expansion

$$A(\mathbf{f}(\mathbf{z})) + \partial_{y_0}(A(\mathbf{f}(\mathbf{z})))\mathcal{H}_t(f_i) + \sum_{j=1}^{k} \partial_{y_j}(A(\mathbf{f}(\mathbf{z})))\mathcal{H}_t(f_j)$$

is contained in $\sum_{j=2}^{t} \langle \mathcal{H}_t(f_i), \mathcal{H}_t(f_1), \ldots, \mathcal{H}_t(f_k)\rangle^{j}_{\mathbb{F}(\mathbf{z})} \bmod \langle \mathbf{x}\rangle^{t+1}$.

Now, $\partial_{y_0}(A(\mathbf{f}(\mathbf{z}))) \neq 0$ as $\partial_{y_0} A \neq 0$ and A is the minimal degree annihilator for $\mathbf{f}$. Thus, using the fact that $A(\mathbf{f}(\mathbf{z})) = 0$,

$$\mathcal{H}_t(f_i) \in \langle \mathcal{H}_t(f_1), \ldots, \mathcal{H}_t(f_k) \rangle_{\mathbb{F}(\mathbf{z})} + \sum_{j=2}^{t} \langle \mathcal{H}_t(f_i), \mathcal{H}_t(f_1), \ldots, \mathcal{H}_t(f_k) \rangle^j_{\mathbb{F}(\mathbf{z})} \bmod \langle \mathbf{x} \rangle^{t+1}.$$

Claim 4.2.3. *If*

$$\mathcal{H}_t(f_i) \in \langle \mathcal{H}_t(f_1), \ldots, \mathcal{H}_t(f_k) \rangle_{\mathbb{F}(\mathbf{z})} + \sum_{j=2}^{t} \langle \mathcal{H}_t(f_i), \mathcal{H}_t(f_1), \ldots, \mathcal{H}_t(f_k) \rangle^j_{\mathbb{F}(\mathbf{z})} \bmod \langle \mathbf{x} \rangle^{t+1},$$

then

$$\mathcal{H}_t(f_i) \in \sum_{j=1}^{t} \langle \mathcal{H}_t(f_1), \ldots, \mathcal{H}_t(f_k) \rangle^j_{\mathbb{F}(\mathbf{z})} \bmod \langle \mathbf{x} \rangle^{t+1}.$$

Proof. Indeed, it is enough to show that for every $r \in \{2, \ldots, t\}$, if $\mathcal{H}_t(f_i)$ is contained in

$$\sum_{j=1}^{r-1} \langle \mathcal{H}_t(f_1), \ldots, \mathcal{H}_t(f_k) \rangle^j_{\mathbb{F}(\mathbf{z})} + \sum_{j=r}^{t} \langle \mathcal{H}_t(f_i), \mathcal{H}_t(f_1), \ldots, \mathcal{H}_t(f_k) \rangle^j_{\mathbb{F}(\mathbf{z})} \bmod \langle \mathbf{x} \rangle^{t+1},$$

then $\mathcal{H}_t(f_i)$ is contained in

$$\sum_{j=1}^{r} \langle \mathcal{H}_t(f_1), \ldots, \mathcal{H}_t(f_k) \rangle^j_{\mathbb{F}(\mathbf{z})} + \sum_{j=r+1}^{t} \langle \mathcal{H}_t(f_i), \mathcal{H}_t(f_1), \ldots, \mathcal{H}_t(f_k) \rangle^j_{\mathbb{F}(\mathbf{z})} \bmod \langle \mathbf{x} \rangle^{t+1}.$$

So, we fix an arbitrary $r \in \{2, \ldots, t\}$, and assume that $\mathcal{H}_t(f_i)$ is contained in

$$\sum_{j=1}^{r-1} \langle \mathcal{H}_t(f_1), \ldots, \mathcal{H}_t(f_k) \rangle^j_{\mathbb{F}(\mathbf{z})} + \sum_{j=r}^{t} \langle \mathcal{H}_t(f_i), \mathcal{H}_t(f_1), \ldots, \mathcal{H}_t(f_k) \rangle^j_{\mathbb{F}(\mathbf{z})} \bmod \langle \mathbf{x} \rangle^{t+1}.$$

Then, it is enough to show that

$$\langle \mathcal{H}_t(f_i), \mathcal{H}_t(f_1), \ldots, \mathcal{H}_t(f_k) \rangle^r_{\mathbb{F}(\mathbf{z})} \in \sum_{j=r}^{t} \langle \mathcal{H}_t(f_1), \ldots, \mathcal{H}_t(f_k) \rangle^j_{\mathbb{F}(\mathbf{z})} \bmod \langle \mathbf{x} \rangle^{t+1},$$

or in other words that for every $p \in [r]$ and every $\{i_1, \ldots, i_{r-p}\} \subseteq \{1, \ldots, k\}$,

$$\mathcal{H}_t(f_i)^p \prod_{j=1}^{r-p} \mathcal{H}_t(f_{i_j}) \in \sum_{j=r}^{t} \langle \mathcal{H}_t(f_1), \ldots, \mathcal{H}_t(f_k) \rangle^j_{\mathbb{F}(\mathbf{z})} \bmod \langle \mathbf{x} \rangle^{t+1},$$

which is clear from our assumption. □

Getting back to the proof of the theorem, by Claim 4.2.3,

$$\mathcal{H}_t(f_i) \in \langle \mathcal{H}_t(f_1), \ldots, \mathcal{H}_t(f_k) \rangle_{\mathbb{F}(\mathbf{z})} + \sum_{j=2}^{t} \langle \mathcal{H}_t(f_1), \ldots, \mathcal{H}_t(f_k) \rangle^j_{\mathbb{F}(\mathbf{z})} \bmod \langle \mathbf{x} \rangle^{t+1}$$

and thus,

$$\mathcal{H}_t(f_i) \in \langle \mathcal{H}_t(f_1), \ldots, \mathcal{H}_t(f_k) \rangle_{\mathbb{F}(\mathbf{z})} \bmod \left(\sum_{j=2}^{t} \langle \mathcal{H}_t(f_1), \ldots, \mathcal{H}_t(f_k) \rangle^j_{\mathbb{F}(\mathbf{z})} + \langle \mathbf{x} \rangle^{t+1} \right).$$

This shows that $\{\mathcal{H}_t(f_1), \ldots, \mathcal{H}_t(f_m)\}$ has linear rank $k < m$ in the vector space

$$\frac{\mathbb{F}(\mathbf{z})[\mathbf{x}]}{\langle \mathcal{H}_t(f_1), \ldots, \mathcal{H}_t(f_m) \rangle^{\geq 2} + \langle \mathbf{x} \rangle^{t+1}}$$

over the field $\mathbb{F}(\mathbf{z})$ proving the theorem. □

Corollary 4.2.4. *Let $\{f_1, f_2, \ldots, f_m\}$ be a set of n-variate polynomials over a field $\mathbb{F}$. If $\mathsf{algrank}(f_1, f_2, \ldots, f_m) = k$, then the f_is can be reordered in such a way that for a random $\mathbf{z} \in \mathbb{F}^n$ and any $t \in \mathbb{N}$,*

$$\forall i \in [m], \exists R_i \in \overline{\mathbb{F}}[y_1, y_2, \ldots, y_k] \text{ such that } f_i^{\leq t}(\mathbf{x} + \mathbf{z}) = R_i^{\leq t}(f_1(\mathbf{x} + \mathbf{z}), \ldots, f_k(\mathbf{x} + \mathbf{z}))$$

Proof. In the proof of Theorem 4.2.2 we saw that for every $i \in [m]$,

$$\mathcal{H}_t(f_i) \in \sum_{j=1}^{t} \langle \mathcal{H}_t(f_1), \ldots, \mathcal{H}_t(f_k) \rangle^j_{\mathbb{F}(\mathbf{z})} \bmod \langle \mathbf{x} \rangle^{t+1}.$$

Thus, $$f(\mathbf{x} + \mathbf{z}) = f_i(\mathbf{z}) + \mathcal{H}_t(f_i) \in \sum_{j=1}^{t} \langle 1, \mathcal{H}_t(f_1), \ldots, \mathcal{H}_t(f_k) \rangle^j_{\mathbb{F}(\mathbf{z})} \bmod \langle \mathbf{x} \rangle^{t+1},$$

and so $\exists R_i, R_i' \in \overline{\mathbb{F}}[y_1, y_2, \ldots, y_k]$ such that

$$\begin{aligned} f_i(\mathbf{x} + \mathbf{z}) &= R_i'(f_1^{\leq t}(\mathbf{x} + \mathbf{z}) - f_1(\mathbf{z}), \ldots, f_k^{\leq t}(\mathbf{x} + \mathbf{z}) - f_k(\mathbf{z})) \bmod \langle x_1, x_2, \ldots, x_n \rangle^{t+1} \\ &= R_i(f_1^{\leq t}(\mathbf{x} + \mathbf{z}), \ldots, f_k^{\leq t}(\mathbf{x} + \mathbf{z})) \bmod \langle \mathbf{x} \rangle^{t+1} \\ &= R_i(f_1(\mathbf{x} + \mathbf{z}), \ldots, f_k(\mathbf{x} + \mathbf{z})) \bmod \langle \mathbf{x} \rangle^{t+1}. \end{aligned}$$

Thus, $f_i^{\leq t}(\mathbf{x} + \mathbf{z}) = R_i^{\leq t}(f_1(\mathbf{x} + \mathbf{z}), \ldots, f_k(\mathbf{x} + \mathbf{z}))$ completing the proof. □

For the converse, we have the following theorem.

Theorem 4.2.5. *Let $\{f_1, f_2, \ldots, f_m\}$ be a set of n-variate algebraically independent polynomials over a field $\mathbb{F}$. Then, there exists $t \in \mathbb{N}$ such that for a random $\mathbf{z} \in \mathbb{F}^n$, the set $\{\mathcal{H}_t(f_1), \ldots, \mathcal{H}_t(f_m)\}$ is linearly independent in $\frac{\mathbb{F}(\mathbf{z})[\mathbf{x}]}{\langle \mathcal{H}_t(f_1), \ldots, \mathcal{H}_t(f_m) \rangle^{\geq 2}_{\mathbb{F}(\mathbf{z})} + \langle \mathbf{x} \rangle^{t+1}}$.*

We will be proving this using the following two lemmas. As before, we have tried to simplify the explanations, but the ideas are exactly as those in [PSS16].

Lemma 4.2.6. *For any field $\mathbb{F}$, if $\{f_1, f_2, \ldots, f_n\} \subseteq \mathbb{F}[\mathbf{x}]$ is a set of algebraically independent polynomials, then there is a $t \in \mathbb{N}$ such that for every $i \in [n]$,*

$$x_i^t \in \sum_{j=1}^{t} \langle \mathcal{H}_t(f_1), \ldots, \mathcal{H}_t(f_n) \rangle^j_{\mathbb{F}(\mathbf{z})} \bmod \langle \mathbf{x} \rangle^{t+1}.$$

Proof. We note that for any i, $\{x_i, f_1, f_2, \ldots, f_n\}$ is a set of algebraically dependent polynomials. And so, if we define $\mathbf{f} = (x_i, f_1, f_2, \ldots, f_n)$, then

$$\exists A_i (\not\equiv 0) \in \mathbb{F}[y_0, y_1, y_2, \ldots, y_n] \text{ such that } A_i(\mathbf{f}(\mathbf{x})) = 0.$$

Now if we want the proof of Theorem 4.2.2 to go through, then we must ensure that $\partial_{y_0} A_i \neq 0$. Note that since $\{f_1, f_2, \ldots, f_n\}$ is algebraically independent, $\deg_{y_0} A_i \neq 0$. Thus, if $\mathbb{F}$ has characteristic zero, then there is no problem.

However, if $\mathbb{F}$ has characteristic $p \neq 0$, then this is need not be the case and if not, make the following changes. If $\partial_{y_0} A_i = 0$, then $A_i \in \mathbb{F}[y_0^{p^k}, y_1, y_2, \ldots, y_n]$ for some $k \in \mathbb{N}$ such that $A_i \in \mathbb{F}[y_0^{p^{k+1}}, y_1, y_2, \ldots, y_n]$. Thus, $A_i(\mathbf{f}) = A_i'(x_i^{p^k}, f_1, f_2, \ldots, f_n)$ for some $A_i' \in \mathbb{F}[y_0, y_1, y_2, \ldots, y_n]$ and so by taking $A_i = A_i'$ and $\mathbf{f} = (x_i^{p^k}, f_1, f_2, \ldots, f_n)$, we get

$$\exists A_i (\not\equiv 0) \in \mathbb{F}[y_0, y_1, \ldots, y_n] \text{ such that } A_i(\mathbf{f}(\mathbf{x})) = 0 \text{ and } \partial_{y_0} A_i \neq 0.$$

Now we are exactly in the same situation as that in the proof of Theorem 4.2.2 and thus by taking $t_i = p^k$, we follow the steps of the proof to get

$$\mathcal{H}_{t_i}(x_i^{t_i}) \in \sum_{j=1}^{t_i} \langle \mathcal{H}_{t_i}(f_1), \ldots, \mathcal{H}_{t_i}(f_n) \rangle_{\mathbb{F}(\mathbf{z})}^j \bmod \langle \mathbf{x} \rangle^{t_i+1}$$

where $\mathcal{H}_{t_i}(x_i^{t_i}) = x_i^{t_i}$.

Note that if we take $t = \max_i \{t_i\}$, then for every $i \in [n]$, $\partial_{y_0}(A_i) \neq 0$. Further, as t will always be a power of a p, $\mathcal{H}_t(x_i^t) = x_i^t$ and so the proof will go through and we will get

$$x_i^t \in \sum_{j=1}^{t} \langle \mathcal{H}_t(f_1), \ldots, \mathcal{H}_t(f_k) \rangle_{\mathbb{F}(\mathbf{z})}^j \bmod \langle \mathbf{x} \rangle^{t+1}$$

completing the proof. □

At this point it is good to note that the "t" in this lemma exactly matches the notion of inseparable degree as defined in Definition 4.1.4.

Now we have the other lemma that is required to prove Theorem 4.2.5.

Lemma 4.2.7. *For any field $\mathbb{F}$ and $\{f_1, f_2, \ldots, f_m\} \subseteq \mathbb{F}[\mathbf{x}]$ if for some $t \in \mathbb{N}$,*

$$\forall i \in [n],\ x_i^t \in \sum_{j=1}^{t} \langle \mathcal{H}_t(f_1), \ldots, \mathcal{H}_t(f_m) \rangle_{\mathbb{F}(\mathbf{z})}^j \bmod \langle \mathbf{x} \rangle^{t+1},\ \textit{then } m \geq n.$$

Proof. By the given condition, for every $i \in [n]$,

$$x_i^t \in \sum_{j=1}^{t} \langle \mathcal{H}_t(f_1), \ldots, \mathcal{H}_t(f_m) \rangle_{\mathbb{F}(\mathbf{z})}^j \bmod \langle \mathbf{x} \rangle^{t+1},$$

or in other words,

$$x_i^t + \alpha_i \in \sum_{j=1}^{t} \langle \mathcal{H}_t(f_1), \ldots, \mathcal{H}_t(f_m) \rangle_{\mathbb{F}(\mathbf{z})}^j$$

for some $\alpha_i \in \langle \mathbf{x} \rangle^{t+1}$. Now consider the set $\{x_1^t + \alpha_1, \ldots, x_n^t + \alpha_n\}$ and note that if we apply the graded lexicographic monomial ordering, then the set of leading monomials for this set would be $\{x_1^t, \ldots, x_n^t\}$.

Claim 4.2.8. *For some set of n-variate polynomials $\{f_1, f_2, \ldots, f_m\} \in \mathbb{F}[\mathbf{x}]$, if there is a monomial ordering $\precsim$ for which the leading monomials of $f_1, f_2, \ldots, f_m$ are algebraically independent, then $f_1, f_2, \ldots, f_m$ are also algebraically independent.*

Proof. Assume that $f_1, f_2, \ldots, f_m$ are algebraically dependent. Then, there is a non-zero polynomial $A \in \mathbb{F}[y_1, y_2, \ldots, y_m]$ such that $A(f_1, f_2, \ldots, f_m) = 0$. Let $\mathsf{LM}(f)$ denote the leading monomial of f and let M be the monomial in A for which $M(\mathsf{LM}(f_1), \ldots, \mathsf{LM}(f_m))$ is maximal. Then, for any monomial M' in A and any monomial $m_1, m_2, \ldots m_m$ in $f_1, f_2, \ldots, f_m$ respectively,

$$\begin{aligned} M'(m_1, \ldots, m_m) &\precsim \mathsf{LM}(M'(f_1, f_2, \ldots, f_m)) \\ &\precsim M'(\mathsf{LM}(f_1), \ldots, \mathsf{LM}(f_m)) \\ &\precsim M(\mathsf{LM}(f_1), \ldots, \mathsf{LM}(f_m)) \end{aligned}$$

where the last step could not have been an equality if $M \neq M'$.

Indeed, if $M'(\mathsf{LM}(f_1), \ldots, \mathsf{LM}(f_m)) = M(\mathsf{LM}(f_1), \ldots, \mathsf{LM}(f_m))$ and $M \neq M'$, then $M - M'$ is a non-zero polynomial for which $(\mathsf{LM}(f_1), \ldots, \mathsf{LM}(f_m))$ is a root, contradicting the assumption of $\mathsf{LM}(f_1), \ldots, \mathsf{LM}(f_m)$ being algebraically independent.

Thus, for every monomial $M' \neq M$ in A and every monomial $m_1, \ldots m_m$ in $f_1, \ldots, f_m$ respectively,

$$M'(m_1, \ldots, m_m) \neq M(\mathsf{LM}(f_1), \ldots, \mathsf{LM}(f_m)).$$

which implies that $M(\mathsf{LM}(f_1), \ldots, \mathsf{LM}(f_m))$ can not be cancelled by any other monomial in $A(f_1, \ldots, f_m)$ and so, $A(f_1, \ldots, f_m) \neq 0$ contradicting our assumption. Hence, $f_1, f_2, \ldots, f_m$ must be algebraically independent, proving the claim. □

Getting back to the main proof, by the above claim, $\{x_1^t + \alpha_1, \ldots, x_n^t + \alpha_n\}$ must be algebraically independent and by the given condition,

$$\mathsf{algrank}(x_1^t + \alpha_1, \ldots, x_n^t + \alpha_n) \leq \mathsf{algrank}(\mathcal{H}_t(f_1), \ldots, \mathcal{H}_t(f_m)).$$

Thus, $n \leq m$ completing the proof. □

We are now in a position to prove Theorem 4.2.5.

Let $\{f_1, f_2, \ldots, f_m\}$ be a set of n-variate algebraically independent polynomials over a field $\mathbb{F}$. Then, it can be extended to a set of algebraically independent polynomials of size n, namely $\{f_1, f_2, \ldots, f_n\}$, by adding some x_is.

Now, assume that t is the inseparable degree of $\{f_1, f_2, \ldots, f_m\}$, and that for a new set of variables, $\mathbf{z}$, $\{\mathcal{H}_t(f_1), \ldots, \mathcal{H}_t(f_m)\}$ is linearly dependent in $\frac{\mathbb{F}(\mathbf{z})[\mathbf{x}]}{\langle \mathcal{H}_t(f_1), \ldots, \mathcal{H}_t(f_m)\rangle^{\geq 2}_{\mathbb{F}(\mathbf{z})} + \langle \mathbf{x}\rangle^{t+1}}$.

Then, without loss of generality,

$$\mathcal{H}_t(f_m) \in \langle \mathcal{H}_t(f_1), \ldots, \mathcal{H}_t(f_{m-1})\rangle_{\mathbb{F}(\mathbf{z})} \text{ in } \frac{\mathbb{F}(\mathbf{z})[\mathbf{x}]}{\langle \mathcal{H}_t(f_1), \ldots, \mathcal{H}_t(f_m)\rangle^{\geq 2}_{\mathbb{F}(\mathbf{z})} + \langle \mathbf{x}\rangle^{t+1}}.$$

In other words,

$$\mathcal{H}_t(f_m) \in \langle \mathcal{H}_t(f_1), \ldots, \mathcal{H}_t(f_{m-1})\rangle_{\mathbb{F}(\mathbf{z})} + \sum_{j=2}^{t} \langle \mathcal{H}_t(f_1), \ldots, \mathcal{H}_t(f_m)\rangle^{j}_{\mathbb{F}(\mathbf{z})} \bmod \langle \mathbf{x}\rangle^{t+1}.$$

Thus, by Claim 4.2.3

$$\mathcal{H}_t(f_m) \in \sum_{j=1}^{t} \langle \mathcal{H}_t(f_1), \ldots, \mathcal{H}_t(f_{m-1})\rangle^{j}_{\mathbb{F}(\mathbf{z})} \bmod \langle \mathbf{x}\rangle^{t+1}$$

and so

$$\mathcal{H}_t(f_m) \in \sum_{j=1}^{t} \langle \mathcal{H}_t(f_1), \ldots, \mathcal{H}_t(f_{m-1}), \mathcal{H}_t(f_{m+1}), \ldots, \mathcal{H}_t(f_n)\rangle^{j}_{\mathbb{F}(\mathbf{z})} \bmod \langle \mathbf{x}\rangle^{t+1}.$$

Now, by Lemma 4.2.6 and our choice of t, for every $i \in [n]$,

$$x_i^t \in \sum_{j=1}^{t} \langle \mathcal{H}_t(f_1), \ldots, \mathcal{H}_t(f_n)\rangle^{j}_{\mathbb{F}(\mathbf{z})} \bmod \langle \mathbf{x}\rangle^{t+1}$$

and so for every $i \in [n]$,

$$x_i^t \in \sum_{j=1}^{t} \langle \mathcal{H}_t(f_1), \ldots, \mathcal{H}_t(f_{m-1}), \mathcal{H}_t(f_{m+1}), \ldots, \mathcal{H}_t(f_n)\rangle^{j}_{\mathbb{F}(\mathbf{z})} \bmod \langle \mathbf{x}\rangle^{t+1}$$

contradicting Lemma 4.2.7. Thus, our assumption is wrong and for a random $\mathbf{z} \in \mathbb{F}^n$, $\{\mathcal{H}_t(f_1), \ldots, \mathcal{H}_t(f_m)\}$ must be linearly independent in $\frac{\mathbb{F}(\mathbf{z})[\mathbf{x}]}{\langle \mathcal{H}_t(f_1), \ldots, \mathcal{H}_t(f_m)\rangle^{\geq 2}_{\mathbb{F}(\mathbf{z})} + \langle \mathbf{x}\rangle^{t+1}}$ completing the proof.

Finally, combining Theorem 4.2.2 and Theorem 4.2.5, we get the required criterion for Algebraic Independence over arbitrary fields.

5 Faithful Maps and PIT

After a lot of algebra, one would want to understand how all of this is related to PIT. As we noted in the introduction, the connection is via the concept of *faithful maps* - maps that preserve algebraic rank. Now given such maps, we know that Lemma 1.1.1 connects algebraic independence and PIT.

Thus, it becomes important to construct faithful maps. In this chapter, we will see how we can do so over fields of characteristic zero and also see a proof of how Algebraic Independence and PITs are connected.

5.1 Rank Extractors

We want to construct faithful maps. Now we already know that checking algebraic rank can be reduced to the problem of checking linear rank of some matrix. Thus, we should first try to find linear maps that preserve linear rank. Gabizon-Raz [GR05] proved that Vandermonde type matrices have this property. Formally, they showed the following lemma.

Lemma 5.1.1. *Let A be an full rank $k \times n$ matrix with entries in a field $\mathbb{F}$, and let t be an indeterminate. Then, for $M_t = (t^{ij}_{i\in[n],j\in[k]})$, there is some $t \in \{0, 1, \ldots, nk^2\}$ for which*

$$\operatorname{rank}(A \times M_t) = k$$

Proof. As the rank does not change by applying row/column operations, let us assume without loss of generality that A has the form

$$\left[\begin{array}{ccc|ccccc} \ldots & a_1 & \ldots & 0 & 0 & \ldots & 0 \\ \ldots & a_2 & \ldots & \ldots & 0 & \ldots & 0 \\ & \vdots & & & & & \\ \ldots & a_{k-1} & \ldots & \ldots & \ldots & \ldots & 0 \\ \ldots & a_k & \ldots & \ldots & \ldots & \ldots & \ldots \end{array}\right].$$

and view each row a_i as an element of $\mathbb{F}^{<n}[x]$. Thus, if $M_t = (t^{ij}_{i\in[n],j\in[k]})$, the matrix AM_t looks like

$$\begin{bmatrix} a_1(t) & a_1(t^2) & \ldots & a_1(t^k) \\ a_2(t) & a_2(t^2) & \ldots & a_1(t^k) \\ \vdots & \vdots & \ddots & \vdots \\ a_k(t) & a_k(t^2) & \ldots & a_k(t^k) \end{bmatrix}.$$

Thus, if we consider

$$\det(AM_t) = \sum_{\sigma} \prod_{i=1}^{k} a_i(t^{\sigma(i)})$$

as a polynomial in t, we notice that for the identity permutation id, $\prod_{i=1}^{k} a_i(t^{\mathrm{id}(i)})$ has the highest degree of t and that for no other permutation is this degree achieved. Indeed, for any $i \neq j$, assume without loss that

$$i < j \Rightarrow \deg(a_i) < \deg(a_j)$$

and so,

$$\begin{aligned} &\deg(a_i(t^i)a_j(t^j)) - \deg(a_i(t^j)a_j(t^i)) \\ &= (i\deg(a_i) + j\deg(a_j)) - (j\deg(a_i) + i\deg(a_j)) \\ &= (i-j)(deg(a_i) - \deg(a_j)) > 0. \end{aligned}$$

Thus, $\det(AM_t)$ is a non-zero polynomial in t of degree at most nk^2 and this proves that for some $t \in \{0, 1, \ldots, nk^2\}$, $\det(AM_t) \neq 0$. □

The matrix M_t defined above is said to be a rank extractor for all $k \times n$ matrices since for any $k \times n$ matrix A it is multiplied to, there is some t from among a "small" set for which $\mathrm{rank}(AM_t) = \mathrm{rank}(A)$. Formally, supoose we are working in the field $\mathbb{F}$.

Definition 5.1.2. *A matrix M_s with entries as polynomials in s, is said to be a rank extractor for all $k \times n$ matrices $\mathcal{M}_{k,n}$ if there exists a* $\mathrm{poly}(n,k)$*-sized set $S \subseteq \mathbb{F}$ such that*

$$\forall A \in \mathcal{M}_{k,n}, \exists s \in S \text{ such that } \mathrm{rank}(AM_s) = \mathrm{rank}(A).$$

◊

5.2 Faithful Maps

Using the concept of rank extractors, we now want to build faithful maps. Formally, we have the following definition.

Definition 5.2.1. *Given a set of polynomials $\{f_1, f_2, \ldots, f_m\}$, a linear map*

$$\varphi : \{x_1, x_2, \ldots, x_n\} \to \mathbb{F}(y_1, y_2, \ldots, y_k)$$

is said to be faithful if the set of polynomials $\{\varphi(f_1), \varphi(f_2), \ldots, \varphi(f_m)\}$ have the same algebraic rank as $\{f_1, f_2, \ldots, f_m\}$. ◊

Clearly, it is enough to define a linear map φ such that if $\{f_1, f_2, \ldots, f_m\}$ is a set of algebraically independent polynomials, then so is $\{\varphi(f_1), \varphi(f_2), \ldots, \varphi(f_m)\}$.

So let us assume that $\mathbf{f} = \{f_1, f_2, \ldots, f_m\}$ is a set of algebraically independent polynomials. Then by Theorem 3.2.1, $\mathbf{J}(\mathbf{f})$ has full rank. We want to define φ in such a way that $\mathbf{J}(\varphi(\mathbf{f}))$ also has full rank. To do that, we should first see how we can write $\mathbf{J}(\varphi(\mathbf{f}))$ in terms of $\mathbf{J}(\mathbf{f})$.

Note that for any f_i, if $\mathbf{x} = (x_1, x_2, \ldots, x_n)$, then

$$\frac{\partial \varphi(f_i)}{\partial y_j} = \frac{\partial (f_i(\varphi(\mathbf{x})))}{\partial y_j} = \sum_{k=1}^{n} \frac{\partial (f_i(\varphi(\mathbf{x})))}{\partial x_k} \times \frac{\partial \varphi(x_k)}{\partial y_j}.$$

Thus, $\mathbf{J}(\mathbf{f}(\varphi)) = \mathbf{J}(\mathbf{f})|_\varphi \times \mathbf{J}(\varphi)$ and so if we can define φ in such a way that $\mathbf{J}(\varphi) = M_t$ and can ensure that $\mathbf{J}(\mathbf{f})|_\varphi$ has full rank, then we are done. Clearly if we define

$$\varphi(x_i) = \sum_{j=1}^{k} t^{ij} y_j + a_i$$

where t is an indeterminate and a_i is a field constant, then $\mathbf{J}(\varphi) = M_t$. The plan is to choose a_i in such a way that $\mathbf{J}(\mathbf{f})|_\varphi$ has full rank.

We note that the rank of $\mathbf{J}(\mathbf{f})$ is full and thus $\det(\mathbf{J}(\mathbf{f}))$ is a non-zero polynomial in $x_1, x_2, \ldots, x_n$ which would mean that $\exists \mathbf{a} = (a_1, \ldots, a_n)$ such that $\det(\mathbf{J}(\mathbf{f}))(\mathbf{a}) \neq 0$. Now,

$$\det(\mathbf{J}(\mathbf{f}))(\mathbf{a}) = \det(\mathbf{J}(\mathbf{f}(\varphi)))(0, 0, \ldots, 0).$$

Thus, since $\det(\mathbf{J}(\mathbf{f}))(\mathbf{a}) \neq 0$, $\det(\mathbf{J}(\mathbf{f}(\varphi))) \neq 0$ and so $\mathbf{J}(\mathbf{f})|_\varphi$ has full rank. As $\mathbf{J}(\mathbf{f}(\varphi)) = \mathbf{J}(\mathbf{f})|_\varphi \times \mathbf{J}(\varphi)$, we will get $\mathbf{J}(\varphi(\mathbf{f}))$ to be a full rank matrix as well, and so $\varphi(f_1), \varphi(f_2), \ldots, \varphi(f_k)$ is a set of algebraically independent polynomials.

5.3 Connection with PITs

Before we see how we can build faithful maps over fields over finite characteristic, we will see how the concept of Algebraic Independence helps us in solving PITs. The following result is surprising because of the following reason. We know that if φ is a faithful map for $\{f_1, f_2, \ldots, f_m\}$ and $\{f_1, f_2, \ldots, f_k\}$ is a transcendence basis, then

$$F(f_1, f_2, \ldots, f_k) \neq 0 \Leftrightarrow \varphi(F(f_1, f_2, \ldots, f_k)) \neq 0.$$

However, the result says that φ preserves non-zeroness even if the polynomial F under consideration depends on all the m polynomials $f_1, f_2, \ldots, f_m$.

Formally, we prove the following lemma. The proof, as we present it here, is from [ASSS12], even though it was first proved in [BMS11].

Lemma 5.3.1. *Suppose $f_1, f_2, \ldots, f_m \in \mathbb{F}[x_1, x_2, \ldots, x_n]$ and φ is a faithful map. Then, for any circuit $C(z_1, \ldots, z_m)$,*

$$C(f_1, f_2, \ldots, f_m) = 0 \Leftrightarrow \varphi\left(C(f_1, f_2, \ldots, f_m)\right) = 0$$

Proof. As φ is a faithful map, there must be some transcendence basis $\{f_1, f_2, \ldots, f_k\}$ that is preserved by φ. Then,

$$\mathbb{F}(f_1, f_2, \ldots, f_k, f_{k+1}, \ldots, f_m) = \mathbb{F}(f_1, f_2, \ldots, f_k)[f_{k+1}, \ldots, f_m]$$

as each of $f_{k+1}, \ldots, f_m$ are algebraic over $\mathbb{F}(f_1, f_2, \ldots, f_k)$. Also,

$$\text{for any } F \in \mathbb{F}[f_1, f_2, \ldots, f_k],\ F \neq 0 \Rightarrow \varphi(F) \neq 0.$$

Now note that

$$\mathcal{C}(f_1, f_2, \ldots, f_m) \in \mathbb{F}[f_1, f_2, \ldots, f_m].$$

However, we can also consider $\mathcal{C}(f_1, f_2, \ldots, f_m)$ as an element in $\mathbb{F}(f_1, f_2, \ldots, f_m)$ which is a field and so,

$$\exists R \in \mathbb{F}(f_1, f_2, \ldots, f_m) = \mathbb{F}(f_1, f_2, \ldots, f_k)[f_{k+1}, \ldots, f_m]$$

such that

$$\mathcal{C}[f_1, f_2, \ldots, f_m] R(f_1, f_2, \ldots, f_k)[f_{k+1}, \ldots, f_m] = 1.$$

Clearing denominators, we get

$$\begin{aligned} &0 \neq \mathcal{C}[f_1, f_2, \ldots, f_m] \tilde{R}[f_1, f_2, \ldots, f_m] = Q[f_1, f_2, \ldots, f_k] \\ &\Rightarrow \varphi(\mathcal{C}[f_1, f_2, \ldots, f_m]) \varphi(\tilde{R}[f_1, f_2, \ldots, f_m]) = \varphi(Q[f_1, f_2, \ldots, f_m]) \neq 0 \\ &\Rightarrow \varphi(\mathcal{C}[f_1, f_2, \ldots, f_m]) \neq 0. \end{aligned}$$

The other direction is completely trivial. □

As noted before, this lemma does not assume anything about the characteristic of the field. So in order to extend the results in [BMS11] and [ASSS12] to fields of arbitrary characteristic, it is essential that we are able to construct faithful maps over such fields.

6 Faithful maps over Arbitrary Fields

Given a set of polynomials $\{f_1, f_2, \ldots, f_m\}$ which are defined on n variables and have algebraic rank k, the intuition is that they actually depend on only k variables. A faithful map is a formal way of expressing this. It relabels the variables $x_1, x_2, \ldots, x_n$ in such a way that $\varphi(f_1), \ldots, \varphi(f_m)$ now become k-variate polynomials and yet continues to have algebraic rank k.

In the last chapter, we saw how to construct faithful maps over fields of characteristic zero. The construction was essentially carried out in the following steps:

- Note that using the Jacobian Criterion, it is enough to show that $\mathbf{J}(\mathbf{f})$ and $\mathbf{J}(\varphi(\mathbf{f}))$ have the same rank.
- Construct a linear map M that preserves linear rank.
- Define φ in such a way that $\operatorname{rank}(\mathbf{J}(\mathbf{f})|_\varphi) = \operatorname{rank}(\mathbf{J}(\mathbf{f}))$ and $\mathbf{J}(\mathbf{f}(\varphi)) = \mathbf{J}(\mathbf{f})|_\varphi \times M$.

We will also be doing something very similar, but using the [PSS16] criterion.

6.1 The Strategy

For a set of n-variate polynomials $\{f_1, f_2, \ldots, f_k\}$, let $\mathbf{f} = (f_1, f_2, \ldots, f_k)$ and

$$\hat{\mathcal{H}}(\mathbf{f}) = \begin{bmatrix} \ldots & \mathcal{H}_t(f_1) & \ldots \\ \ldots & \mathcal{H}_t(f_2) & \ldots \\ & \vdots & \\ \ldots & \mathcal{H}_t(f_k) & \ldots \end{bmatrix}.$$

The columns in $\mathcal{H}(\mathbf{f})$ are labelled by monomials $\{m\}$ in $\mathbf{x} = (x_1, x_2, \ldots, x_n)$ of degree upto t and the element in position (m, i) is the coefficient of m in $\mathcal{H}(f_i)$. By Theorem 4.2.1, if $\{f_1, f_2, \ldots, f_k\}$ is a set of algebraically independent polynomials, then $\hat{\mathcal{H}}(\mathbf{f})$ has full rank in

$$\frac{\mathbb{F}(\mathbf{z})[\mathbf{x}]}{\langle \mathcal{H}_t(f_1), \ldots, \mathcal{H}_t(f_k) \rangle^{\geq 2}_{\mathbb{F}(\mathbf{z})} + \langle \mathbf{x} \rangle^{t+1}},$$

where t is the inseparable degree of $\{f_1, f_2, \ldots, f_k\}$.

Note that this is equivalent to saying that for every $\mathbf{v} = [v_1, v_2, \ldots, v_k]^{\mathrm{T}}$ with

$$v_i\text{'s in } \langle \mathcal{H}_t(f_1), \ldots, \mathcal{H}_t(f_k) \rangle^{\geq 2}_{\mathbb{F}(\mathbf{z})} \bmod \langle \mathbf{x} \rangle^{t+1},$$

the matrix $\mathcal{H}(\mathbf{f}, \mathbf{v}) = \hat{\mathcal{H}}(\mathbf{f}) + \mathbf{v}$ has full rank in $\mathbb{F}(\mathbf{z})[\mathbf{x}]$.

By Theorem 4.2.1, what we want is a linear map $\varphi : \{x_1, x_2, \ldots, x_n\} \to \mathbb{F}(y_1, y_2, \ldots, y_k)$ for which the following is true: For every $\mathbf{u} = [u_1, u_2, \ldots, u_k]^{\mathrm{T}}$ with

$$\text{"}u_i\text{"s in } \langle \mathcal{H}_t(f_1(\varphi))), \ldots, \mathcal{H}_t(f_k(\varphi)))\rangle^{\geq 2}_{\mathbb{F}(\mathbf{w})} \bmod \langle \mathbf{y} \rangle^{t+1},$$

the matrix $\mathcal{H}(\mathbf{f}(\varphi), \mathbf{u}) = \hat{\mathcal{H}}(\mathbf{f}(\varphi)) + \mathbf{u}$ has full rank in $\mathbb{F}(\mathbf{w})[\mathbf{y}]$.

Just to spell it out, the columns of $\mathcal{H}(\mathbf{f}, \mathbf{v})$ are indexed by monomials $\{m\}$ in $\mathbf{x}$, of degree upto t. The entry at position (i, m) is the coefficient of m in $\mathcal{H}_t(f_i) + v_i$, which in general is a polynomial in $\mathbf{z} = (z_1, z_2, \ldots, z_n)$.

On the other hand, the columns of $\mathcal{H}(\mathbf{f}(\varphi), \mathbf{u})$ are indexed by monomials $\{m'\}$ in $\mathbf{y} = (y_1, y_2, \ldots, y_k)$, of degree upto t. The entry at position (i, m') is the coefficient of m' in $\mathcal{H}_t(f_i(\varphi)) + u_i$, which in general is a polynomial in $\mathbf{w} = (w_1, w_2, \ldots, w_k)$.

In order to construct a faithful map, we claim that the following theorem is enough.

Theorem 6.1.1. *There exists a family of linear maps $\varphi_s : \{x_i\}_{i \in [n]} \to \mathbb{F}[\mathbf{y}]$ such that,*

1. *for every* $u \in \langle \mathcal{H}_t(f_1(\varphi_s))), \ldots, \mathcal{H}_t(f_k(\varphi_s)))\rangle^{\geq 2}_{\mathbb{F}(\mathbf{w})}$,

   there should exist some $v \in \langle \mathcal{H}_t(f_1), \ldots, \mathcal{H}_t(f_k)\rangle^{\geq 2}_{\mathbb{F}(\mathbf{z})}$

   such that $v(\varphi_s) = u$. This will imply that for every s, $\mathbf{u}$, there exists some $\mathbf{v}$ for which

   $$\mathcal{H}(\mathbf{f}(\varphi_s), \mathbf{u}) = \mathcal{H}(\mathbf{f}(\varphi_s), \mathbf{v}(\varphi_s))$$

2. *for every s, $\mathbf{v}$, $\mathcal{H}(\mathbf{f}, \mathbf{v})|_{\varphi_s} \times M_s$ is a sub-matrix of $\mathcal{H}(\mathbf{f}(\varphi_s), \mathbf{v}(\varphi_s))$*

3. *$\exists s$ such that for every $\mathbf{v}$, if $\mathcal{H}(\mathbf{f}, \mathbf{v})|_{\varphi_s}$ has full rank, then so does $\mathcal{H}(\mathbf{f}, \mathbf{v})|_{\varphi_s} \times M_s$.*

where $\mathbf{f} = (f_1, f_2, \ldots, f_k)$ and M_s is some matrix dependent on φ_s.

Once we have such a family $\Phi_s = \{\varphi_s\}$, if $\mathbb{H}$ is a hitting set for $\tilde{\mathcal{H}}(\mathbf{f}, \mathbf{v})$ — the set of all $k \times k$ minors in $\mathcal{H}(\mathbf{f}, \mathbf{v})$ — then one of the following maps will be faithful for $\mathbf{f}$.

$$\{\tilde{\varphi}_{s,\mathbf{a}} : x_i \to \varphi_s(x_i) + a_i \text{ and } z_i \to \varphi_s(z_i) + a_i \ : \ \mathbf{a} = (a_1, a_2, \ldots, a_n) \in \mathbb{H}\}_s.$$

The reason for this is very similar to the characteristic zero case. Assume that $\mathcal{H}(\mathbf{f}, \mathbf{v})$ has full rank. Then for some $\mathcal{H}'(\mathbf{f}, \mathbf{v}) \in \tilde{\mathcal{H}}(\mathbf{f}, \mathbf{v})$, $\det(\mathcal{H}'(\mathbf{f}, \mathbf{v}))$ is a non-zero polynomial in $\mathbf{z}$, and hence $\det(\mathcal{H}'(\mathbf{f}, \mathbf{v}))(\mathbf{a}) \neq 0$ for some $\mathbf{a} \in \mathbb{H}$.

For the s in the third part of Theorem 6.1.1, let $\varphi : \tilde{\varphi}_{s,\mathbf{a}}$. Note that for any $\mathbf{v}$,

$$\det(\mathcal{H}'(\mathbf{f}, \mathbf{v}))(\mathbf{a}) = \det(\mathcal{H}'(\mathbf{f}, \mathbf{v})|_{\varphi})(\mathbf{0}),$$

and so $\det(\mathcal{H}'(\mathbf{f}, \mathbf{v}))(\mathbf{a}) \neq 0$ will imply that $\det(\mathcal{H}'(\mathbf{f}, \mathbf{v})|_{\varphi}) \neq 0$. This shows that $\mathcal{H}'(\mathbf{f}, \mathbf{v})|_{\varphi}$ will have full rank whenever $\mathcal{H}'(\mathbf{f}, \mathbf{v})$ does.

Thus, we can make the following observation.

Observation 6.1.2. *There exists s, $\mathbf{a}$ such that for $\varphi = \varphi_{s,\mathbf{a}}$, $\mathcal{H}'(\mathbf{f},\mathbf{v})|_\varphi$ will have full rank whenever $\mathcal{H}'(\mathbf{f},\mathbf{v})$ does.*

Further, the following will not be too hard to observe once we define φ_s

- *The matrices corresponding to $\tilde{\varphi}_s$ and φ_s are equal for any $\mathbf{a}$, and thus*

$$\mathcal{H}(\mathbf{f},\mathbf{v})|_\varphi \times M_s \text{ is a sub-matrix of } \mathcal{H}(\mathbf{f}(\varphi),\mathbf{v}(\varphi)).$$

- *The proof of the first part of Theorem 6.1.1 will work even for $\tilde{\varphi}_s$, and so for any $\mathbf{u}$, there exists a $\mathbf{v}$ such that*

$$\mathcal{H}(\mathbf{f}(\varphi),\mathbf{u}) = \mathcal{H}(\mathbf{f}(\varphi),\mathbf{v}(\varphi)).$$

Using the above observations, the fact that M_s preserves rank and that the rank of $\mathcal{H}(\mathbf{f}(\varphi),\mathbf{v}(\varphi))$ will always be greater than that of any of its sub-matrices, we get:

$$\mathcal{H}(\mathbf{f},\mathbf{v}) \text{ has full rank for every } \mathbf{v} \Rightarrow \mathcal{H}(\mathbf{f}(\varphi),\mathbf{u}) \text{ has full rank for every } \mathbf{u}.$$

The other direction is trivial and so there exists s, $\mathbf{a}$ such that for $\varphi = \varphi_{s,\mathbf{a}}$,

$$\mathcal{H}(\mathbf{f},\mathbf{v}) \text{ has full rank for every } \mathbf{v} \Leftrightarrow \mathcal{H}(\mathbf{f}(\varphi),\mathbf{u}) \text{ has full rank for every } \mathbf{u}.$$

In general, suppose we are given polynomials $f_1, f_2, \ldots, f_m \in \mathbb{F}[x_1, x_2, \ldots, x_n]$ with transcendence basis $\{f_1, f_2, \ldots, f_k\}$. By Theorem 4.2.1, this implies that $\mathcal{H}(\mathbf{f},\mathbf{v})$ has full rank for every $\mathbf{v}$. This we saw, is equivalent to saying that for φ defined as above, $\mathcal{H}(\mathbf{f}(\varphi),\mathbf{u})$ has full rank for every $\mathbf{u}$. Thus by Theorem 4.2.1, $\{f_1(\varphi), f_2(\varphi), \ldots, f_k(\varphi)\}$ is algebraically independent and so $\mathsf{algrank}(\mathbf{f}) \leq \mathsf{algrank}(\mathbf{f}(\varphi))$.

The other direction of inequality is trivially true and thus we have

$$\mathsf{algrank}(\mathbf{f}) = \mathsf{algrank}(\mathbf{f}(\varphi)),$$

proving that φ is a faithful map for $f_1, f_2, \ldots, f_m$.

Before we go into the proof of Theorem 6.1.1, let us fix some notation.

Notation 6.1.3. *From now on, we will assume the following:*

- $\mathbf{x} = (x_1, x_2, \ldots, x_n)$, $\mathbf{e} = (e_1, e_2, \ldots, e_n)$;
- $f_1, \ldots f_k \in \mathbb{F}[\mathbf{x}]$ *are algebraically independent polynomials of inseparable degree t;*
- $\mathbf{f} = (f_1, f_2, \ldots, f_k)$, $\mathbf{y} = (y_1, y_2, \ldots, y_k)$, $\mathbf{p} = (p_1, p_2, \ldots, p_k)$;
- $\mathbf{x}^\mathbf{e} = (x_1^{e_1}, x_2^{e_2} \ldots, x_n^{e_n})$, $\mathbf{y}^\mathbf{p} = (y_1^{p_1}, y_2^{p_2} \ldots, y_k^{p_k})$;
- $\partial_\mathbf{e} = \frac{\partial^{\sum p_i}}{\partial x_1^{e_1} \partial x_2^{e_2} \ldots \partial x_n^{e_n}}$;
- $\mathcal{H}$ *is as defined at the beginning of this section.* ◊

6.2 Finding a Rank Extractor

The first step towards finding a φ that satisfies the properties in Theorem 6.1.1 is to see how $\mathcal{H}(\mathbf{f}(\varphi), \mathbf{v}(\varphi))$ can be written in terms of $\mathcal{H}(\mathbf{f}, \mathbf{v})$.

Let us define the following set:

$$\mathsf{shuff}(\mathbf{e}) = \{\sigma : \sigma \text{ is a permutation of } S_{\mathbf{e}}\}$$

where $S_{\mathbf{e}}$ denotes the ordered multi-set consisting of e_i "i"s for each $i \in [n]$. Also, let $S_{\mathbf{p}}$ denote the ordered multi-set consisting of p_i "i"s for each $i \in [k]$.

Then for any linear map φ and any $f \in \mathbb{F}[\mathbf{x}]$, using chain rule it is not hard to see that the following relation holds.

$$\frac{\partial^{\sum p_i} f(\varphi(\mathbf{x}))}{\partial y_1^{p_1} \partial y_2^{p_2} \dots \partial y_k^{p_k}} = \sum_{\mathbf{e}:\sum e_i = \sum p_i} \left(\partial_{\mathbf{e}}(f(\mathbf{x}))(\varphi) \times \sum_{\sigma \in \mathsf{shuff}(\mathbf{e})} \left(\prod_{j \in S_{\mathbf{e}}} \frac{\partial(\varphi(x_{\sigma(j)}))}{\partial y_{S_{\mathbf{p}}[\mathsf{pos}(j)]}} \right) \right)$$

Thus ignoring scalars, we seem to have a matrix decomposition. Consider the matrix M_φ with the following structure.

- The rows are indexed by monomials in $\mathbf{x}$, and the columns are indexed by monomials in $\mathbf{y}$.
- The element at position $(\mathbf{x}^{\mathbf{e}}, \mathbf{y}^{\mathbf{p}})$ is $\begin{cases} \sum_{\sigma \in \mathsf{shuff}(\mathbf{e})} \left(\prod_{j \in S_{\mathbf{e}}} \frac{\partial(\varphi(x_{\sigma(j)}))}{\partial y_{S_{\mathbf{p}}[\mathsf{pos}(j)]}} \right) & \text{if } \sum e_i = \sum p_i \\ 0 & \text{otherwise} \end{cases}$

Clearly, M_φ is a block diagonal matrix where the k^{th} block has row labels $\mathbf{x}^{\mathbf{e}}$ and column labels $\mathbf{y}^{\mathbf{p}}$ such that $\sum e_i = k = \sum p_i$.

Now, since we know that Vandermonde type matrices are rank extractors, it would be helpful if each block in M_φ were to look like a Vandermonde. However, this is clearly not the case since each element in the matrix is a sum of many monomials, even if we define $\varphi(x_i) = \sum s^{ij} y_j$ as in the zero characteristic case.

This motivated us to consider a sub-matrix of M_φ that does look like a Vandermonde if $\varphi(x_i) = \sum s^{ij} y_j$. Let $\tilde{M}_\varphi$ be the sub-matrix of M_φ that has only those columns that are labelled by "pure monomials" — monomials of the type y_i^e for different "i"s.

Thus, for $\varphi : x_i \to \sum s^{ij} y_j$, $\tilde{M}_\varphi$ has the following structure:

- The rows are indexed by monomials in $\mathbf{x}$ of degree upto t, and the columns are indexed by monomials in $\mathbf{y}$ of the type y_i^e.
- The element at position $(\mathbf{x}^{\mathbf{e}}, y_j^e)$ is $\begin{cases} \frac{e!}{e_1! \dots e_n!} \times s^{j \sum_{l \in S_{\mathbf{e}}} l} & \text{if } \sum e_i = e \\ 0 & \text{otherwise} \end{cases}$

The problem with $\tilde{M}_\varphi$ however, is that the value of $\left(\sum_{l \in S_{\mathbf{e}}} l\right)$ is not necessarily distinct for distinct "$\mathbf{e}$"s. Thus, $\tilde{M}_\varphi$ does not remain a rank extractor. This caused us to define φ as follows:

$$\varphi(x_i) = \sum s^{(t+1)^i j} y_j.$$

For this choice of φ, $\tilde{M}_\varphi$ is a block diagonal matrix with the e^{th} block having rows indexed by monomials $\mathbf{x}^{\mathbf{e}}$ for which $\sum e_i = e$ and columns indexed by y_j^e for various "j"s. Further, each block looks like a Vandermonde type matrix. Hence, $\tilde{M}_\varphi$ is a good candidate for a rank extractor.

6.3 Constructing a Faithful Map

As we saw in the last section, a good candidate for a faithful map is the following:

$$\varphi_s(x_i) = \sum s^{(t+1)^i j} y_j.$$

We will now proceed to show that it satisfies the conditions of Theorem 6.1.1. Before that however, note that the first point in Observation 6.1.2 is true for φ_s.

To check that φ_s satisfies the first condition, note that by the definition of φ_s,

$$\begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} = M_{\varphi_s} \times \begin{bmatrix} y_1 \\ y_2 \\ \vdots \\ y_k \end{bmatrix} \text{ for } M_{\varphi_s} = \begin{bmatrix} s^t & s^{2t} & \dots & s^{kt} \\ s^{t^2} & s^{2t^2} & \dots & s^{kt^2} \\ \vdots & \vdots & \ddots & \vdots \\ s^{t^n} & s^{2t^n} & \dots & s^{kt^n} \end{bmatrix}.$$

Clearly, M_{φ_s} has full column-rank and thus has a left inverse. Note that there might be many left inverses, but we can choose any one of them and call the corresponding linear operator φ_s^{-1}.

Thus for every $u \in \langle \mathcal{H}_t(f_1(\varphi_s)), \dots, \mathcal{H}_t(f_k(\varphi_s)) \rangle^{\geq 2}_{\mathbb{F}(\mathbf{w})}$, if

$$u = \sum g(\mathbf{w}) \times h(\mathcal{H}_t(f_1(\varphi_s)), \dots, \mathcal{H}_t(f_k(\varphi_s))),$$

then we get the element $v \in \langle \mathcal{H}_t(f_1), \dots, \mathcal{H}_t(f_k) \rangle^{\geq 2}_{\mathbb{F}(\mathbf{z})}$ required for the first part of Theorem 6.1.1 as follows:

$$v = \sum g(\varphi_s^{-1}(\mathbf{w})) \times h(\mathcal{H}_t(f_1), \dots, \mathcal{H}_t(f_k)).$$

Further note that a similar argument holds for $\tilde{\varphi}_s$ as well, and thus the second point in Observation 6.1.2 is also true.

Next, we want to check that φ_s satisfies the second condition of Theorem 6.1.1. So, let us define the matrix M_s as follows:

- The rows are indexed by $\{\mathbf{x}^{\mathbf{e}}\}_{\mathbf{e}}$ and the columns are indexed by $\left\{y_j^e\right\}_{j,e}$.
- The element at position $(\mathbf{x}^{\mathbf{e}}, y_j^p)$ is $\begin{cases} s^{j \sum_{l \in S_{\mathbf{e}}} (t+1)^l} & \text{if } \sum e_i = e \\ 0 & \text{otherwise} \end{cases}$

We want to show that $\mathcal{H}(\mathbf{f},\mathbf{v})|_{\varphi_s} \times M_s$ is a sub-matrix of $\mathcal{H}(\mathbf{f}(\varphi_s),\mathbf{v}(\varphi_s))$.

By chain rule, for any $f \in \mathbb{F}(\mathbf{z})[\mathbf{x}]$,

$$\frac{\partial^e f(\varphi_s(\mathbf{x}))}{\partial y_j^e} = \sum_{\mathbf{e}:\sum e_i = e} \left(\partial_{\mathbf{e}}(f(\mathbf{x}))\right)(\varphi_s) \times \frac{e!}{e_1!\ldots e_n!} \times s^{j\sum_{l\in S_{\mathbf{e}}}(t+1)^l}$$

and so,

$$\frac{1}{e!} \times \frac{\partial^e f(\varphi_s(\mathbf{x}))}{\partial y_j^e} = \sum_{\mathbf{e}:\sum e_i = e} \left(\frac{1}{e_1!\ldots e_n!} \times \left(\partial_{\mathbf{e}}(f(\mathbf{x}))\right)(\varphi_s) \times s^{j\sum_{l\in S_{\mathbf{e}}}(t+1)^l} \right).$$

In other words,

$$\text{coeff. of } y_j^e \text{ in } f(\varphi_s(\mathbf{x})) = \sum_{\mathbf{e}:\sum e_i = e} \left((\text{ coeff. of } \mathbf{x}^{\mathbf{e}} \text{ in } f(\mathbf{x}))(\varphi_s) \times s^{j\sum_{l\in S_{\mathbf{e}}}(t+1)^l} \right)$$

which implies that

$$\begin{aligned}
\left(\text{coeff. of } y_j^e \text{ in } f(\varphi_s(\mathbf{x}))\right)(\mathbf{w}) &= \sum_{\mathbf{e}:\sum e_i = e} \left((\text{ coeff. of } \mathbf{x}^{\mathbf{e}} \text{ in } f(\mathbf{x}))(\varphi_s)(\mathbf{w}) \times s^{j\sum_{l\in S_{\mathbf{e}}}(t+1)^l} \right) \\
&= \sum_{\mathbf{e}:\sum e_i = e} \left((\text{ coeff. of } \mathbf{x}^{\mathbf{e}} \text{ in } f(\mathbf{x}))(\varphi_s(\mathbf{z})) \times s^{j\sum_{l\in S_{\mathbf{e}}}(t+1)^l} \right) \\
&= \sum_{\mathbf{e}:\sum e_i = e} \left((\text{ coeff. of } \mathbf{x}^{\mathbf{e}} \text{ in } f(\mathbf{x}))(\mathbf{z})(\varphi_s) \times s^{j\sum_{l\in S_{\mathbf{e}}}(t+1)^l} \right)
\end{aligned}$$

if we define $\varphi_s(z_i) = \sum s^{(t+1)^i j} w_j$.

Hence,

$$\begin{aligned}
&\left(\text{coeff. of } y_j^e \text{ in } f(\varphi_s(\mathbf{x}),\varphi_s(\mathbf{z}))\right)(\varphi_s(\mathbf{z})) \\
&= \sum_{\mathbf{e}:\sum e_i = e} \left((\text{ coeff. of } \mathbf{x}^{\mathbf{e}} \text{ in } f(\mathbf{x},\mathbf{z}))|_{\mathbf{x}=\mathbf{z}}(\varphi_s) \times s^{j\sum_{l\in S_{\mathbf{e}}}(t+1)^l} \right).
\end{aligned}$$

This clearly shows that in particular, if $\bar{\mathcal{H}}(\mathbf{f}(\varphi_s),\mathbf{v}(\varphi_s))$ were to be the sub-matrix of $\mathcal{H}(\mathbf{f}(\varphi_s),\mathbf{v}(\varphi_s))$ consisting of only those columns which are indexed by monomials of the type $\left\{y_j^e\right\}_{j,e}$, then

$$\bar{\mathcal{H}}(\mathbf{f}(\varphi),\mathbf{v}(\varphi)) = \mathcal{H}(\mathbf{f},\mathbf{v})|_{\varphi} \times M_s,$$

proving that φ_s satisfies the second condition of Theorem 6.1.1.

So now, the only thing left to prove is, that if $\mathcal{H}(\mathbf{f},\mathbf{v})|_{\varphi_s}$ has full rank, then so does $\mathcal{H}(\mathbf{f},\mathbf{v})|_{\varphi_s} \times M_s$. Clearly, the following lemma is enough.

Lemma 6.3.1. *If A is a full row rank matrix with at most k rows and has columns indexed by monomials in $\mathbf{x}$, then AM_s also has full row-rank.*

Proof. Let us associate with each x_i a weight $w_i = (t+1)^i$ and extend it naturally to all the monomials in $\mathbf{x}$. Namely, $\mathrm{wt} : \{\mathbf{x}^{\mathbf{e}}\} \to \mathbb{N}$ is defined as $\mathrm{wt}(\mathbf{x}^{\mathbf{e}}) = \sum_{i=1}^n e_i w_i$. As $e_i \le t$ for every i, it is clear that each monomial gets a distinct weight. We will see that this is the only property that we will use.

Next, let us assume that A has k' rows. Then, we extend the definition of wt to every $k' \times k'$ minors of A as follows.

- Choose any $k' \times k'$ minor of A and call it A'. Say it has columns indexed by $\mathbf{x}^{\mathbf{e}_1}, \ldots, \mathbf{x}^{\mathbf{e}_{k'}}$ with the property that $\mathsf{wt}(\mathbf{x}^{\mathbf{e}_1}) < \mathsf{wt}(\mathbf{x}^{\mathbf{e}_2}) < \ldots < \mathsf{wt}(\mathbf{x}^{\mathbf{e}_{k'}})$.
- Define the weight of this minor as $\mathsf{wt}(A') = \sum_{i=1}^{k'} i\, \mathsf{wt}(\mathbf{x}^{\mathbf{e}_i})$

Claim 6.3.2. *There is a unique non-zero minor with maximum weight.*

Assume there are two non-zero minors A' and A'', both having the same weight. Then, to prove the claim, it is enough to find a non-zero minor of greater weight. Now among the symmetric difference of the columns in A' and those in A'', assume that A' has the one with minimum weight, say $\mathbf{x}^{\mathbf{e}'}$. Then, by the matroid property, there is a column in A'' say $\mathbf{x}^{\mathbf{e}''}$ such that $A''' = \left(A' \setminus \left\{\mathbf{x}^{\mathbf{e}'}\right\}\right) \cup \left\{\mathbf{x}^{\mathbf{e}''}\right\}$ is also a non-zero minor. By construction, $\mathsf{wt}(\mathbf{x}^{\mathbf{e}''}) > \mathsf{wt}(\mathbf{x}^{\mathbf{e}'})$.

Further, if $\mathbf{x}^{\mathbf{e}'}$ appears at position i' in A' when the columns are arranged in ascending order by weight and $\mathbf{x}^{\mathbf{e}''}$ appears at position i'' in A''', then by construction $i'' > i'$ and

$$\begin{aligned}\mathsf{wt}(A''') &= \mathsf{wt}(A') + i'(\mathsf{wt}(\mathbf{x}^{\mathbf{e}''}) - \mathsf{wt}(\mathbf{x}^{\mathbf{e}'})) + \sum_{i=i'+1}^{i''} (\mathsf{wt}(\mathbf{x}^{\mathbf{e}''}) - \mathsf{wt}(\mathbf{x}^{\mathbf{e}_i})) \\ &> \mathsf{wt}(A') = \mathsf{wt}(A'')\end{aligned}$$

assuming $\mathbf{x}^{\mathbf{e}_i}$ was at position i in A' for $i \in \{i'+1, \ldots, i''\}$. This completes the proof of the claim.

Now, note that M_s is a block diagonal matrix with the e^{th} block consisting of rows $\mathbf{x}^{\mathbf{e}}$ for which $\sum_{i=1}^{n} e_i = e$ and columns of the type $\left\{y_i^e\right\}_{i \in [k]}$. We will choose k' columns from M_s as follows.

- Let A_0 be the unique $k' \times k'$ minor of A having minimum weight. Further, assume its columns are indexed by $\mathbf{x}^{\mathbf{e}_1}, \ldots, \mathbf{x}^{\mathbf{e}_{k'}}$ with the property that $\mathsf{wt}(\mathbf{x}^{\mathbf{e}_1}) < \mathsf{wt}(\mathbf{x}^{\mathbf{e}_2}) < \ldots < \mathsf{wt}(\mathbf{x}^{\mathbf{e}_{k'}})$.
- Choose the columns $\left\{y_i^{\sum_{j=1}^{n} (\mathbf{e}_i)_j}\right\}_{i \in [k']}$ and let this sub-matrix of M_s be M_s'. Further, let the number of columns chosen from the j^{th} block be k_j'.

Clearly, the following claim will prove the lemma.

Claim 6.3.3. *AM_s', which is a $k' \times k'$ matrix, has non-zero determinant.*

Note that by Binet-Cauchy formula,

$$\det(AM_s') = \sum_{B \subseteq \{\mathbf{x}^{\mathbf{e}}\},\, |B| = k'} \det(A_B) \det((M_s')_B).$$

Thus, if we define $B_1 = \{B : B \subset \{\mathbf{x}^{\mathbf{e}}\}, |B| = k' \text{ and } A_B \text{ is a non-zero minor of } A\}$ and $B_2 = \left\{B : B \subset \{\mathbf{x}^{\mathbf{e}}\}, |B| = k' \text{ and for every } j, \left|\{\mathbf{x}^{\mathbf{e}} : \sum_{i=1}^{n} e_i = j\}\right| = k'_j\right\}$, then

$$\det(AM'_s) = \sum_{B \subseteq B_1 \cap B_2} \det(A_B) \det((M'_s)_B).$$

Now for any $B \subseteq B_1 \cap B_2$, note that $(M'_s)_B$ is again a block-diagonal matrix and the determinant of $(M'_s)_B$ is equal to the product of the determinants of the blocks. Thus, the maximum degree of s in $\det((M'_s)_B)$ is got when the maximum degree of t is achieved in each of the blocks. Further, if we focus on any block, the maximum degree of s is achieved when we choose the identity permutation, assuming that the rows are ordered in ascending order by weight and the columns are ordered in ascending order of the indices of y.

Again, for any $B \subseteq B_1 \cap B_2$, notice that the maximum degree of s achieved by $\det((M'_s)_B)$ is at most $\mathrm{wt}(A_B)$. Thus, for any $B \subseteq B_1 \cap B_2$ such that $A_B \neq A_0$, the maximum degree of s achieved by $\det((M'_s)_B) < \mathrm{wt}(A_B)$.

Finally, we can thus say that if $B_0 \subseteq B_1 \cap B_2$ is such that $A_{B_0} = A_0$, and d_0 is the maximum degree of s achieved by $\det((M'_s)_{B_0})$, then $d_0 = \mathrm{wt}(A_0)$, and the coefficient of t^{d_0} in $\det(AM'_s)$ is exactly $\det(A_0) \neq 0$. Hence, $\det(AM'_s) \neq 0$. □

6.4 A Small family of Faithful Maps

Note that the only property we used of wt is that each monomial gets a distinct weight. Thus if we define $\varphi(x_i) = \sum s^{j((t+1)^i \pmod p)} y_j$ and similarly define $w_i = (t+1)^i \pmod p$, then assuming t to be a constant we claim that there are not too many ps that we have to try out before we can ensure that the weight of every monomial is distinct.

The number of monomials possible in $\mathbf{x}$ is $\binom{n+t}{t} \approx n^t$. For any pair of monomials $\mathbf{x}^{\mathbf{e}}$, $\mathbf{x}^{\mathbf{e}'}$; a prime p is bad if it divides their weight. Note that the difference in weight between any pair of monomials is at most $t(t+1)^n$ and hence can have at most $n \log(t(t+1))$ distinct prime factors. Thus, the total number of bad primes is at most $n^{2t} \times n \log(t(t+1)) = O(n^{3t})$. Assuming t to be a constant, this is $\mathrm{poly}(n)$.

Further for each p that we try, we need to ensure that $\det(AM_s) \neq 0$ whenever $\det(AM_s)$ is a non-zero polynomial in s. This is ensured for some $s \in \{0, 1, \ldots, p\}$. Thus, given a set of polynomials $\{f_1, f_2, \ldots, f_m\}$ with constant inseparable degree, the following is a small family of faithful maps as required by Theorem 6.1.1.

$$\Phi_s = \left\{\varphi_{s,p}(x_i) = \sum s^{j((t+1)^i \bmod p)} y_j \;:\; p = O\left(n^{3t}\right), s \in \{0, 1, \ldots, p\}\right\}.$$

Using the observations in the first section of this chapter, we have thus formally proved the following theorem.

Theorem 6.4.1. *Given a set of polynomials $\{f_1, f_2, \ldots, f_m\} \in \mathbb{F}[x_1, x_2, \ldots, x_n]$ with inseparable degree t, there exists a $n^{\text{poly}(t)}$ sized family of linear maps Φ such that for some $\varphi \in \Phi$,*

$$\mathsf{algrank}(f_1, f_2, \ldots, f_m) = \mathsf{algrank}(f_1(\varphi, \ldots, f_m(\varphi))).$$

Thus, in the case where t is constant, we have a $\text{poly}(n)$ sized family of faithful maps.

6.5 PIT for Sparse Polynomials

We will now extend the sparse polynomial PIT presented in [BMS11] to fields of arbitrary characteristic. Let us assume that $\mathcal{C}$ is a circuit over m variables and $\{f_1, f_2, \ldots, f_m\} \subseteq \mathbb{F}[\mathbf{x}]$ is a set of s-sparse polynomials. Further, let their algebraic rank be at most k and their inseparable degree be t.

Since every f_i is s-sparse, so is each element in $\mathcal{H}(\mathbf{f}, \mathbf{v})$ for every $\mathbf{v}$. Hence, any $k \times k$ minor of $\mathcal{H}(\mathbf{f}, \mathbf{v})$ is $(k!s^k)$-sparse. For k constant, by the PIT result in [AB99], there is a $\text{poly}(n)$ sized hitting set for $\tilde{H}(\mathbf{f}, \mathbf{v})$ — the set of all $k \times k$ minors of $\mathcal{H}(\mathbf{f}, \mathbf{v})$. Thus, for t constant, Theorem 6.4.1 gives us a small family of maps Φ such that for atleast one $\varphi \in \Phi$, φ is faithful for $\{f_1, f_2, \ldots, f_m\}$.

By Lemma 5.3.1, checking whether $\mathcal{C}(f_1, f_2, \ldots, f_m) \neq 0$ is reduced to checking whether $\mathcal{C}(f_1(\varphi), f_2(\varphi), \ldots, f_m(\varphi)) \neq 0$. Since we are now dealing with a polynomial that depends on only constantly many variables, a trivial de-randomisation of the Schwartz-Zippel lemma gives a poly-sized hitting set.

Thus, we have proved the following theorem.

Theorem 6.5.1. *If $\{f_1, f_2, \ldots, f_m\} \in \mathbb{F}[x_1, x_2, \ldots, x_n]$ is a set of sparse polynomials with algebraic rank k and inseparable degree t, then for any circuit $\mathcal{C}$ over m variables, there is a $n^{\text{poly}(k,t)}$ time* PIT *for $\mathcal{C}(f_1, f_2, \ldots, f_m)$.*

Thus if k, t were constant, we have a $\text{poly}(n)$-time PIT.

7 Conclusion and Open Threads

In this thesis, we have focussed on the connection between Algebraic Independence and PITs. We started by surveying a few properties of algebraic independence and annihilating polynomials. We went on to discuss about the Jacobian Criterion and then the Jacobian-like criterion in [PSS16]. Finally we saw how these concepts were used to solve PITs in [BMS11] and [ASSS12].

We noticed that their technique used the Jacobian Criterion and hence required the field to have characteristic zero. We then used the [PSS16] criterion to construct "faithful maps" over arbitrary fields. This allowed us to extend the sparse polynomial PIT result of [BMS11] to arbitrary fields, in the case where the inseparable degree is constant.

A natural way forward is of course to try and extend the PIT results in [ASSS12]. Also, while working on this thesis, we made the following observations which provide a couple of interesting threads that need to be investigated further.

A Basis Isolating Weight Assignment will also work

Recently Agrawal-Gurjar-Korwar-Saxena [AGKS14] introduced the concept of a basis isolating weight assignment (or BIWA), while trying to solve PIT for a class of circuits called ROABPs. Interestingly, BIWAs have a lot of rank extractor like properties, and this was used in [AGKS14] and a thread of subsequent works.

Let $\mathsf{wt} : \{x_i\}_{i\in[n]} \to \mathbb{N}^l$ be a weight assignment. Extend it to define a weight for monomials in the usual manner: $\mathsf{wt}(\mathbf{x^e}) = \sum_{i=1}^{n} e_i x_i$. We say that wt is a BIWA for a class of polynomials if when we write these down as vectors, the corresponding matrix with columns indexed by monomials in $x_1, x_2, \ldots, x_n$ has the following property.

There should exist some basis $\mathcal{B}$ from among the set of columns such that

- Weights of distinct monomials among the set of indices of $\mathcal{B}$ are distinct.
- If $\mathbf{x^e} \notin \mathcal{B}$, then it is spanned by columns with indices having weight strictly greater than $\mathsf{wt}(\mathbf{x^e})$.

It is interesting to note that in our context, instead of defining $\varphi_s(x_i) = \sum s^{j(t^i \bmod p)}$, if we define

$$\varphi_s(x_i) = \sum s^{\mathsf{wt}(i)j}$$

where wt is a BIWA for $\mathcal{H}(\mathbf{f}, \mathbf{v})$, our proof will continue to hold.

To see why this is the case, we keep the weight of a minor as earlier. Note however, that when we arrange the column indices by weight, the sequence is now non-decreasing and not strictly increasing. Thus, if we ensure that the basis isolated by the BIWA is the unique minor with maximum weight, then the rest of the arguments remain the same.

Let us call $\mathcal{B}$ the basis isolated by wt and let M be any non-zero minor. Say $\mathcal{B}$ has columns indexed by $\mathbf{x}^{\mathbf{e}_1}, \ldots, \mathbf{x}^{\mathbf{e}_{k'}}$ with $\mathsf{wt}(\mathbf{x}^{\mathbf{e}_1}) < \mathsf{wt}(\mathbf{x}^{\mathbf{e}_2}) < \ldots < \mathsf{wt}(\mathbf{x}^{\mathbf{e}_{k'}})$ and M has columns indexed by $\mathbf{x}^{\mathbf{e}'_1}, \ldots, \mathbf{x}^{\mathbf{e}'_{k'}}$ with $\mathsf{wt}(\mathbf{x}^{\mathbf{e}'_1}) \leq \mathsf{wt}(\mathbf{x}^{\mathbf{e}'_2}) \leq \ldots \leq \mathsf{wt}(\mathbf{x}^{\mathbf{e}'_{k'}})$.

By the property of BIWAs, for any $i \in [k']$, the space of columns with indices having weight $\geq \mathsf{wt}(\mathbf{x}^{\mathbf{e}_i})$ has dimension $(k' - i)$ if we remove the column indexed by $\mathbf{x}^{\mathbf{e}_i}$ from it. Thus, for any $i \in [k']$,

$$\mathbf{x}^{\mathbf{e}_i} \neq \mathbf{x}^{\mathbf{e}'_i} \Rightarrow \mathsf{wt}(\mathbf{x}^{\mathbf{e}_i}) > \mathsf{wt}(\mathbf{x}^{\mathbf{e}'_i})$$

and so clearly, if $M \neq \mathcal{B}$, then $\mathsf{wt}(M) < \mathsf{wt}(\mathcal{B})$.

Thus, constructing faithful maps boil down to constructing BIWAs for some class of polynomials, depending on which circuit class we started with. This leads us to ask the natural question of whether we can also construct faithful maps for circuit classes for which BIWAs are known.

Working with high inseparable degree

The [PSS16] criterion shows that checking algebraic independence of a set of polynomials can be reduced to checking the rank of a Jacobian-like matrix. While constructing faithful maps, we realised that after we make a substitution for the variables, checking the rank of this matrix reduces to checking the rank of a sub-matrix that have columns indexed by only "pure monomials".

The reason we needed the inseparable degree t to be constant was that the matrix whose rank had to be tested had as many columns as the number of monomials of degree at most t. The natural question to ask is thus whether we can make some local substitution which will allow us to check algebraic independence by checking the rank of matrix with columns indexed by only "pure monomials". This would drastically reduce the size of the matrix under consideration and hence might allow us to construct faithful maps even when the inseparable degree is large.

Bibliography

[AB99] Manindra Agrawal and Somenath Biswas. „Primality and Identity Testing via Chinese Remaindering“. In: *40th Annual Symposium on Foundations of Computer Science, FOCS '99, 17-18 October, 1999, New York, NY, USA*. 1999, pp. 202–209. URL: https://doi.org/10.1109/SFFCS.1999.814592 (cit. on pp. 2, 39).

[AGKS14] Manindra Agrawal, Rohit Gurjar, Arpita Korwar, and Nitin Saxena. „Hitting-sets for ROABP and Sum of Set-Multilinear circuits“. In: *CoRR* abs/1406.7535 (2014). arXiv: 1406.7535. URL: http://arxiv.org/abs/1406.7535 (cit. on p. 41).

[Agr05] Manindra Agrawal. „Proving Lower Bounds Via Pseudo-random Generators“. In: *FSTTCS 2005: Foundations of Software Technology and Theoretical Computer Science, 25th International Conference, Hyderabad, India, December 15-18, 2005, Proceedings*. 2005, pp. 92–105. URL: https://doi.org/10.1007/11590156_6 (cit. on p. 1).

[Agr11] Manindra Agrawal. „On the Arithmetic Complexity of Euler Function“. In: *Computer Science - Theory and Applications - 6th International Computer Science Symposium in Russia, CSR 2011, St. Petersburg, Russia, June 14-18, 2011. Proceedings*. 2011, pp. 43–49. URL: https://doi.org/10.1007/978-3-642-20712-9_4 (cit. on p. 1).

[ASS12] Manindra Agrawal, Chandan Saha, and Nitin Saxena. „Quasi-polynomial Hitting-set for Set-depth-Δ Formulas“. In: *Electronic Colloquium on Computational Complexity (ECCC)* 19 (2012), p. 113. URL: http://eccc.hpi-web.de/report/2012/113 (cit. on p. 2).

[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 44th Symposium on Theory of Computing Conference, STOC 2012, New York, NY, USA, May 19 - 22, 2012*. 2012, pp. 599–614. URL: http://doi.acm.org/10.1145/2213977.2214033 (cit. on pp. v, 3–5, 7, 29, 30, 41).

[AV08] Manindra Agrawal and V. Vinay. „Arithmetic Circuits: A Chasm at Depth Four“. In: *49th Annual IEEE Symposium on Foundations of Computer Science, FOCS 2008, October 25-28, 2008, Philadelphia, PA, USA*. 2008, pp. 67–75. URL: https://doi.org/10.1109/FOCS.2008.32 (cit. on p. 2).

[BMS11] Malte Beecken, Johannes Mittmann, and Nitin Saxena. „Algebraic Independence and Blackbox Identity Testing“. In: *CoRR* abs/1102.2789 (2011). URL: http://arxiv.org/abs/1102.2789 (cit. on pp. v, 3–5, 29, 30, 39, 41).

[CLO97] David A. Cox, John Little, and Donal O'Shea. *Ideals, varieties, and algorithms - an introduction to computational algebraic geometry and commutative algebra (2. ed.)* Undergraduate texts in mathematics. Springer, 1997 (cit. on p. 11).

[DL78] Richard A. DeMillo and Richard J. Lipton. „A Probabilistic Remark on Algebraic Program Testing". In: *Inf. Process. Lett.* 7.4 (1978), pp. 193–195. URL: https://doi.org/10.1016/0020-0190(78)90067-4 (cit. on p. 2).

[DS05] Zeev Dvir and Amir Shpilka. „Locally decodable codes with 2 queries and polynomial identity testing for depth 3 circuits". In: *Proceedings of the 37th Annual ACM Symposium on Theory of Computing, Baltimore, MD, USA, May 22-24, 2005*. 2005, pp. 592–601. URL: http://doi.acm.org/10.1145/1060590.1060678 (cit. on p. 2).

[DSY08] Zeev Dvir, Amir Shpilka, and Amir Yehudayoff. „Hardness-randomness tradeoffs for bounded depth arithmetic circuits". In: *Proceedings of the 40th Annual ACM Symposium on Theory of Computing, Victoria, British Columbia, Canada, May 17-20, 2008*. 2008, pp. 741–748. URL: http://doi.acm.org/10.1145/1374376.1374482 (cit. on p. 1).

[FS13] Michael A. Forbes and Amir Shpilka. „Quasipolynomial-Time Identity Testing of Non-commutative and Read-Once Oblivious Algebraic Branching Programs". In: *54th Annual IEEE Symposium on Foundations of Computer Science, FOCS 2013, 26-29 October, 2013, Berkeley, CA, USA*. 2013, pp. 243–252. URL: https://doi.org/10.1109/FOCS.2013.34 (cit. on p. 2).

[GKKS13] Ankit Gupta, Pritish Kamath, Neeraj Kayal, and Ramprasad Saptharishi. „Arithmetic Circuits: A Chasm at Depth Three". In: *54th Annual IEEE Symposium on Foundations of Computer Science, FOCS 2013, 26-29 October, 2013, Berkeley, CA, USA*. 2013, pp. 578–587. URL: https://doi.org/10.1109/FOCS.2013.68 (cit. on p. 2).

[GKS16] Rohit Gurjar, Arpita Korwar, and Nitin Saxena. „Identity Testing for Constant-Width, and Commutative, Read-Once Oblivious ABPs". In: *31st Conference on Computational Complexity, CCC 2016, May 29 to June 1, 2016, Tokyo, Japan*. 2016, 29:1–29:16. URL: https://doi.org/10.4230/LIPIcs.CCC.2016.29 (cit. on p. 2).

[GR05] Ariel Gabizon and Ran Raz. „Deterministic Extractors for Affine Sources over Large Fields". In: *46th Annual IEEE Symposium on Foundations of Computer Science (FOCS 2005), 23-25 October 2005, Pittsburgh, PA, USA, Proceedings*. 2005, pp. 407–418. URL: https://doi.org/10.1109/SFCS.2005.31 (cit. on p. 27).

[HS80] Joos Heintz and Claus-Peter Schnorr. „Testing Polynomials which Are Easy to Compute (Extended Abstract)". In: *Proceedings of the 12th Annual ACM Symposium on Theory of Computing, April 28-30, 1980, Los Angeles, California, USA*. 1980, pp. 262–272. URL: http://doi.acm.org/10.1145/800141.804674 (cit. on p. 1).

[Jac41] C.G.J. Jacobi. „De Determinantibus functionalibus." lat. In: *Journal für die reine und angewandte Mathematik* 22 (1841), pp. 319–359. URL: http://eudml.org/doc/147138 (cit. on p. 13).

[Kay09] Neeraj Kayal. „The Complexity of the Annihilating Polynomial“. In: *Proceedings of the 24th Annual IEEE Conference on Computational Complexity, CCC 2009, Paris, France, 15-18 July 2009*. 2009, pp. 184–193. URL: https://doi.org/10.1109/CCC.2009.37 (cit. on pp. 10, 11).

[Kay10] Neeraj Kayal. „Algorithms for Arithmetic Circuits“. In: *Electronic Colloquium on Computational Complexity (ECCC)* 17 (2010), p. 73. URL: http://eccc.hpi-web.de/report/2010/073 (cit. on p. 2).

[Kay12] Neeraj Kayal. „An exponential lower bound for the sum of powers of bounded degree polynomials“. In: *Electronic Colloquium on Computational Complexity (ECCC)* 19 (2012), p. 81. URL: http://eccc.hpi-web.de/report/2012/081 (cit. on p. 2).

[KI03] Valentine Kabanets and Russell Impagliazzo. „Derandomizing polynomial identity tests means proving circuit lowerbounds“. In: *Proceedings of the 35th Annual ACM Symposium on Theory of Computing, June 9-11, 2003, San Diego, CA, USA*. 2003, pp. 355–364. URL: http://doi.acm.org/10.1145/780542.780595 (cit. on p. 1).

[Kna07] Anthony W Knapp. *Advanced algebra*. Springer Science & Business Media, 2007 (cit. on p. 19).

[Koi12] Pascal Koiran. „Arithmetic circuits: The chasm at depth four gets wider“. In: *Theor. Comput. Sci.* 448 (2012), pp. 56–65. URL: https://doi.org/10.1016/j.tcs.2012.03.041 (cit. on p. 2).

[KS01] Adam R. Klivans and Daniel A. Spielman. „Randomness efficient identity testing of multivariate polynomials“. In: *Proceedings on 33rd Annual ACM Symposium on Theory of Computing, July 6-8, 2001, Heraklion, Crete, Greece*. 2001, pp. 216–223. URL: http://doi.acm.org/10.1145/380752.380801 (cit. on p. 2).

[KS07] Neeraj Kayal and Nitin Saxena. „Polynomial Identity Testing for Depth 3 Circuits“. In: *Computational Complexity* 16.2 (2007), pp. 115–138. URL: https://doi.org/10.1007/s00037-007-0226-9 (cit. on p. 2).

[KS09] Neeraj Kayal and Shubhangi Saraf. „Blackbox Polynomial Identity Testing for Depth 3 Circuits“. In: *50th Annual IEEE Symposium on Foundations of Computer Science, FOCS 2009, October 25-27, 2009, Atlanta, Georgia, USA*. 2009, pp. 198–207. URL: https://doi.org/10.1109/FOCS.2009.67 (cit. on p. 2).

[Oxl06] James G Oxley. *Matroid theory*. Vol. 3. Oxford University Press, USA, 2006 (cit. on pp. 3, 7).

[PSS16] Anurag Pandey, Nitin Saxena, and Amit Sinhababu. „Algebraic Independence over Positive Characteristic: New Criterion and Applications to Locally Low Algebraic Rank Circuits“. In: *41st International Symposium on Mathematical Foundations of Computer Science, MFCS 2016, August 22-26, 2016 - Kraków, Poland*. 2016, 74:1–74:15. URL: https://doi.org/10.4230/LIPIcs.MFCS.2016.74 (cit. on pp. v, 4, 5, 19–21, 23, 31, 41, 42).

[Sax08] Nitin Saxena. „Diagonal Circuit Identity Testing and Lower Bounds“. In: *Automata, Languages and Programming, 35th International Colloquium, ICALP 2008, Reykjavik, Iceland, July 7-11, 2008, Proceedings, Part I: Tack A: Algorithms, Automata, Complexity, and Games*. 2008, pp. 60–71. URL: https://doi.org/10.1007/978-3-540-70575-8_6 (cit. on p. 2).

[Sch80] Jacob T. Schwartz. „Fast Probabilistic Algorithms for Verification of Polynomial Identities“. In: *J. ACM* 27.4 (1980), pp. 701–717. URL: http://doi.acm.org/10.1145/322217.322225 (cit. on p. 2).

[SS09] Nitin Saxena and C. Seshadhri. „An Almost Optimal Rank Bound for Depth-3 Identities“. In: *Proceedings of the 24th Annual IEEE Conference on Computational Complexity, CCC 2009, Paris, France, 15-18 July 2009*. 2009, pp. 137–148. URL: https://doi.org/10.1109/CCC.2009.20 (cit. on p. 2).

[SS10] Nitin Saxena and C. Seshadhri. „From Sylvester-Gallai Configurations to Rank Bounds: Improved Black-Box Identity Test for Depth-3 Circuits“. In: *51th Annual IEEE Symposium on Foundations of Computer Science, FOCS 2010, October 23-26, 2010, Las Vegas, Nevada, USA*. 2010, pp. 21–29. URL: https://doi.org/10.1109/FOCS.2010.9 (cit. on p. 2).

[SS11] Nitin Saxena and C. Seshadhri. „Blackbox identity testing for bounded top fanin depth-3 circuits: the field doesn't matter“. In: *Proceedings of the 43rd ACM Symposium on Theory of Computing, STOC 2011, San Jose, CA, USA, 6-8 June 2011*. 2011, pp. 431–440. URL: http://doi.acm.org/10.1145/1993636.1993694 (cit. on p. 2).

[SV11] Shubhangi Saraf and Ilya Volkovich. „Black-box identity testing of depth-4 multilinear circuits“. In: *Proceedings of the 43rd ACM Symposium on Theory of Computing, STOC 2011, San Jose, CA, USA, 6-8 June 2011*. 2011, pp. 421–430. URL: http://doi.acm.org/10.1145/1993636.1993693 (cit. on p. 2).

[Tav15] Sébastien Tavenas. „Improved bounds for reduction to depth 4 and depth 3“. In: *Inf. Comput.* 240 (2015), pp. 2–11. URL: https://doi.org/10.1016/j.ic.2014.09.004 (cit. on p. 2).

[Val79] Leslie G. Valiant. „Completeness Classes in Algebra“. In: *Proceedings of the 11h Annual ACM Symposium on Theory of Computing, April 30 - May 2, 1979, Atlanta, Georgia, USA*. 1979, pp. 249–261. URL: http://doi.acm.org/10.1145/800135.804419 (cit. on p. 1).

[Zip79] Richard Zippel. „Probabilistic algorithms for sparse polynomials“. In: *Symbolic and Algebraic Computation, EUROSAM '79, An International Symposiumon Symbolic and Algebraic Computation, Marseille, France, June 1979, Proceedings*. 1979, pp. 216–226. URL: https://doi.org/10.1007/3-540-09519-5_73 (cit. on p. 2).