Independence in Algebraic Complexity Theory

Dissertation

zur

Erlangung des Doktorgrades (Dr. rer. nat.)

der

Mathematisch-Naturwissenschaftlichen Fakultät

der

Rheinischen Friedrich-Wilhelms-Universität Bonn

vorgelegt von

Johannes Mittmann

aus

Nürnberg

Bonn, Dezember 2012

Angefertigt mit Genehmigung der Mathematisch-Naturwissenschaftlichen
Fakultät der Rheinischen Friedrich-Wilhelms-Universität Bonn

1. Gutachter: Prof. Dr. Nitin Saxena
2. Gutachter: Prof. Dr. Markus Bläser
Tag der Promotion: 5. Dezember 2013
Erscheinungsjahr: 2013

Zusammenfassung

Die vorliegende Arbeit untersucht die Konzepte der linearen und algebraischen Unabhängigkeit innerhalb der algebraischen Komplexitätstheorie.

Arithmetische Schaltkreise, die multivariate Polynome über einem Körper berechnen, bilden die Grundlage unserer Komplexitätsbetrachtungen. Wir befassen uns mit dem *polynomial identity testing* (PIT) Problem, bei dem entschieden werden soll ob ein gegebener Schaltkreis das Nullpolynom berechnet. Für dieses Problem sind effiziente randomisierte Algorithmen bekannt, aber deterministische Polynomialzeitalgorithmen konnten bisher nur für eingeschränkte Klassen von Schaltkreisen angegeben werden. Besonders von Interesse sind Blackbox-Algorithmen, welche den gegebenen Schaltkreis nicht inspizieren, sondern lediglich an Punkten auswerten.

Bekannte Ansätze für das PIT Problem basieren auf den Begriffen der linearen Unabhängigkeit und des Rangs von Untervektorräumen des Polynomrings. Wir übertragen diese Methoden auf algebraische Unabhängigkeit und den Transzendenzgrad von Unteralgebren des Polynomrings. Dadurch erhalten wir effiziente Blackbox-PIT-Algorithmen für neue Klassen von Schaltkreisen.

Eine effiziente Charakterisierung der algebraischen Unabhängigkeit von Polynomen ist durch das Jacobi-Kriterium gegeben. Dieses Kriterium ist jedoch nur in Charakteristik Null gültig. Wir leiten ein neues Jacobi-artiges Kriterium für die algebraische Unabhängigkeit von Polynomen über endlichen Körpern her. Dieses liefert einen weiteren Blackbox-PIT-Algorithmus und verbessert die Komplexität des Problems arithmetische Schaltkreise über endlichen Körpern auf algebraische Unabhängigkeit zu testen.

Synopsis

This thesis examines the concepts of linear and algebraic independence in algebraic complexity theory.

Arithmetic circuits, computing multivariate polynomials over a field, form the framework of our complexity considerations. We are concerned with polynomial identity testing (PIT), the problem of deciding whether a given arithmetic circuit computes the zero polynomial. There are efficient randomized algorithms known for this problem, but as yet deterministic polynomial-time algorithms could be found only for restricted circuit classes. We are especially interested in blackbox algorithms, which do not inspect the given circuit, but solely evaluate it at some points.

Known approaches to the PIT problem are based on the notions of linear independence and rank of vector subspaces of the polynomial ring. We generalize those methods to algebraic independence and transcendence degree of subalgebras of the polynomial ring. Thereby, we obtain efficient blackbox PIT algorithms for new circuit classes.

The Jacobian criterion constitutes an efficient characterization for algebraic independence of polynomials. However, this criterion is valid only in characteristic zero. We deduce a novel Jacobian-like criterion for algebraic independence of polynomials over finite fields. We apply it to obtain another blackbox PIT algorithm and to improve the complexity of testing the algebraic independence of arithmetic circuits over finite fields.

Acknowledgements

I am deeply indebted to my advisor Nitin Saxena. I would like to thank him for sharing his expertise with me and for pointing me in the right direction. Our countless research sessions have been highly pleasant and beneficial for me. Without his guidance and support this thesis would not have been possible.

Working with my co-authors Malte Mink (né Malte Beecken) and Peter Scheiblechner has also been a great pleasure for me. I would like to thank them for many interesting scientific and non-scientific discussions.

I am very grateful to the Hausdorff Center for Mathematics, Bonn, for its financial support and for providing an excellent working environment.

Finally, I would like to thank my parents for their everlasting encouragement and support.

Contents

Chapter 1

Introduction

Algebraic complexity theory studies the computational resources required to solve algebraic problems algorithmically. A large class of algebraic and symbolic computations deal with polynomials in one or several variables.

The standard model for computations with multivariate polynomials are *arithmetic circuits*. Starting with variables $\boldsymbol{x} = \{x_1, \ldots, x_n\}$ and constants from a field K, an arithmetic circuit C computes an element of the polynomial ring $K[\boldsymbol{x}]$ by recursively adding and multiplying already computed expressions. The circuit C can be modeled by a directed acyclic graph whose sources are labeled with a variable or constant and whose remaining vertices are labeled with $+$ or $\times$. We define the *size* of C as the number vertices and edges in this graph. The *depth* of C is defined as the length of a longest directed path.

The most fundamental open problem connected with arithmetic circuits is to prove super-polynomial *lower bounds*, i. e. find an explicit polynomial of polynomial degree that cannot be computed by a polynomial-size circuit. In this thesis we are concerned with a computational problem that is seemingly unrelated to lower bounds.

Polynomial identity testing

Polynomial identity testing (PIT) is the problem of deciding whether a given arithmetic circuit C computes the zero polynomial. Note that over finite fields this is a different question than asking whether a circuit computes the zero function $K^n \to K$.

There is a *randomized* polynomial-time algorithm known for PIT which is based on the *Schwartz–Zippel lemma* [Sch80, Zip79, DL78]. In simplified form, this test runs as follows: Given a circuit C, pick a point $\boldsymbol{a} \in K^n$ at random and declare "C computes the zero polynomial" if and only if

$C(\boldsymbol{a}) = 0$. By the Schwartz–Zippel lemma, the probability that we pick a root of a non-zero circuit is small, thus PIT is in **coRP**.

Giving a *deterministic* polynomial-time algorithm for PIT is a major open problem. Surprisingly, derandomizing PIT is related to proving arithmetic and boolean circuit lower bounds [KI04, DSY09].

The importance of PIT is further underlined by many algorithmic applications such as primality testing [AB03, AKS04], perfect matchings [Lov79, GK87, Agr03, AHT07], matrix completion [Lov89], equivalence testing of read-once branching programs [BCW80, IM83], multiset equality testing [BK95, CK00], or equivalence testing of probabilistic automata [KMO$^+$12]. In complexity theory, identity tests for polynomials played a role in proving **IP** = **PSPACE** [LFKN92, Sha92], **MIP** = **NEXP** [BFL91], and the **PCP**-Theorems [BFLS91, FGL$^+$96, AS98, ALM$^+$98]. Recently, PIT has also found applications in geometric complexity theory [Mul12].

The randomized Schwartz–Zippel test is an example of a *blackbox* PIT algorithm, because it relies solely on evaluations and does not "look inside" the arithmetic circuit. Blackbox algorithms require the computation of hitting sets. A *hitting set* for a class of circuits $\mathcal{C}$ over $K[\boldsymbol{x}]$ is a set of points $\mathcal{H} \subseteq K^n$ such that for all non-zero circuits $C \in \mathcal{C}$ there exists $\boldsymbol{a} \in \mathcal{H}$ satisfying $C(\boldsymbol{a}) \neq 0$. There is interest in deterministic blackbox algorithms, because of direct connections to arithmetic circuit lower bounds [HS80a, Agr05].

Since derandomizing PIT in general seems to be a complicated endeavor, attempts have been made for restricted circuit classes. A natural restriction is to consider *constant-depth* circuits. In depth 2, it suffices to consider $\Sigma\Pi$-circuits computing sums of monomials. For those circuits, PIT is trivial, and also polynomial-time blackbox algorithms are known [KS01, BHLV09]. In depth 3, we may limit ourselves to examine $\Sigma\Pi\Sigma$-circuits of the form $\sum_{i=1}^{k} \prod_{j=1}^{\delta} \ell_{i,j}$, computing sums of products of linear forms $\ell_{i,j}$. Even for this class of circuits the PIT question is open. However, in the case of constant *top fan-in* k, a polynomial-time blackbox algorithm was found [SS11b]. Special classes of depth-4 circuits were considered in [Sax08, AM10, SV11]. On the other hand, a polynomial-time blackbox PIT algorithm for (unrestricted) depth-4 circuits would already imply a quasipolynomial-time PIT algorithm for low-degree circuits [AV08], hence, in some sense, depth-4 circuits can be regarded as a very general case.

Linear independence

Many known PIT algorithms work by *reducing* the number of variables of a given arithmetic circuit C. Such a reduction can be achieved by replacing the input variables $\boldsymbol{x}$ by elements of a polynomial ring $K[\boldsymbol{z}] = K[z_1, \ldots, z_r]$ with

less variables. Algebraically, this amounts to applying a K-algebra homomorphism $\varphi\colon K[\boldsymbol{x}] \to K[\boldsymbol{z}]$ to C. To be useful for PIT, the homomorphism should satisfy $\varphi(C) = 0$ if and only if $C = 0$.

The concept of linear independence in $K[\boldsymbol{x}]$, viewed as K-vector space, can be beneficial for finding a desired homomorphism. A set of polynomials $\{f_1, \ldots, f_m\} \subset K[\boldsymbol{x}]$ is called *K-linearly independent* if $\lambda_1 f_1 + \cdots + \lambda_m f_m \neq 0$ for all non-zero $\lambda \in K^m$. A vector $\lambda \in K^m$ satisfying $\lambda_1 f_1 + \cdots + \lambda_m f_m = 0$ is called a *linear relation* of $f_1, \ldots, f_m$. The *rank* of the set $\{f_1, \ldots, f_m\}$, denoted by $\mathrm{rk}_K(f_1, \ldots, f_m)$, is the cardinality of a maximal linearly independent subset.

We say that the homomorphism φ is *rank-preserving* for $\{f_1, \ldots, f_m\}$ if it satisfies

$$\mathrm{rk}_K(\varphi(f_1), \ldots, \varphi(f_m)) = \mathrm{rk}_K(f_1, \ldots, f_m).$$

In this case, φ is injective on the K-subspace $\langle f_1, \ldots, f_m \rangle_K$ spanned by $f_1, \ldots, f_m$. In particular, it preserves the non-zeroness of circuits $C = \lambda_1 f_1 + \cdots + \lambda_m f_m$ living in that space. Rank-preserving homomorphisms for sets of linear forms found applications in blackbox PIT algorithms for $\Sigma\Pi\Sigma$-circuits with constant top fan-in [KS11a, SS11b]. They were obtained from a construction of rank-preserving matrices in [GR08].

Linear independence testing is the problem of deciding whether given arithmetic circuits $C_1, \ldots, C_m$ are linearly independent. It reduces to (the complement of) PIT and is therefore contained in **RP** [Kay10]. This follows from a characterization of linear independence of polynomials which we term *alternant criterion*. It says that polynomials $f_1, \ldots, f_m$ are linearly independent if and only if

$$\det\big(f_i(\boldsymbol{t}_j)\big)_{i,j} \neq 0,$$

where $\boldsymbol{t}_1, \ldots, \boldsymbol{t}_m$ are disjoint tuples of respectively n variables. Since determinants can be computed by polynomial-size circuits [Ber84], we obtain the desired reduction.

The computation of a basis of the K-subspace of linear relations can be considered a search version of linear independence testing. This problem was dealt with in [Kay10, CKW11] and can be solved by PIT methods as well.

Algebraic independence

Algebraic independence is a generalization of linear independence. It is a well-known concept from field theory, but is also applicable to K-algebras such as $K[\boldsymbol{x}]$. A set of polynomials $\{f_1, \ldots, f_m\} \subset K[\boldsymbol{x}]$ is called *algebraically independent* over K if $F(f_1, \ldots, f_m) \neq 0$ for all non-zero polynomials $F \in$

$K[\boldsymbol{y}] = K[y_1, \ldots, y_m]$. A polynomial $F \in K[\boldsymbol{y}]$ satisfying $F(f_1, \ldots, f_m) = 0$ is called an *algebraic relation* of $f_1, \ldots, f_m$. A non-zero algebraic relation is also called an *annihilating polynomial*. The *transcendence degree* of the set $\{f_1, \ldots, f_m\}$, denoted by $\operatorname{trdeg}_K(f_1, \ldots, f_m)$, is the cardinality of a maximal algebraically independent subset.

Algebraic independence testing is the problem of deciding whether given arithmetic circuits $C_1, \ldots, C_m$ are algebraically independent. An effective criterion for algebraic independence is provided by *Perron's degree bound* for annihilating polynomials [Per27]. This bound is exponential in the number of variables, but can be shown to be best possible. It enables the computation of annihilating polynomials by linear algebra and puts algebraic independence testing in **PSPACE**. The *Jacobian criterion* [Jac41] constitutes a more efficient characterization, which is applicable if the characteristic of K is zero (or sufficiently large for given polynomials). It says that polynomials $f_1, \ldots, f_n$ are algebraically independent if and only if

$$\det J_{\boldsymbol{x}}(f_1, \ldots, f_n) \neq 0,$$

where $J_{\boldsymbol{x}}(f_1, \ldots, f_n) = \left(\partial_{x_j} f_i\right)_{i,j}$ denotes the *Jacobian matrix*. In characteristic $p > 0$, the Jacobian criterion fails due to $\partial_x x^p = 0$. Since the partial derivatives of a circuit can be computed efficiently [BS83], algebraic independence testing in characteristic zero reduces to (the complement of) PIT and is therefore contained in **RP** [DGW09].

The computation of a generating system for the ideal of algebraic relations can be considered a search version of the algebraic independence testing problem. This can be done by Gröbner basis methods in exponential space. Even the computation of a single annihilating polynomial can be shown to be a hard problem [Kay09].

In complexity theory, the notions of algebraic independence and transcendence degree were applied to find program invariants [L'v84], to prove arithmetic circuit lower bounds [Kal85, ASSS12], and for randomness extractors [DGW09, Dvi09]. In this thesis we bring algebraic independence into the realm of PIT.

1.1 Contributions

Central parts of this thesis have already been published in form of two refereed papers [BMS11, BMS13] and a preprint [MSS12]. Our main results can be divided into two parts accordingly.

Faithful homomorphisms

The first main contribution of this thesis is a new approach to PIT based on the notions of algebraic independence and transcendence degree. This research was initiated as joint work with Malte Beecken (now Malte Mink) and Nitin Saxena [BMS11, BMS13] and is expanded in this thesis.

Taking rank-preserving homomorphisms as a role model, we consider K-algebra homomorphisms $\varphi\colon K[\boldsymbol{x}] \to K[\boldsymbol{z}]$ preserving the transcendence degree of polynomials. We say that φ is *faithful* to a set of polynomials $\{f_1, \ldots, f_m\} \subset K[\boldsymbol{x}]$ if

$$\operatorname{trdeg}_K(\varphi(f_1), \ldots, \varphi(f_m)) = \operatorname{trdeg}_K(f_1, \ldots, f_m).$$

We show that, in this case, φ is injective on the K-subalgebra $K[f_1, \ldots, f_m]$ generated by $f_1, \ldots, f_m$. In particular, it preserves the non-zeroness of circuits $C = F(f_1, \ldots, f_m)$ living in that subalgebra. In this way, faithful homomorphisms enable us to reduce the number of variables from n to r.

This motivates the first application of faithful homomorphisms. Let F be a polynomial-degree circuit over $K[\boldsymbol{y}]$ and let $f_1, \ldots, f_m$ be polynomial-degree circuits over $K[\boldsymbol{x}]$ of *constant* transcendence degree r. If we can construct faithful homomorphisms efficiently and "in a blackbox way" for sets of type $\{f_1, \ldots, f_m\}$, then we obtain an efficient hitting set construction for circuits of the form $C = F(f_1, \ldots, f_m)$. In this thesis, we give such constructions for the cases that $f_1, \ldots, f_m$ are linear forms, monomials, constant-degree polynomials, sparse polynomials (in zero or sufficiently large characteristic), and products of constant-degree forms (of transcendence degree 2). A further construction of this type will be mentioned below. Note that those results are non-trivial, because both m and the number of variables n are unbounded. In particular, C might have exponential sparsity.

As a second application of faithful homomorphisms, we generalize the rank-based approach for $\Sigma\Pi\Sigma$-circuits with bounded top fan-in by [DS07, KS11a]. We consider $\Sigma\Pi\Sigma\Pi$-circuits with bounded top and bottom fan-in, i. e. circuits of the form $\sum_{i=1}^{k} \prod_{j=1}^{d} f_{i,j}$, where k is constant and $f_{i,j}$ are constant-degree polynomials given in sparse $\Sigma\Pi$-representation. We propose a blackbox algorithm for this circuit class. For $k \geq 3$, this test is conditional in the sense that its efficiency depends on proving a certain *rank bound*. This question we leave open.

The Witt-Jacobian criterion

The second main result of this thesis is a novel Jacobian-like criterion for algebraic independence of polynomials over finite fields. We term it the

Witt-Jacobian criterion. This is joint work with Nitin Saxena and Peter Scheiblechner [MSS12].

Let $\mathbb{F}_q$ be a finite field of characteristic $p > 0$ and let $f_1, \ldots, f_n \in \mathbb{F}_q[\boldsymbol{x}]$ be polynomials of degree at most δ.

The idea of the Witt-Jacobian criterion is to lift polynomials from $\mathbb{F}_q[\boldsymbol{x}]$ to $\mathbb{Z}_q[\boldsymbol{x}]$, where $\mathbb{Z}_q := \mathrm{W}(\mathbb{F}_q)$ is the ring of *Witt vectors* of $\mathbb{F}_q$. The ring $\mathbb{Z}_q$ has characteristic zero and is the ring of integers of an unramified extension of the p-adic numbers. We have $\mathbb{Z}_q/\langle p\rangle = \mathbb{F}_q$, so we can choose lifts $g_1, \ldots, g_n \in \mathbb{Z}_q[\boldsymbol{x}]$ such that $f_i = g_i \pmod{\langle p\rangle}$ for all $i \in [n]$.

The criterion is stated via a degeneracy condition for polynomials in $\mathbb{Z}_q[\boldsymbol{x}]$. Let $\ell \geq 0$. For a non-zero exponent vector $\alpha \in \mathbb{N}^n$, we denote by $v_p(\alpha)$ the maximal number $v \in \mathbb{N}$ such that p^v divides α_i for all $i \in [n]$. Furthermore, we set $v_p(\mathbf{0}) := \infty$. A polynomial $g \in \mathbb{Z}_q[\boldsymbol{x}]$ is called $(\ell+1)$-*degenerate* if the coefficient of $\boldsymbol{x}^\alpha$ in g is divisible by $p^{\min\{v_p(\alpha),\ell\}+1}$ for all $\alpha \in \mathbb{N}$.

Now fix some $\ell \geq n \cdot \log_p(\delta)$. Then the Witt-Jacobian criterion says that $f_1, \ldots, f_n$ are algebraically independent over $\mathbb{F}_q$ if and only if the polynomial

$$g := (g_1 \cdots g_n)^{p^\ell - 1} \cdot x_1 \cdots x_n \cdot \det J_{\boldsymbol{x}}(g_1, \ldots, g_n) \in \mathbb{Z}_q[\boldsymbol{x}]$$

is not $(\ell+1)$-degenerate.

We call g the *Witt-Jacobian polynomial* of $g_1, \ldots, g_n$. The main tool for the proof of the criterion is the *de Rham-Witt complex* constructed by Illusie [Ill79].

We also give two applications of the Witt-Jacobian criterion. First, we use it to efficiently construct faithful homomorphisms for polynomials of sub-logarithmic sparsity over $\mathbb{F}_q$. This looks like a rather weak result, but this method is more efficient than our constructions based on classical criteria in small prime characteristic.

The second application is an algorithm for the algebraic independence testing problem over $\mathbb{F}_q$. We show that this problem is in $\mathbf{NP}^{\#\mathbf{P}}$, i. e. it can be decided by a non-deterministic polynomial-time Turing machine with a $\#\mathbf{P}$-oracle [Val79]. The basic idea of the test is that a non-deterministic machine can guess α and the coefficient of $\boldsymbol{x}^\alpha$ in the Witt-Jacobian polynomial g can be computed by a $\#\mathbf{P}$-oracle. Since we have the inclusion $\mathbf{NP}^{\#\mathbf{P}} \subseteq \mathbf{PSPACE}$, this improves the **PSPACE**-algorithm obtained from Perron's degree bound.

1.2 Thesis Outline

The material of this thesis is distributed over the chapters as follows.

In Chapter 2 we give a detailed introduction to arithmetic circuits and the polynomial identity testing problem.

Chapter 3 deals with the theme of linear independence. First we present a criterion for the linear independence of polynomials. Then we construct rank-preserving homomorphisms and hitting sets for several circuit classes. Finally, we investigate the complexity of testing linear independence and computing the linear relations of arithmetic circuits.

Chapter 4 is about the theme of algebraic independence and is structured analogously to Chapter 3. It contains the main results of this thesis. We start with criteria for the algebraic independence of polynomials. Subsequently, we construct faithful homomorphisms and hitting sets for several circuit classes. Finally, we deal with the algebraic independence testing problem and the computation of algebraic relations of arithmetic circuits.

In Chapter 5 we conclude by stating some problems that were left open in this thesis.

Appendix A contains notation used throughout this thesis and introduces preliminaries from algebra and complexity theory. Some definitions and notation introduced in the appendix will be used in the main text without reference. They can be located from the index which also includes a list of symbols.

Chapter 2

Polynomial Identity Testing

Identity is such a crucial affair
that one shouldn't rush into it.
(David Quammen)

In this chapter we give a thorough introduction to the polynomial identity testing problem. We pay special attention to the input representation, i. e. the encoding of arithmetic circuits and their constants. We will distinguish between the size of a circuit (in the common definition) and the encoding size of a circuit (which takes into account the bit-size of the constants). The classical randomized PIT algorithms will be presented for circuits over $\mathbb{Q}$ and $\mathbb{F}_q$. We also point out efficient randomized parallel algorithms for polynomial-degree circuits. Finally, we present a proof for the existence of small hitting sets for arbitrary circuits which can be turned into a polynomial space bounded algorithm for their computation.

For further reading about PIT, we refer to the surveys [Sax09, AS09, SY10] and the references therein.

Chapter outline

This chapter is organized as follows. Section 2.1 lists some famous polynomial identities. In Section 2.2, we define arithmetic circuits and discuss encodings of constants. A formal definition of the polynomial identity testing problem is given in Section 2.3. In Section 2.4, we address the complexity of evaluating arithmetic circuits. Randomized algorithms for PIT are presented in Section 2.5, and general attempts at derandomization are discussed in Section 2.6. Finally, in Section 2.7 we define and examine hitting sets.

2.1 Some Polynomial Identities

Before we investigate the computational aspect of polynomial identities, we give a compilation of some famous identities. Most of them appeared in connection with number-theoretic questions such as Waring's problem [Nar12, Section 2.4.2] or Fermat's Last Theorem [Edw00]. More algebraic identities can be found in [Pie10].

(a) The Difference-of-Powers Identity:

$$x^d - y^d = \big(x - y\big) \cdot \big(x^{d-1} + x^{d-2}y + \cdots + xy^{d-2} + y^{d-1}\big).$$

(b) The Multinomial Theorem:

$$\big(x_1 + \cdots + x_n\big)^d = \sum_{\alpha_1 + \cdots + \alpha_n = d} \binom{d}{\alpha_1, \ldots, \alpha_n} x_1^{\alpha_1} \cdots x_n^{\alpha_n}.$$

(c) Euclid's parametrization of primitive Pythagorean triples:

$$\big(x^2 - y^2\big)^2 + \big(2xy\big)^2 = \big(x^2 + y^2\big)^2.$$

(d) The Brahmagupta–Fibonacci Two-Square Identity:

$$\big(x_1^2 + x_2^2\big) \cdot \big(y_1^2 + y_2^2\big) = \big(x_1y_1 \pm x_2y_2\big)^2 + \big(x_1y_2 \mp x_2y_1\big)^2.$$

(e) The Euler Four-Square Identity:

$$\begin{aligned}\big(x_1^2 + x_2^2 + x_3^2 + x_4^2\big) \cdot \big(y_1^2 + y_2^2 + y_3^2 + y_4^2\big) = \\ (x_1y_1 - x_2y_2 - x_3y_3 - x_4y_4)^2 + (x_1y_2 + x_2y_1 + x_3y_4 - x_4y_3)^2 + \\ (x_1y_3 - x_2y_4 + x_3y_1 + x_4y_2)^2 + (x_1y_4 + x_2y_3 - x_3y_2 + x_4y_1)^2.\end{aligned}$$

This identity was communicated by Euler in a letter to Goldbach on May 4, 1748.

(f) The Degen–Graves–Cayley Eight-Square Identity:

$$\begin{aligned}\big(x_1^2 + x_2^2 + \cdots + x_8^2\big) \cdot \big(y_1^2 + y_2^2 + \cdots + y_8^2\big) = \\ (x_1y_1 - x_2y_2 - x_3y_3 - x_4y_4 - x_5y_5 - x_6y_6 - x_7y_7 - x_8y_8)^2 + \\ (x_1y_2 + x_2y_1 + x_3y_4 - x_4y_3 + x_5y_6 - x_6y_5 - x_7y_8 + x_8y_7)^2 + \\ (x_1y_3 - x_2y_4 + x_3y_1 + x_4y_2 + x_5y_7 + x_6y_8 - x_7y_5 - x_8y_6)^2 + \\ (x_1y_4 + x_2y_3 - x_3y_2 + x_4y_1 + x_5y_8 - x_6y_7 + x_7y_6 - x_8y_5)^2 + \\ (x_1y_5 - x_2y_6 - x_3y_7 - x_4y_8 + x_5y_1 + x_6y_2 + x_7y_3 + x_8y_4)^2 + \\ (x_1y_6 + x_2y_5 - x_3y_8 + x_4y_7 - x_5y_2 + x_6y_1 - x_7y_4 + x_8y_3)^2 + \\ (x_1y_7 + x_2y_8 + x_3y_5 - x_4y_6 - x_5y_3 + x_6y_4 + x_7y_1 - x_8y_2)^2 + \\ (x_1y_8 - x_2y_7 + x_3y_6 + x_4y_5 - x_5y_4 - x_6y_3 + x_7y_2 + x_8y_1)^2.\end{aligned}$$

(g) Lagrange's Identity:

$$\Big(\sum_{i=1}^{n} x_i^2\Big)\cdot\Big(\sum_{i=1}^{n} y_i^2\Big) - \Big(\sum_{i=1}^{n} x_i y_i\Big)^2 = \sum_{1\le i<j\le n} \big(x_i y_j - x_j y_i\big)^2.$$

(h) The Binet–Cauchy Identity:

$$\Big(\sum_{i=1}^{n} x_i z_i\Big)\cdot\Big(\sum_{i=1}^{n} y_i w_i\Big) - \Big(\sum_{i=1}^{n} x_i w_i\Big)\cdot\Big(\sum_{i=1}^{n} y_i z_i\Big) = \sum_{1\le i<j\le n} \big(x_i y_j - x_j y_i\big)\cdot\big(z_i w_j - z_j w_i\big).$$

This is a generalization of (g) and can be proven using the Cauchy–Binet Formula (see Lemma A.3.2).

(i) Maillet's Identity:

$$6x\big(x^2 + y_1^2 + y_2^2 + y_3^2\big) = \sum_{i=1}^{3}\big(x + y_i\big)^3 + \sum_{i=1}^{3}\big(x - y_i\big)^3.$$

(j) The Lucas–Liouville Identity:

$$6\big(x_1^2 + x_2^2 + x_3^2 + x_4^2\big)^2 = \sum_{1\le i<j\le 4}\big(x_i + x_j\big)^4 + \sum_{1\le i<j\le 4}\big(x_i - x_j\big)^4.$$

(k) Lamé-type identities:

$$\big(x+y+z\big)^3 - \big(x^3+y^3+z^3\big) = 3\big(x+y\big)\big(x+z\big)\big(y+z\big),$$

$$\big(x+y+z\big)^5 - \big(x^5+y^5+z^5\big) = 5\big(x+y\big)\big(x+z\big)\big(y+z\big)\big(x^2+y^2+z^2+xy+xz+yz\big),$$

$$\big(x+y+z\big)^7 - \big(x^7+y^7+z^7\big) = 7\big(x+y\big)\big(x+z\big)\big(y+z\big)\cdot\Big(\big(x^2+y^2+z^2+xy+xz+yz\big)^2 + xyz\big(x+y+z\big)\Big).$$

The last identity appears in Lamé's proof of the $n = 7$ case of Fermat's Last Theorem [Edw00].

2.2 Arithmetic Circuits

Let $n \geq 1$, let K be a ring, and let $K[\boldsymbol{x}] = K[x_1, \ldots, x_n]$ be a polynomial ring in n variables over K. Elements of $K[\boldsymbol{x}]$ can be succinctly encoded by arithmetic circuits.

Definition 2.2.1. Let K be a ring and let $\boldsymbol{x} = \{x_1, \ldots, x_n\}$ be a set of variables.

(a) An **arithmetic circuit** over $K[\boldsymbol{x}]$ is a finite, labeled, directed, acyclic multigraph $C = (V(C), E(C))$ with the following properties. The vertices $V(C)$ are called **gates**, and the directed edges $E(C)$ are called **wires**. The in- and out-degree of a gate $v \in V(C)$ is called **fan-in** and **fan-out** and is denoted by $\operatorname{fanin}(v)$ and $\operatorname{fanout}(v)$, respectively. We also set $\operatorname{fanin}(C) := \max\{1, \operatorname{fanin}(v) \mid v \in V(C)\}$ and $\operatorname{fanout}(C) := \max\{1, \operatorname{fanout}(v) \mid v \in V(C)\}$. A gate of fan-in 0 is called **input gate** and is labeled either by a **constant** (an element of K) or a **variable** (an element of $\boldsymbol{x}$). A gate of positive fan-in is called **arithmetic gate** and is labeled either by the symbol $+$ (then it is called **sum gate**) or $\times$ (then it is called **product gate**). Finally, we assume that there is exactly one gate of fan-out 0 which is called the **output gate** and is denoted by v_{out}. We denote the set of input gates and the set of arithmetic gates by $V_{\text{in}}(C)$ and $V_{\text{arith}}(C)$, respectively.

(b) At each gate $v \in V(C)$, an arithmetic circuit C **computes** a polynomial $C_v \in K[\boldsymbol{x}]$ in the following way. An input gate computes the constant or variable it is labeled with. A sum gate computes the sum of the polynomials computed by its predecessors (with repetition in case of parallel wires) and, likewise, a product gate computes the product of the polynomials computed by its predecessors (again with repetition). Finally, we say that C computes the polynomial $C_{v_{\text{out}}}$ that is computed at the output gate. By abuse of notation, we denote the polynomial $C_{v_{\text{out}}}$ also by C.

(c) The **size** of C is defined as $|C| := |V(C)| + |E(C)| \in \mathbb{N}_{>0}$.

(d) The **depth** of a gate $v \in V(C)$ is defined as the maximum length of a path in C with terminal gate v and is denoted by $\operatorname{depth}(v)$. (A path of maximal length necessarily starts at an input gate.) The depth of C is defined by $\operatorname{depth}(C) := \operatorname{depth}(v_{\text{out}})$.

(e) The **formal degree** of a gate $v \in V(C)$, written $\operatorname{fdeg}(v)$, is defined as follows. The formal degree of an input gate is 1. The formal degree of a sum gate is defined as the maximum of the formal degrees of its predecessors, and the formal degree of a product gate is defined as the

sum of the formal degrees of its predecessors (with repetition in case of parallel wires). Finally, the formal degree of C is defined by $\mathrm{fdeg}(C) := \mathrm{fdeg}(v_{\mathrm{out}})$.

(f) An arithmetic circuit C is called an **arithmetic formula** if $\mathrm{fanout}(C) = 1$. In this case, C is a directed tree with root v_{out}.

Remark 2.2.2.

(a) In many sources, arithmetic gates are defined to be of fan-in 2. We prefer a more flexible definition. Also note that for constant-depth circuits unbounded fan-in is necessary (see Lemma 2.2.4 (b)).

(b) The size of an arithmetic circuit is sometimes defined as the number of gates and sometimes as the number of edges. Since we allow parallel wires, the former definition would not be suitable for us. While the latter definition would be possible, we still prefer our flexible choice.

(c) Straight-line programs are a model for computing polynomials similar to arithmetic circuits (see for example [IM83]). Arithmetic circuits and straight-line programs can be efficiently converted into each other.

Figure 2.1 gives an example of an arithmetic circuit and an arithmetic formula computing the same polynomial. Here the circuit representation is more compact, since we are allowed to reuse already computed expressions. The following example demonstrates that symbolic determinants can be computed by polynomial-size circuits, although they have exponential sparsity.

Example 2.2.3. Let $K[\boldsymbol{x}] = K[x_{i,j} \mid 1 \le i, j \le n]$. By the Berkowitz algorithm (see Lemma A.3.1), the polynomial $\det\big(x_{i,j}\big)_{i,j} \in K[\boldsymbol{x}]$ can be computed by an arithmetic circuit C with $|C| = \mathrm{poly}(n)$. On the other hand, we have $\mathrm{sp}(C) = n! > (n/3)^n$.

The following lemma gives bounds for the formal degree of arithmetic circuits. The examples in Figure 2.2 show that those bounds are tight.

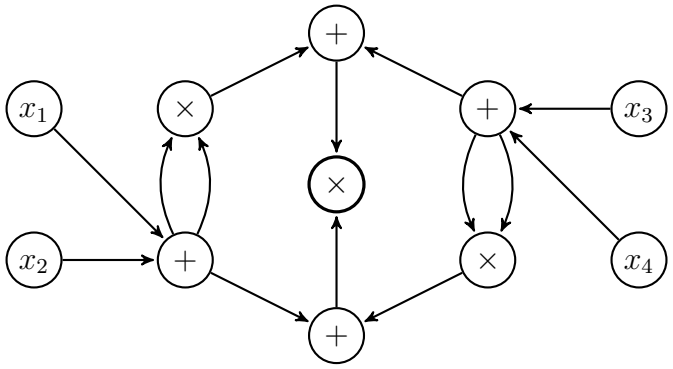
Lemma 2.2.4. *Let C be an arithmetic circuit over $K[\boldsymbol{x}]$.*

(a) If $C \neq 0$, then $\deg(C) \le \mathrm{fdeg}(C)$.

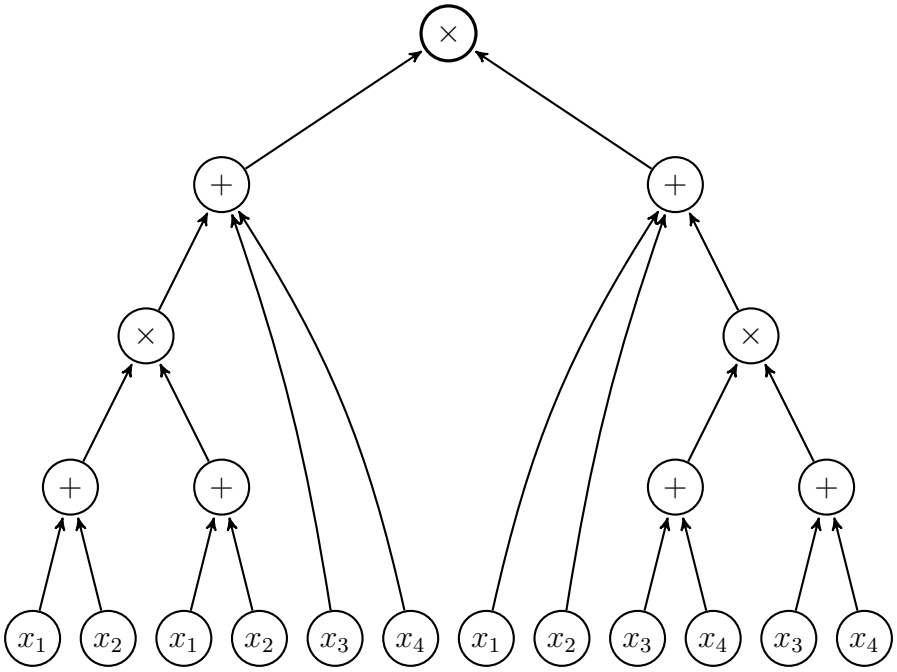
(b) We have $\mathrm{fdeg}(C) \le \mathrm{fanin}(C)^{\mathrm{depth}(C)}$.

(c) If C is a formula, then $\mathrm{fdeg}(C) \le |V_{\mathrm{in}}(C)|$.

Proof. For (a), we show $\deg(C_v) \le \mathrm{fdeg}(v)$ for all $v \in V(C)$ such that $C_v \neq 0$ by structural induction. If $v \in V(C)$ is an input gate with $C_v \neq 0$, then $\deg(C_v) \le 1 = \mathrm{fdeg}(C_v)$. Now let $v \in V(C)$ be an arithmetic gate such that $C_v \neq 0$, and let $v_1, \ldots, v_k \in V(C)$ be its predecessors (with repetition in case



(a) A general circuit.



(b) A formula.

Figure 2.1: Two arithmetic circuits computing the polynomial $\big((x_1+x_2)^2+x_3+x_4\big)\cdot\big(x_1+x_2+(x_3+x_4)^2\big)$.

of parallel wires). By induction, we have $\deg(C_{v_i}) \leq \mathrm{fdeg}(v_i)$ for all $i \in [k]$ with $C_{v_i} \neq 0$. If v is a sum gate, then $\deg(C_v) \leq \max\{\deg(C_{v_i}) \mid C_{v_i} \neq 0\} \leq \max\{\mathrm{fdeg}(v_i) \mid i \in [k]\} = \mathrm{fdeg}(v)$. If v is a product gate, then $C_{v_i} \neq 0$ for all $i \in [k]$, hence $\deg(C_v) = \sum_{i=1}^{k} \deg(C_{v_i}) \leq \sum_{i=1}^{k} \mathrm{fdeg}(v_i) = \mathrm{fdeg}(v)$.

For (b), we show $\mathrm{fdeg}(v) \leq \mathrm{fanin}(C)^{\mathrm{depth}(v)}$ for all $v \in V(C)$ by structural induction. If $v \in V(C)$ is an input gate, then $\mathrm{fdeg}(v) = 1 = \mathrm{fanin}(C)^{\mathrm{depth}(v)}$. Now let $v \in V(C)$ be an arithmetic gate, and let $v_1, \ldots, v_k \in V(C)$ be its predecessors (with repetition in case of parallel wires), where $k = \mathrm{fanin}(v)$. By induction, we have $\mathrm{fdeg}(v_i) \leq \mathrm{fanin}(C)^{\mathrm{depth}(v_i)} \leq \mathrm{fanin}(C)^{\mathrm{depth}(v)-1}$ for all $i \in [k]$. We conclude $\mathrm{fdeg}(v) \leq \sum_{i=1}^{k} \mathrm{fdeg}(v_i) \leq k \cdot \mathrm{fanin}(C)^{\mathrm{depth}(v)-1} \leq \mathrm{fanin}(C)^{\mathrm{depth}(v)}$.

For (c), assume that C is a formula. Hence C is a tree with root v_{out} and wires directed towards v_{out}. For a gate $v \in V(C)$, we denote by C_v the subtree of C with root v and wires directed towards v. We show $\mathrm{fdeg}(v) \leq |V_{\mathrm{in}}(C_v)|$ for all $v \in V(C)$ by structural induction. If $v \in V(C)$ is an input gate, then $\mathrm{fdeg}(v) = 1 = |V_{\mathrm{in}}(C_v)|$. Now let $v \in V(C)$ be an arithmetic gate, and let $v_1, \ldots, v_k \in V(C)$ be its predecessors (with repetition in case of parallel wires), where $k = \mathrm{fanin}(v)$. By induction, we have $\mathrm{fdeg}(v_i) \leq |V_{\mathrm{in}}(C_{v_i})|$ for all $i \in [k]$. We conclude $\mathrm{fdeg}(v) \leq \sum_{i=1}^{k} \mathrm{fdeg}(v_i) \leq \sum_{i=1}^{k} |V_{\mathrm{in}}(C_{v_i})| \leq |V_{\mathrm{in}}(C_v)|$. □

Now we term some often encountered classes of arithmetic circuits. The classes in the following definition are ordered from most general to most specific.

Definition 2.2.5. A **circuit class** $\mathcal{C}$ over K is a union $\mathcal{C} = \bigcup_{n \geq 1} \mathcal{C}_n$, where $\mathcal{C}_n$ is a set of arithmetic circuits over $K[x_1, \ldots, x_n]$ for all $n \geq 1$. In particular, we define the circuit classes

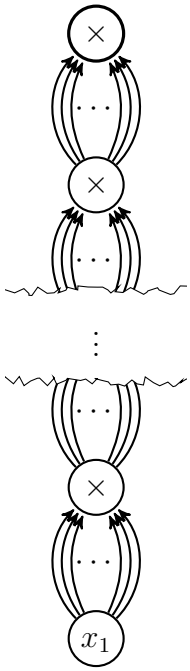
(a) $\mathcal{C}_{\text{all}} := \bigcup_{n \geq 1} \mathcal{C}_{\text{all},n}$, where $\mathcal{C}_{\text{all},n}$ is the set of all arithmetic circuits over $K[x_1, \ldots, x_n]$,

(b) $\mathcal{C}_{\text{poly-deg}} := \bigcup_{n \geq 1} \mathcal{C}_{\text{poly-deg},n}$, where $\mathcal{C}_{\text{poly-deg},n}$ is the set of all arithmetic circuits C over $K[x_1, \ldots, x_n]$ such that $\mathrm{fdeg}(C) \leq f(|C|)$ for some fixed polynomial $f \in \mathbb{N}[z]$,

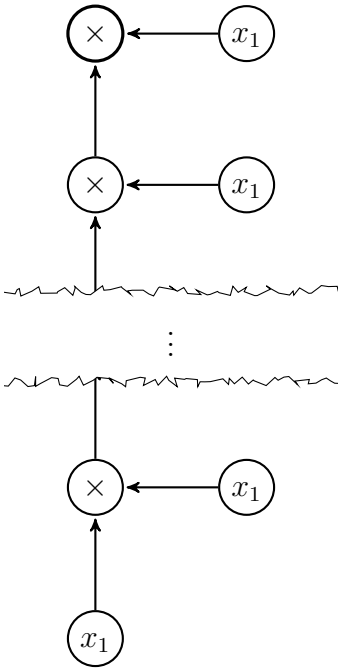
(c) $\mathcal{C}_{\text{formula}} := \bigcup_{n \geq 1} \mathcal{C}_{\text{formula},n}$, where $\mathcal{C}_{\text{formula},n}$ is the set of all arithmetic formulas over $K[x_1, \ldots, x_n]$, and

(d) $\mathcal{C}_{\text{depth-}k} := \bigcup_{n \geq 1} \mathcal{C}_{\text{depth-}k,n}$, where $k \geq 1$ is fixed and $\mathcal{C}_{\text{depth-}k,n}$ is the set of all arithmetic circuits over $K[x_1, \ldots, x_n]$ of depth at most k.

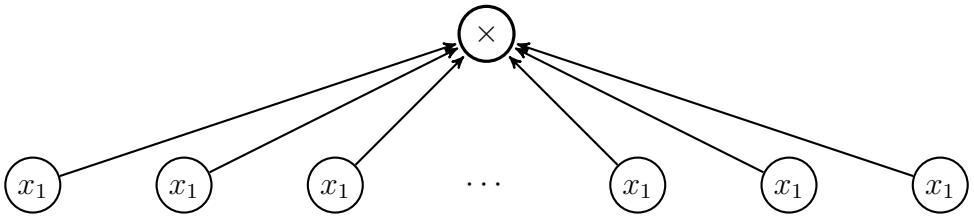
It is easy to see that a constant-depth circuit C can be converted into a formula of size $\mathrm{poly}(|C|)$ computing the same polynomial. By Lemma 2.2.4, constant-depth circuits and formulas are polynomial-degree circuits.



(a) A general circuit.



(b) A formula of fan-in 2.



(c) A formula of depth 1.

Figure 2.2: Arithmetic circuits exhibiting extremal formal degrees.

Polynomial-degree arithmetic circuits can be assumed to have polylogarithmic depth. Let $f \in K[\boldsymbol{x}]$ be a polynomial that is computed by an arithmetic circuit C with $d := \mathrm{fdeg}(C)$ and $s := |C|$. Then, by [VSBR83], f can be computed by an arithmetic circuit with fan-in 2, depth $O\big((\log d)(\log d + \log s)\big)$, and size $\mathrm{poly}(s, d)$.

From now on we will assume that K is a field. We defined the size $|C|$ of an arithmetic circuit C as the size of the underlying directed acyclic graph. For algorithms dealing with arithmetic circuits, we also have to take the encoding of the constants into account. We say that a field K is **computable** if its elements $c \in K$ can be encoded as binary strings in $\{0,1\}^{O(\mathrm{bs}(c))}$, where $\mathrm{bs}\colon K \to \mathbb{N}_{>0}$ is some function, and the field operations on those encodings can be carried out by a Turing machine. We call $\mathrm{bs}(c)$ the **bit-size** of c.

Definition 2.2.6. Let K be a computable field. The **encoding size** of an arithmetic circuit C over $K[\boldsymbol{x}]$ is defined as $\mathrm{size}(C) := |C| + \sum_{i=1}^{m} \mathrm{bs}(c_i)$, where $c_1, \ldots, c_m \in K$ are the constants of C.

The standard examples of computable fields are the rationals $\mathbb{Q}$ and finite fields $\mathbb{F}_q$ for prime powers q.

Arithmetic circuits over $\mathbb{Q}$

Let $K = \mathbb{Q}$. For an integer $a \in \mathbb{Z}$, let $\ell(a) := \lceil \log_2(|a|+1) \rceil \in \mathbb{N}$ be the length of its binary representation (without sign). Now let $q = a/b \in \mathbb{Q}$ be a rational number in canonical form, i. e. $a \in \mathbb{Z}$ and $b \in \mathbb{N}_{>0}$ such that $\gcd(a, b) = 1$. We denote $\mathrm{num}(q) := a$ and $\mathrm{den}(q) := b$, hence $q = \mathrm{num}(q)/\mathrm{den}(q)$. We define the **bit-size** of a rational number $q \in \mathbb{Q}$ as

$$\mathrm{bs}(q) := \max\big\{\ell(\mathrm{num}(q)), \ell(\mathrm{den}(q))\big\} \in \mathbb{N}_{>0}.$$

The following lemma collects some basic properties of the bit-size function.

Lemma 2.2.7. *Let $q, q_1, \ldots, q_k \in \mathbb{Q}$ be rational numbers.*

(a) We have $|\mathrm{num}(q)| \le 2^{\mathrm{bs}(q)}$ and $\mathrm{den}(q) \le 2^{\mathrm{bs}(q)}$.

(b) We have $\mathrm{bs}\big(\sum_{i=1}^{k} q_i\big) \le \big(\sum_{i=1}^{k} \mathrm{bs}(q_i)\big) + \ell(k-1)$ and $\mathrm{bs}\big(\prod_{i=1}^{k} q_i\big) \le \sum_{i=1}^{k} \mathrm{bs}(q_i)$.

(c) If $q_1, \ldots, q_k \in \mathbb{Z}$, then we have $\mathrm{bs}\big(\sum_{i=1}^{k} q_i\big) \le \max\{\mathrm{bs}(q_i) \mid i \in [k]\} + \ell(k-1)$.

Proof. Part (a) is clear by definition. To show (c), suppose that $q_1, \ldots, q_k \in \mathbb{Z}$. Furthermore, we may assume $0 < |q_1| \le \cdots \le |q_k|$. Then $\mathrm{bs}\big(\sum_{i=1}^{k} q_i\big) \le$

$\mathrm{bs}(k \cdot |q_k|) \leq \ell(k \cdot q_k) \leq \mathrm{bs}(q_k) + \ell(k-1) = \max\{\mathrm{bs}(q_i) \mid i \in [k]\} + \ell(k-1)$. To show (b), let $q_1, \ldots, q_k \in \mathbb{Q}$ be arbitrary and denote $a_i := \mathrm{num}(q_i)$ and $b_i := \mathrm{den}(q_i)$ for all $i \in [k]$. Then

$$\begin{aligned}\mathrm{bs}\big(\textstyle\prod_{i=1}^k q_i\big) &\leq \max\big\{\ell(a_1 \cdots a_k), \ell(b_1 \cdots b_k)\big\}\\ &\leq \max\big\{\textstyle\sum_{i=1}^k \ell(a_i), \sum_{i=1}^k \ell(b_i)\big\}\\ &\leq \textstyle\sum_{i=1}^k \max\{\ell(a_i), \ell(b_i)\}\\ &= \textstyle\sum_{i=1}^k \mathrm{bs}(q_i).\end{aligned}$$

Together with (c), this yields

$$\begin{aligned}\mathrm{bs}\big(\textstyle\sum_{i=1}^k q_i\big) &\leq \max\big\{\ell\big(\textstyle\sum_{i=1}^k b_1 \cdots a_i \cdots b_k\big), \ell(b_1 \cdots b_k)\big\}\\ &\leq \max\big\{\ell(b_1 \cdots a_i \cdots b_k) + \ell(k-1), \ell(b_1 \cdots b_k) \mid i \in [k]\big\}\\ &\leq \max\big\{\ell(a_i) + \textstyle\sum_{j \neq i} \ell(b_j), \sum_{j=1}^k \ell(b_j) \mid i \in [k]\big\} + \ell(k-1)\\ &\leq \big(\textstyle\sum_{i=1}^k \max\{\ell(a_i), \ell(b_i)\}\big) + \ell(k-1)\\ &= \big(\textstyle\sum_{i=1}^k \mathrm{bs}(q_i)\big) + \ell(k-1),\end{aligned}$$

finishing the proof. □

The following theorem shows that the rational number computed by a variable-free arithmetic circuit C over $\mathbb{Q}$ has bit-size $\mathrm{poly}(\mathrm{fdeg}(C), \mathrm{size}(C))$. The argument for bounding the bit-size of the denominator in terms of the formal degree was shown to me by Peter Scheiblechner.

Theorem 2.2.8. *Let C be a variable-free arithmetic circuit over $\mathbb{Q}$, and assume that the sum of the bit-sizes of its constants is bounded by $B \geq 1$. Then we have* $\mathrm{bs}(\mathrm{den}(C)) \leq \mathrm{fdeg}(C) \cdot B$ *and*

$$\mathrm{bs}(C) \leq \mathrm{fdeg}(C) \cdot \ell(\mathrm{fanin}(C)) \cdot (2\,\mathrm{depth}(C) + 1) \cdot B.$$

Proof. Let $c_1, \ldots, c_m \in \mathbb{Q}$ be the constants of C, and let

$$a := \mathrm{lcm}(\mathrm{den}(c_1), \ldots, \mathrm{den}(c_m)) \in \mathbb{N}_{>0}.$$

By assumption, we have $\mathrm{bs}(a) \leq \sum_{i=1}^m \mathrm{bs}(c_i) \leq B$. Using structural induction, we prove that, for all $v \in V(C)$, we have

(a) $\mathrm{den}(C_v)$ divides $a^{\mathrm{fdeg}(v)}$,

(b) $\mathrm{bs}(\mathrm{den}(C_v)) \leq \mathrm{fdeg}(v) \cdot B$, and

(c) $\mathrm{bs}(\mathrm{num}(C_v)) \leq \mathrm{fdeg}(v) \cdot \ell(\mathrm{fanin}(C)) \cdot (2\,\mathrm{depth}(v) + 1) \cdot B$.

If $v \in V(C)$ is an input gate, then (a)–(c) are satisfied. Now let $v \in V(C)$ be an arithmetic gate, and let $v_1, \ldots, v_k \in V(C)$ be its predecessors (with repetition in case of parallel wires), where $k = \operatorname{fanin}(v)$.

First, we assume that v is a sum gate. Then $\operatorname{den}(C_v)$ divides

$$\operatorname{lcm}(\operatorname{den}(C_{v_1}), \ldots, \operatorname{den}(C_{v_k})).$$

Hence, by induction, $\operatorname{den}(C_v)$ divides

$$\operatorname{lcm}\big(a^{\operatorname{fdeg}(v_1)}, \ldots, a^{\operatorname{fdeg}(v_k)}\big) = a^{\max\{\operatorname{fdeg}(v_i) \mid i \in [k]\}} = a^{\operatorname{fdeg}(v)},$$

showing (a). Since $\operatorname{bs}(a) \leq B$, (a) implies (b). To prove (c), observe that $\operatorname{num}(C_v)$ divides

$$\sum_{i=1}^{k} \operatorname{num}(C_{v_i}) \cdot \frac{\operatorname{lcm}(\operatorname{den}(C_{v_1}), \ldots, \operatorname{den}(C_{v_k}))}{\operatorname{den}(C_{v_i})}.$$

Therefore, we obtain

$$\begin{aligned}
\operatorname{bs}(\operatorname{num}(C_v)) &\leq \operatorname{bs}\big(\textstyle\sum_{i=1}^{k} \operatorname{num}(C_{v_i}) \cdot a^{\operatorname{fdeg}(v)}\big) \\
&\leq \max\big\{\operatorname{bs}(\operatorname{num}(C_{v_i})) + \operatorname{bs}(a^{\operatorname{fdeg}(v)}) \mid i \in [k]\big\} + \ell(k-1) \\
&\leq \max\big\{\operatorname{bs}(\operatorname{num}(C_{v_i})) \mid i \in [k]\big\} + \operatorname{fdeg}(v) \cdot B + \ell(k-1).
\end{aligned}$$

By induction, we have

$$\begin{aligned}
\operatorname{bs}(\operatorname{num}(C_{v_i})) &\leq \operatorname{fdeg}(v_i) \cdot \ell(\operatorname{fanin}(C)) \cdot (2\operatorname{depth}(v_i) + 1) \cdot B \\
&\leq \operatorname{fdeg}(v) \cdot \ell(\operatorname{fanin}(C)) \cdot (2\operatorname{depth}(v) - 1) \cdot B
\end{aligned}$$

for all $i \in [k]$. We conclude

$$\operatorname{bs}(\operatorname{num}(C_v)) \leq \operatorname{fdeg}(v) \cdot \ell(\operatorname{fanin}(C)) \cdot (2\operatorname{depth}(v) + 1) \cdot B.$$

Now we assume that v is a product gate. Then $\operatorname{num}(C_v)$ and $\operatorname{den}(C_v)$ divide $\prod_{i=1}^{k} \operatorname{num}(C_{v_i})$ and $\prod_{i=1}^{k} \operatorname{den}(C_{v_i})$, respectively. Therefore, by induction, $\operatorname{den}(C_v)$ divides

$$\prod_{i=1}^{k} a^{\operatorname{fdeg}(v_i)} = a^{\sum_{i=1}^{k} \operatorname{fdeg}(v_i)} = a^{\operatorname{fdeg}(v)},$$

showing (a) and implying (b). Again by induction, we obtain

$$\begin{aligned}
\operatorname{bs}(\operatorname{num}(C_v)) &\leq \operatorname{bs}\big(\textstyle\prod_{i=1}^{k} \operatorname{num}(C_{v_i})\big) \\
&\leq \textstyle\sum_{i=1}^{k} \operatorname{bs}(\operatorname{num}(C_{v_i})) \\
&\leq \textstyle\sum_{i=1}^{k} \operatorname{fdeg}(v_i) \cdot \ell(\operatorname{fanin}(C)) \cdot (2\operatorname{depth}(v_i) + 1) \cdot B \\
&\leq \big(\textstyle\sum_{i=1}^{k} \operatorname{fdeg}(v_i)\big) \cdot \ell(\operatorname{fanin}(C)) \cdot (2\operatorname{depth}(v) + 1) \cdot B \\
&= \operatorname{fdeg}(v) \cdot \ell(\operatorname{fanin}(C)) \cdot (2\operatorname{depth}(v) + 1) \cdot B.
\end{aligned}$$

This shows (c) and finishes the proof. □

Arithmetic circuits over $\mathbb{F}_q$

Let p be a prime, let $m \geq 1$, and let $q = p^m$. We assume that we are given the finite field $K = \mathbb{F}_q$ as $\mathbb{F}_p[x]/\langle f \rangle$, where $f \in \mathbb{F}_p[x]$ is an irreducible polynomial of degree m. Then $\{1 + \langle f \rangle, x + \langle f \rangle, \ldots, x^{m-1} + \langle f \rangle\}$ is an $\mathbb{F}_p$-basis of $\mathbb{F}_q$, so we can represent the elements of $\mathbb{F}_q$ by their coordinate vectors in $\mathbb{F}_p^m$ with respect to this basis. A discussion of alternative representations of finite fields is given in [Len91].

In situations where we deal with a fixed finite field we can define the **bit-size** of an element $c \in \mathbb{F}_q$ as $\mathrm{bs}(c) = 1$. In situations where we have to compute finite field extensions of various degrees, it is convenient to set $\mathrm{bs}(c) := m \cdot \ell(p)$ for all $c \in \mathbb{F}_q$.

The following lemma shows that finite field extensions can be constructed efficiently. In part (a), a field extension of polynomial degree is constructed in polynomial time (cf. [Sah08, Theorem 1.2]). The asserted irreducible polynomial is computed by an algorithm in [LP11]. Part (b) demonstrates how an extension field of polynomial cardinality can be computed efficiently in parallel (cf. [GKS90] and [Fra91, Theorem 3 (2.)]). Here the irreducible polynomial can be computed by brute force using the Ben-Or irreducibility test (see Lemma A.3.5).

Lemma 2.2.9. *Let $q = p^m$ be a prime power, and let $\mathbb{F}_q$ be given as $\mathbb{F}_p[x]/\langle f \rangle$, where $f \in \mathbb{F}_p[x]$ is an irreducible polynomial of degree m.*

(a) There exists an algorithm that, given $D \geq (\log p)^2$ and $\mathbb{F}_q$ as above, computes an irreducible polynomial $g \in \mathbb{F}_p[x]$ of degree md for some $D \leq d < 2D$ and an embedding $\mathbb{F}_p[x]/\langle f \rangle \hookrightarrow \mathbb{F}_p[x]/\langle g \rangle$. This yields a field extension $\mathbb{F}_{q^d}/\mathbb{F}_q$ of degree at least D. The algorithm runs in $\mathrm{poly}(D, m, \log p)$ time.

(b) There exists an algorithm that, given $N \geq q$ and $\mathbb{F}_q$ as above, computes an irreducible polynomial $g \in \mathbb{F}_q[x]$ of degree d such that $q^d \geq N$. This yields a field extension $\mathbb{F}_{q^d}/\mathbb{F}_q$ such that $|\mathbb{F}_{q^d}| \geq N$. The algorithm runs in $\mathrm{poly}(\log N)$ parallel time using $\mathrm{poly}(N)$ processors.

Proof. First we show (a). Let $D \geq (\log p)^2$. Then an irreducible polynomial $f' \in \mathbb{F}_p[x]$ of degree d for some $D \leq d < 2D$ can be computed in $\mathrm{poly}(d, \log p)$ time by [LP11, Theorem 2]. By [Len91, Theorem 1.1, (b) $\Rightarrow$ (c)], for each prime r dividing m resp. d, an irreducible polynomial in $\mathbb{F}_p[x]$ of degree r can be computed from f resp. f' in $\mathrm{poly}(D, m \log p)$ time. By [Len91, Theorem 1.1, (c) $\Rightarrow$ (b)], an irreducible polynomial $g \in \mathbb{F}_p[x]$ of degree md can be computed from those polynomials in $\mathrm{poly}(D, m, \log p)$ time. The embedding $\mathbb{F}_p[x]/\langle f \rangle \hookrightarrow \mathbb{F}_p[x]/\langle g \rangle$ can be computed within the same time bound by [Len91, §2].

To show (b), let $N \geq q$. Let $d \geq 1$ be the least integer such that $q^d \geq N$. There are $q^d - 1 = \text{poly}(N)$ non-zero degree-d polynomials in $\mathbb{F}_q[x]$, so we can test each of them for irreduciblity in parallel. To this end, we will use the irreduciblity test of Lemma A.3.5. Let $f \in \mathbb{F}_q[x]$ be a polynomial of degree d and let $k \in \{1, \ldots, \lfloor d/2 \rfloor\}$. We have to check whether $\gcd(f, x^{q^k} - x) = 1$. By [BvzGH82, Theorem 2], the gcd computation can be performed in $\text{poly}(\log N)$ parallel time using $\text{poly}(N)$ processors (note that $\deg(x^{q^k} - x) = \text{poly}(N)$). □

2.3 Problem Statement

The heart of mathematics is its problems.
(Paul Halmos)

Now we can formally define the polynomial identity testing problem. This decision problem asks whether a given arithmetic circuit computes the zero polynomial. The input size is the encoding size of the circuit.

Problem 2.3.1. Let K be a computable field and let $\mathcal{C}$ be a circuit class over K. Then the **polynomial identity testing** problem $\mathsf{PIT}_K(\mathcal{C})$ is defined as follows: Given a circuit $C \in \mathcal{C}$, decide whether $C = 0$. We set $\mathsf{PIT}_K := \mathsf{PIT}_K(\mathcal{C}_{\text{all}})$.

Remark 2.3.2. We consider the field K of constants as fixed. If K is a finite field, one could make a description of K part of the input. However, for all computational problems in this thesis which are dealing with finite fields, the computation of a field extension L/K is required anyways (and can be done efficiently by Lemma 2.2.9). Therefore, the additional input does not alter the complexity of the problem.

The zero function testing problem

An arithmetic circuit C over $K[\boldsymbol{x}]$ gives rise to a function $K^n \to K$ defined by $\boldsymbol{a} \mapsto C(\boldsymbol{a})$. So it is also natural to consider the following computational problem, which asks whether an arithmetic circuit defines the zero function.

Problem 2.3.3. Let K be a computable field. Then the **zero function testing** problem ZFT_K is defined as follows: Given an arithmetic circuit C over $K[\boldsymbol{x}]$, decide whether $C(\boldsymbol{a}) = 0$ for all $\boldsymbol{a} \in K^n$.

If K is infinite, then Theorem 2.5.4 implies that a circuit C over $K[\boldsymbol{x}]$ is zero if and only if $C(\boldsymbol{a}) = 0$ for all $\boldsymbol{a} \in K^n$, hence $\mathsf{PIT}_K = \mathsf{ZFT}_K$.

By contrast, if $K = \mathbb{F}_q$ for some prime power q, then the non-zero polynomial $x^q - x \in K[x]$ vanishes on K, hence $\mathsf{PIT}_K \subset \mathsf{ZFT}_K$. By the following theorem, ZFT_K is **coNP**-hard (cf. [IM83, Theorem 3.2]). In view of Theorem 2.5.5, this means that ZFT_K is computationally harder than PIT_K (under standard complexity-theoretic assumptions).

Theorem 2.3.4. *Let $K = \mathbb{F}_q$ for some prime power q. Then ZFT_K is* **coNP***-complete.*

The proof, given below, uses a reduction from the **coNP**-complete problem $\overline{\mathsf{SAT}}$ (unsatisfiability of boolean formulas).

We recall a few definitions. A **boolean circuit** over the variables $\boldsymbol{x} = \{x_1, \ldots, x_n\}$ is a finite, labeled, directed acyclic graph ϕ with the following properties. Vertices of fan-in 0 are called input gates and are labeled by a variable in $\boldsymbol{x}$. Vertices of positive fan-in are called logic gates and are labeled by a symbol in $\{\vee, \wedge, \neg\}$ (OR-, AND-, and NOT-gates). NOT-gates are required to have fan-in 1. Finally, we assume that there is a unique gate of fan-out 0, called the output gate. The circuit ϕ computes a boolean function $\phi\colon \{0,1\}^n \to \{0,1\}$ in a natural way. The **size** of ϕ, denoted by $|\phi|$, is defined as the number of vertices plus the number of edges. If the fan-out is at most 1 for all gates, then ϕ is called a **boolean formula**. A boolean circuit can be turned into an arithmetic circuit as follows.

Definition 2.3.5. Let K be a computable field. Let ϕ be a boolean circuit over $\boldsymbol{x}$. Then the **arithmetization** of ϕ over $K[\boldsymbol{x}]$, written arith_ϕ, is an arithmetic circuit over $K[\boldsymbol{x}]$ which is inductively defined as follows. If $\phi = x_i$ for some $i \in [n]$, then we define $\mathrm{arith}_\phi := x_i$. Now let $\phi_1, \ldots, \phi_m$ be boolean circuits.

(a) If $\phi = \neg\phi_1$, then we define $\mathrm{arith}_\phi := 1 - \mathrm{arith}_{\phi_1}$.

(b) If $\phi = \bigwedge_{i=1}^m \phi_i$, then we define $\mathrm{arith}_\phi := \prod_{i=1}^m \mathrm{arith}_{\phi_i}$.

(c) If $\phi = \bigvee_{i=1}^m \phi_i$, then we define $\mathrm{arith}_\phi := 1 - \prod_{i=1}^m (1 - \mathrm{arith}_{\phi_i})$.

The following lemma shows that a boolean circuit agrees with its arithmetization on $\{0,1\}^n$. The proof follows directly from Definition 2.3.5.

Lemma 2.3.6. *Let ϕ be a boolean circuit over $\boldsymbol{x}$.*

(a) We have $\mathrm{arith}_\phi(\boldsymbol{a}) = \phi(\boldsymbol{a})$ for all $\boldsymbol{a} \in \{0,1\}^n$.

(b) We have $\mathrm{size}(\mathrm{arith}_\phi) = \mathrm{poly}(|\phi|)$.

Proof of Theorem 2.3.4. Since circuits over $K[\boldsymbol{x}]$ can be evaluated in polynomial time, we have $\mathsf{ZFT}_K \in$ **coNP**. To show **coNP**-hardness, we reduce

$\overline{\mathsf{SAT}}$ to ZFT_K. Let ϕ be a boolean formula over $\boldsymbol{x}$. Define the arithmetic circuit

$$C := \mathrm{arith}_\phi\big(x_1^{q-1}, \ldots, x_n^{q-1}\big).$$

By Lemma 2.3.6 (b), we have $\mathrm{size}(C) = \mathrm{poly}(|\phi|, \log q)$, and C can be constructed in polynomial time. For $a \in K$, we have $a^{q-1} = 0$ if $a = 0$, and $a^{q-1} = 1$ otherwise. Thus, by Lemma 2.3.6 (a), we get $\phi \in \overline{\mathsf{SAT}}$ if and only if $C \in \mathsf{ZFT}_K$. □

2.4 Evaluation

In this section, we study the complexity of evaluating an arithmetic circuit C over $K[\boldsymbol{x}]$ at a point $\boldsymbol{a} \in K^n$.

Problem 2.4.1. Let K be a computable field and let $\mathcal{C}$ be a circuit class over K. Then the **evaluation** problem $\mathsf{Eval}_K(\mathcal{C})$ is defined as follows: Given a circuit $C \in \mathcal{C} \cap K[\boldsymbol{x}]$ and $\boldsymbol{a} \in K^n$, decide whether $C(\boldsymbol{a}) = 0$. We set $\mathsf{Eval}_K := \mathsf{Eval}_K(\mathcal{C}_{\mathrm{all}})$.

The decision problem $\mathsf{Eval}_K(\mathcal{C})$ can be considered as a special case of $\mathsf{PIT}_K(\mathcal{C})$, because identity testing of variable-free arithmetic circuits amounts to evaluation. On the other hand, most PIT algorithms use evaluation as a subroutine.

Randomized evaluation of arithmetic circuits over $\mathbb{Q}$

Arithmetic circuits over $\mathbb{Q}[\boldsymbol{x}]$ cannot be efficiently evaluated in a straightforward manner, because the value of the evaluation might have exponential bit-size. For instance, by repeated squaring, the number 2^{2^n} can be computed by a circuit of size $O(n)$. However, with the help of randomization, a modular approach can be used. The following theorem is a variant of [IM83, Lemma 2.5] (which deals with evaluation of straight-line programs over $\mathbb{Z}$) for arithmetic circuits over $\mathbb{Q}$.

Theorem 2.4.2. *We have* $\mathsf{Eval}_{\mathbb{Q}} \in \mathbf{coRP}$.

The algorithm and proof, given below, are based on the following fact: Given an instance $(C, \boldsymbol{a})$ of $\mathsf{Eval}_{\mathbb{Q}}$ with $C(\boldsymbol{a}) \neq 0$, a random integer $m \geq 1$ will with high probability divide neither the numerator of $C(\boldsymbol{a})$ nor any occuring denominator. To compute with "rational numbers modulo integers", we use the following setting. Regard $C(\boldsymbol{a})$ as a variable-free circuit, let $b_1, \ldots, b_k \geq 1$ be the denominators of its constants, and consider the multiplicative set $U := \{b_1^{i_1} \cdots b_k^{i_k} \mid i_1, \ldots, i_k \geq 0\}$. Then the rational numbers computed at the gates

of $C(\boldsymbol{a})$ are contained in the localization $U^{-1}\mathbb{Z}$. Let $\varphi\colon \mathbb{Z} \twoheadrightarrow \mathbb{Z}/\langle m\rangle$ be the canonical surjection. If $\gcd(m, b_i) = 1$ for all $i \in [k]$, then $\varphi(U) \subseteq (\mathbb{Z}/\langle m\rangle)^*$. This implies that there is a ring homomorphism $\varphi'\colon U^{-1}\mathbb{Z} \to \mathbb{Z}/\langle m\rangle$ given by $u^{-1}a \mapsto \varphi(u)^{-1}\varphi(a)$ for $u \in U$ and $a \in \mathbb{Z}$. Given $c \in U^{-1}\mathbb{Z}$, the image $\varphi'(c)$ will be called c **modulo** m and will be denoted by $c \pmod m$. If m does not divide the numerator of $C(\boldsymbol{a})$, then $C(\boldsymbol{a}) \neq 0 \pmod m$.

Algorithm 2.4.3.
Input: An arithmetic circuit C over $\mathbb{Q}[\boldsymbol{x}]$ and $\boldsymbol{a} \in \mathbb{Q}^n$.
Acceptance: If $C(\boldsymbol{a}) = 0$, then the algorithm always accepts. If $C(\boldsymbol{a}) \neq 0$, then the algorithm rejects with probability $\geq 1/2$.

(1) Set $s \leftarrow \max\{\operatorname{size}(C) + \operatorname{bs}(\boldsymbol{a}), 4\} \in \mathbb{N}_{>0}$, set $j \leftarrow 0$, and set $d \leftarrow (\prod_{i=1}^{k} \operatorname{den}(c_i)) \cdot (\prod_{i=1}^{n} \operatorname{den}(a_i)) \in \mathbb{N}_{>0}$, where $c_1, \ldots, c_k \in \mathbb{Q}$ are the constants of C.

(2) Set $j \leftarrow j + 1$. If $j > 3s^2$, then accept.

(3) Pick $m \in [2^{2s^2}]$ at random.

(4) If $\gcd(m, d) \neq 1$, then go to step (2).

(5) If $C(\boldsymbol{a}) = 0 \pmod m$, then go to step (2), otherwise reject.

Proof of Theorem 2.4.2. We will show that Algorithm 2.4.3 is correct and runs in polynomial time. If $C(\boldsymbol{a}) = 0$, then the algorithm obviously always accepts, so assume $C(\boldsymbol{a}) \neq 0$.

By Lemma 2.2.7 (b), we have $\operatorname{bs}(d) \leq \sum_{i=1}^{k} \operatorname{bs}(\operatorname{den}(c_i)) + \sum_{i=1}^{n} a_i \leq \operatorname{size}(C) + \operatorname{bs}(\boldsymbol{a}) \leq s$. Since $d \neq 0$, this implies that there are at most s prime numbers dividing s.

Consider $C(\boldsymbol{a})$ as a variable-free arithmetic circuit and let $B \geq 1$ be the sum of the bit-sizes of its constants. Then we have

$$B \leq |C| \cdot \max\{\operatorname{size}(C), \operatorname{bs}(\boldsymbol{a})\} \leq s^2.$$

By Theorem 2.2.8, we obtain

$$\begin{aligned} \operatorname{bs}(C(\boldsymbol{a})) &\leq \operatorname{fdeg}(C) \cdot \ell(\operatorname{fanin}(C)) \cdot (2\operatorname{depth}(C) + 1) \cdot B \\ &\leq s^s \cdot s \cdot (2s + 1) \cdot s^2 \leq 2^{s^2}. \end{aligned}$$

Since $C(\boldsymbol{a}) \neq 0$, this implies that there are at most 2^{s^2} prime numbers dividing $\operatorname{num}(C(\boldsymbol{a}))$.

By Corollary A.1.2, the set $[2^{2s^2}]$ contains at least $2^{2s^2}/(2s^2)$ prime numbers. This implies that $[2^{2s^2}]$ contains at least $2^{2s^2}/(2s^2) - 2^{s^2} - s$ primes

m such that $\gcd(m, d) = 1$ and m does not divide $\operatorname{num}(C(\boldsymbol{a}))$. Since $2^{2s^2}/(2s^2) - 2^{s^2} - s \geq 2^{2s^2}/(3s^2)$, we obtain

$$\Pr_{m \in [2^{2s^2}]} \big[\gcd(m, d) = 1 \text{ and } m \nmid \operatorname{num}(C(\boldsymbol{a}))\big] \geq \frac{1}{3s^2}. \tag{2.4.1}$$

If this event happens for some integer $m \in [2^{2s}]$, then C may be evaluated at $\boldsymbol{a}$ modulo m and we have $C(\boldsymbol{a}) \neq 0 \pmod{m}$.

Now consider one round of Algorithm 2.4.3, i. e. steps (2) to (5). By (2.4.1), the probability that $(C, \boldsymbol{a})$ is rejected at the end of the round is at least $1/(3s^2)$. We conclude that the probability that $(C, \boldsymbol{a})$ is rejected in one of the $3s^2$ rounds is at least

$$1 - \left(1 - \frac{1}{3s^2}\right)^{3s^2} \geq 1 - \exp(-1) \geq 1/2,$$

hence Algorithm 2.4.3 works correctly.

The algorithm runs in polynomial time, because all computations are performed on rational numbers of bit-size at most $\operatorname{poly}(s)$. □

Remark 2.4.4. It is tempting to hope that an integer which is computed by a variable-free arithmetic circuit has just a small number of prime divisors, so that Algorithm 2.4.3 could be derandomized. However, this is not the case by the following example due to Noam Elkies. Let $n \geq 2$ and let π_n be the product of the first n prime numbers. By [Koi96, Lemma 4], the integer

$$\pi_n^{\pi_n} - 1$$

has at least 2^n distinct prime factors. Using repeated squaring, this number can be computed by an arithmetic circuit of encoding size $\operatorname{poly}(n)$.

Parallel evaluation of polynomial-degree arithmetic circuits

Arithmetic circuits of polynomial degree can be evaluated efficiently, even in parallel [MRK88, BCGR92].

Theorem 2.4.5. *Let $K = \mathbb{Q}$ or $K = \mathbb{F}_q$ for some prime power q. Then we have* $\mathsf{Eval}_K(\mathcal{C}_{\text{poly-deg}}) \in$ **NC**.

Proof. We want to invoke [MRK88, Theorem 5.3]. Let $C \in \mathcal{C}_{\text{poly-deg}} \cap K[\boldsymbol{x}]$ and let $\boldsymbol{a} \in K^n$. Consider $C(\boldsymbol{a})$ as a variable-free arithmetic circuit and set $s := \operatorname{size}(C(\boldsymbol{a}))$ and $d := \operatorname{fdeg}(C(\boldsymbol{a})) = \operatorname{poly}(s)$.

First note that $C(\boldsymbol{a})$ can be converted to an arithmetic circuit C' in accordance with [MRK88, Definition 2.1] that computes the same value and

satisfies $|C'| = \text{poly}(s)$ and $\text{fdeg}(C') = d$. The conversion can be done in $O(\log s)$ parallel time using $\text{poly}(s)$ processors.

By [MRK88, Theorem 5.3], the value of C' can be computed in parallel in time $O((\log s)(\log sd)) = O(\log^2 s)$ using $\text{poly}(s)$ processors, where addition and multiplication in K are assumed to consume unit time. If $K = \mathbb{F}_q$ for some prime power q, this implies $\mathsf{Eval}_K(\mathcal{C}_{\text{poly-deg}}) \in \mathbf{NC}$, because addition and multiplication in $\mathbb{F}_q$ can be done in $\text{poly}(\log\log q)$ parallel time using $\text{poly}(\log q)$ processors.

Now let $K = \mathbb{Q}$. By Theorem 2.2.8, we have $\text{bs}(C(\boldsymbol{a})) \le \text{fdeg}(C(\boldsymbol{a})) \cdot \ell(\text{fanin}(C(\boldsymbol{a}))) \cdot (2\,\text{depth}(C(\boldsymbol{a})) + 1) \cdot s = \text{poly}(s)$. Since it is not known whether the gcd of two $\text{poly}(s)$-bit integers can be computed in $\text{poly}(\log s)$ parallel time, we cannot perform the computations directly in K. However, for a $\text{poly}(\log s)$-bit prime p, addition, multiplication, and inversion in $\mathbb{F}_p$ are easily possible in $\text{poly}(\log s)$ parallel time using $\text{poly}(s)$ processors. Since $\text{bs}(C(\boldsymbol{a})) = \text{poly}(s)$, there are only $N = \text{poly}(s)$ prime numbers dividing $\text{num}(C(\boldsymbol{a}))$ or any denominator in C or $\boldsymbol{a}$. By Corollary A.1.2 (b), the interval $[(N+1)^2]$ contains a prime p that does divide neither of them, thus $C(\boldsymbol{a}) = 0$ if and only if $C(\boldsymbol{a}) = 0 \pmod p$. Such a prime can be computed in $\text{poly}(\log s)$ parallel time using $\text{poly}(s)$ processors, therefore we obtain $\mathsf{Eval}_K(\mathcal{C}_{\text{poly-deg}}) \in \mathbf{NC}$. □

P-hardness of evaluating general arithmetic circuits

By the following theorem, it is unlikely (under standard complexity-theoretic conjectures) that general arithmetic circuits can be evaluated efficiently in parallel.

Theorem 2.4.6. *Let K be a computable field. Then Eval_K is $\mathbf{P}$-hard under log-space reductions.*

Proof. By [Lad75], the evaluation of boolean circuits is $\mathbf{P}$-hard. By Lemma 2.3.6, this problem reduces to Eval_K. The reduction can be carried out in logarithmic space. □

Corollary 2.4.7. *The problem $\mathsf{Eval}_{\mathbb{F}_q}$ is $\mathbf{P}$-complete for all prime powers q.*

Proof. Arithmetic circuits over finite fields can be evaluated in polynomial time, thus the assertion follows from Theorem 2.4.6. □

Summary

The results of this section are summarized in the following table.

$\mathcal{C}$	K	Complexity of $\mathsf{Eval}_K(\mathcal{C})$	Reference
$\mathcal{C}_{\text{all}}$	$\mathbb{Q}$	**coRP**, **P**-hard	Theorem 2.4.2, 2.4.6
	$\mathbb{F}_q$	**P**-complete	Corollary 2.4.7
$\mathcal{C}_{\text{poly-deg}}$	$\mathbb{Q}$ or $\mathbb{F}_q$	**NC**	Theorem 2.4.5

This table raises the question whether the algorithm for $\mathsf{Eval}_{\mathbb{Q}}$ could be derandomized. By Theorem 2.6.3, $\mathsf{Eval}_{\mathbb{Q}}$ is computationally equivalent to $\mathsf{PIT}_{\mathbb{Q}}$, therefore such a derandomization seems difficult with the proof techniques currently available.

2.5 Randomized Algorithms

Everything of importance has been said before
by somebody who did not discover it.
(Alfred N. Whitehead)

In this section we review the classical randomized algorithms for PIT_K when $K = \mathbb{Q}$ or $K = \mathbb{F}_q$ for some prime power q. We also present randomized parallel algorithms for the case of polynomial-degree arithmetic circuits.

The Schwartz–Zippel Lemma

The randomized algorithms in this section are based on a famous lemma which is usually attributed to Schwartz [Sch80] and Zippel [Zip79], but was discovered before [DL78] (a version with $R = S = \mathbb{F}_q$ even dates back to [Ore22], but was not used for PIT). The lemma bounds the probability of a point being the root of a non-zero polynomial. The following variant of the lemma is similar to [AM10, Lemma 25].

Lemma 2.5.1 (Schwartz–Zippel Lemma)**.** *Let R be a ring and let $S \subseteq R$ be a non-empty finite subset such that $a-b$ is a non-zerodivisor for all $\{a, b\} \in \binom{S}{2}$. Let $f \in R[\boldsymbol{x}]$ be a non-zero polynomial of degree $d \geq 0$. Then*

$$\Pr_{\boldsymbol{a} \in S^n}\big[f(\boldsymbol{a}) = 0\big] \leq \frac{d}{|S|}.$$

Proof. We use induction on n. The case $n = 0$ is clear (in this case, $d = 0$). Now let $n \geq 1$. Let $\delta := \deg_{x_n}(f)$ and write $f = \sum_{i=1}^{\delta} g_i \cdot x_n^i$, where $g_i \in R[x_1, \ldots, x_{n-1}]$ for $i \in [\delta]$. The polynomial g_δ is non-zero and of degree $d-\delta$, hence we have

$$N_1 := \#\big\{(\boldsymbol{a}, a) \in S^{n-1} \times S \mid g_\delta(\boldsymbol{a}) = 0\big\} \leq (d-\delta)|S|^{n-2}|S| = (d-\delta)|S|^{n-1}$$

by induction hypothesis. If $g_\delta(\boldsymbol{a}) \neq 0$ for some $\boldsymbol{a} \in S^{n-1}$, then $f_{\boldsymbol{a}} := f(\boldsymbol{a}, x_n) \in R[x_n]$ is a non-zero univariate polynomial of degree δ, thus Lemma 2.5.3 implies

$$N_2 := \#\big\{(\boldsymbol{a}, a) \in S^{n-1} \times S \mid g_\delta(\boldsymbol{a}) \neq 0 \text{ and } f_{\boldsymbol{a}}(a) = 0\big\} \leq \delta \cdot |S|^{n-1}.$$

We conclude $\#\big\{\boldsymbol{a} \in S^n \mid f(\boldsymbol{a}) = 0\big\} \leq N_1 + N_2 = d \cdot |S|^{n-1}$. □

Remark 2.5.2. If R is an integral domain, then $a - b$ is a non-zerodivisor for all $\{a, b\} \in \binom{R}{2}$. If R is a K-algebra, where K is a field, then $a - b$ is a non-zerodivisor for all $\{a, b\} \in \binom{K}{2}$.

In the proof of the Schwartz–Zippel Lemma we used the following fact.

Lemma 2.5.3. *Let R be a ring and let $S \subseteq R$ be a subset such that $a - b$ is a non-zerodivisor for all $\{a, b\} \in \binom{S}{2}$. Let $f \in R[x]$ be a non-zero polynomial of degree $d \geq 0$. Then f has at most d zeros in S.*

Proof. We use induction on d. The case $d = 0$ is clear. Now let $d \geq 1$. Assume that there exists $b \in S$ such that $f(b) = 0$ (otherwise we are done). By long division, we can write $f = g \cdot (x - b)$ for some non-zero polynomial $q \in R[x]$ of degree $d - 1$. By induction hypothesis, g has at most $d - 1$ zeros in S. Since $a - b$ is a non-zerodivisor for all $a \in S \setminus \{b\}$, we infer that f has at most d zeros in S. □

Alon's Combinatorial Nullstellensatz [Alo99] (in the "non-vanishing version") is similar to the Schwartz–Zippel Lemma. In fact, the special case [Alo99, Lemma 2.1] is a direct corollary of Lemma 2.5.1. The following variant of the Nullstellensatz is proven in [Mic10].

Theorem 2.5.4 (Combinatorial Nullstellensatz)**.** *Let R be a ring and let $S_1, \ldots, S_n \subseteq R$ be non-empty finite subsets such that $a - b$ is a non-zerodivisor for all $\{a, b\} \in \binom{S_i}{2}$ and all $i \in [n]$. Let $f \in R[\boldsymbol{x}]$ be a non-zero polynomial, and let $d_1, \ldots, d_n \geq 0$ such that $d_1 + \cdots + d_n = \deg(f)$ and $x_1^{d_1} \cdots x_n^{d_n} \in \operatorname{Supp}(f)$. If $|S_i| \geq d_i + 1$ for all $i \in [n]$, then $f(\boldsymbol{a}) \neq 0$ for some $\boldsymbol{a} \in S_1 \times \cdots \times S_n$.*

Randomized PIT over $\mathbb{F}_q$

Over finite fields, the Schwartz–Zippel Lemma gives (almost) directly rise to a randomized algorithm. Given an arithmetic circuit C over $\mathbb{F}_q[\boldsymbol{x}]$, pick a point $\boldsymbol{a} \in \mathbb{F}_q^n$ at random and declare C to be zero if and only if $C(\boldsymbol{a}) = 0$. This algorithm can err only if $C \neq 0$ and we are unlucky enough to draw a root of C. To keep the probability of this event low, the finite field has to

be large enough, so we might have to compute a field extension of $\mathbb{F}_q$ first. The evaluation of C can be done in polynomial time, for polynomial-degree circuits even in poly-logarithmic parallel time using a polynomial number of processors.

Theorem 2.5.5. *Let q be a prime power.*

(a) We have $\mathsf{PIT}_{\mathbb{F}_q} \in \mathbf{coRP}$.

(b) We have $\mathsf{PIT}_{\mathbb{F}_q}(\mathcal{C}_{\text{poly-deg}}) \in \mathbf{coRNC}$.

Algorithm 2.5.6 (Randomized PIT over $\mathbb{F}_q$)**.**
Input: An arithmetic circuit C over $\mathbb{F}_q[x_1, \ldots, x_n]$.
Acceptance: If $C = 0$, then the algorithm always accepts. If $C \neq 0$, then the algorithm rejects with probability $\geq 1/2$.

(1) Determine an upper bound d for $\operatorname{fdeg}(C)$.

(2) Compute a finite field extension $L/\mathbb{F}_q$ such that $|L| \geq 2d$.

(3) Pick a point $\boldsymbol{a} \in L^n$ at random.

(4) If $C(\boldsymbol{a}) = 0$, then accept, otherwise reject.

Proof of Theorem 2.5.5. First we show that Algorithm 2.5.6 works correctly. Let C be an arithmetic circuit over $\mathbb{F}_q[\boldsymbol{x}]$ given as input. If $C = 0$, then the algorithm obviously always accepts, so assume $C \neq 0$. Then we have $\deg(C) \leq d$, thus, by Lemma 2.5.1, the algorithm rejects with probability

$$\Pr_{\boldsymbol{a} \in L^n}\big[C(\boldsymbol{a}) \neq 0\big] = 1 - \Pr_{\boldsymbol{a} \in L^n}\big[C(\boldsymbol{a}) = 0\big] \geq 1 - \frac{\deg(C)}{|L|} \geq 1 - \frac{d}{2d} = 1/2.$$

Therefore, Algorithm 2.5.6 is correct.

To show (a), let C be an arithmetic circuit over $\mathbb{F}_q[\boldsymbol{x}]$ given as input, and let $s := |C|$. By Lemma 2.2.4, we have $\operatorname{fdeg}(C) \leq \operatorname{fanin}(C)^{\operatorname{depth}(C)} \leq 2^{s^2}$, hence we may take $d := 2^{s^2}$ in step (1). By Lemma 2.2.9 (a), we can compute a finite field extension $L/\mathbb{F}_q$ of degree at least s^2 in $\operatorname{poly}(s, \log q)$ time. The evaluation of C at a point $\boldsymbol{a} \in L^n$ can be done in $\operatorname{poly}(s, \log q)$ time, too.

To show (b), let C be an arithmetic circuit over $\mathbb{F}_q[\boldsymbol{x}]$ given as input such that $\operatorname{fdeg}(C) \leq f(s)$ for some fixed polynomial $f \in \mathbb{N}[z]$ (associated with the circuit class $\mathcal{C}_{\text{poly-deg}}$), where $s := |C|$. Thus, we may take $d := f(s)$ in step (1). By Lemma 2.2.9 (b), we can compute a finite field extension $L/\mathbb{F}_q$ such that $|L| \geq 2d$ in $\operatorname{poly}(\log s)$ parallel time using $\operatorname{poly}(s)$ processors. Since addition and multiplications in L can be performed in $\operatorname{poly}(\log s)$ parallel time using $\operatorname{poly}(s)$ processors, the proof of Theorem 2.4.5 shows that C can be evaluated at a point $\boldsymbol{a} \in L^n$ in $\operatorname{poly}(\log s)$ parallel time using $\operatorname{poly}(s)$ processors, too. □

Randomized PIT over $\mathbb{Q}$

Over the rationals, we also obtain algorithms based on the Schwartz–Zippel Lemma. Here we do not have to care about the field being too small, but rather about the rationals growing too big during the evaluation. The evaluation of polynomial-degree arithmetic circuits can be done deterministically in poly-logarithmic parallel time using a polynomial number of processors. For circuits of unbounded degree, additional randomness is required for their evaluation (see [IM83, Lemma 2.6], [KI04, Lemma 2.20], and Section 2.4). Alternatively, Theorem 2.4.2 in conjunction with Theorem 2.6.3 below yields an algorithm that sidesteps the Schwartz–Zippel Lemma.

Theorem 2.5.7.

(a) We have $\mathsf{PIT}_{\mathbb{Q}} \in \mathbf{coRP}$.

(b) We have $\mathsf{PIT}_{\mathbb{Q}}(\mathcal{C}_{\text{poly-deg}}) \in \mathbf{coRNC}$.

Algorithm 2.5.8 (Randomized PIT over $\mathbb{Q}$)**.**
Input: An arithmetic circuit C over $\mathbb{Q}[x_1, \ldots, x_n]$.
Acceptance: If $C = 0$, then the algorithm always accepts. If $C \neq 0$, then the algorithm rejects with probability $\geq 1/2$.

(1) Set $s \leftarrow \max\{\text{size}(C), 5\}$ and set $j \leftarrow 0$.

(2) Set $j \leftarrow j + 1$. If $j > 6s^2$, then accept.

(3) Pick $\boldsymbol{a} \in [2s^s]^n$ and $m \in [2^{2s^2}]$ at random.

(4) If $\gcd(m, \text{den}(c)) \neq 1$ for some constant c of C, then go to step (2).

(5) If $C(\boldsymbol{a}) = 0 \pmod{m}$, then go to step (2), otherwise reject.

Proof of Theorem 2.5.7. Part (a) follows from Algorithm 2.5.8, whose correctness can be shown along the lines of the proofs of Theorem 2.5.5 (invoking the Schwartz–Zippel Lemma) and Theorem 2.4.2 (evaluating the circuit).

Part (b) can be shown using an algorithm similar to Algorithm 2.5.8, where the evaluation is done in deterministic poly-logarithmic time using a polynomial amount of processors as in the proof of Theorem 2.4.5. □

Remark 2.5.9. This thesis focuses on deterministic PIT algorithms for restricted circuit classes. Another line of research deals with reducing the randomness of PIT algorithms for more general circuit classes, see for example [CK00, LV98, AB03, KS01, BHS08, BE11].

2.6 Derandomization Hypotheses

Creativity is the ability to introduce order into the randomness of nature.
(Eric Hoffer)

Many researchers believe that randomness "does not help" in efficient computation. In particular, it is conjectured that we have $\mathbf{BPP} = \mathbf{P}$ and $\mathbf{RNC} = \mathbf{coRNC} = \mathbf{NC}$. This leads to the big main conjecture of PIT.

Conjecture 2.6.1 (Main)**.** *Let $K = \mathbb{Q}$ or $K = \mathbb{F}_q$ for some prime power q. Then we have $\mathsf{PIT}_K \in \mathbf{P}$ and $\mathsf{PIT}_K(\mathcal{C}_{\text{poly-deg}}) \in \mathbf{NC}$.*

In this section, we present some general strategies for attacking the PIT problem, together with a few more concrete derandomization hypotheses.

Kronecker substitution

A common theme of many PIT algorithms is the reduction of the number of variables. One way to achieve this is a method, usually referred to as *Kronecker substitution*, that goes back to [Kro82, §4]. Let $d \geq 0$ and let $f \in K[\boldsymbol{x}]$ be a non-zero polynomial of degree at most d. Then, for $D \geq d+1$, the univariate polynomial

$$f\big(z, z^D, \ldots, z^{D^{n-1}}\big) \in K[z] \tag{2.6.1}$$

is non-zero, because the terms of f are being mapped to distinct terms. This is a consequence of the following simple lemma.

Lemma 2.6.2. *Let $d_1, \ldots, d_n \geq 0$ be integers and let $D_i := \prod_{j=1}^{i-1}(d_j + 1)$ for $i \in [n+1]$. Then the map*

$$[0, d_1] \times \cdots \times [0, d_n] \to [0, D_{n+1} - 1], \quad (\delta_1, \ldots, \delta_n) \mapsto \sum_{i=1}^{n} \delta_i D_i$$

is bijective.

Proof. We use induction on n. For $n = 1$, the map under consideration is the indentity $[0, d_1] \to [0, d_1]$, hence it is bijective.

Now let $n > 1$, and let $a \in [0, D_{n+1} - 1]$. Then there exist unique $a', \delta_n \geq 0$ such that $a = a' + \delta_n D_n$ and $a' < D_n$. We have $\delta_n \in [0, d_n]$, because otherwise $a \geq (\delta_n + 1)D_n = D_{n+1}$. By induction, there exists a unique $(\delta_1, \ldots, \delta_{n-1}) \in [0, d_1] \times \cdots \times [0, d_{n-1}]$ such that $a' = \sum_{i=1}^{n-1} \delta_i D_i$. Altogether, there exists a unique $(\delta_1, \ldots, \delta_n) \in [0, d_1] \times \cdots \times [0, d_n]$ such that $a = \sum_{i=1}^{n} \delta_i D_i$. Therefore, the map under consideration is bijective. □

Note that a Kronecker substitution causes an exponential blowup of the degree. However, if f is given as arithmetic circuit of size s, we can compute a circuit for (2.6.1) of size $\mathrm{poly}(s)$ by repeated squaring.

The Kronecker substitution can be used to show that identity testing over $\mathbb{Q}$ is actually computationally equivalent to evaluation (cf. [ABKM06, Proposition 2.2]).

Theorem 2.6.3. *The problems* $\mathsf{PIT}_{\mathbb{Q}}$ *and* $\mathsf{Eval}_{\mathbb{Q}}$ *are polynomial-time equivalent.*

The proof, given below, is based on the following lemma, which states that the absolute value of the roots of complex univariate polynomials can be bounded by the absolute values of the coefficients. As a consequence, in order to reduce $\mathsf{PIT}_{\mathbb{Q}}$ to $\mathsf{Eval}_{\mathbb{Q}}$, we can first apply a Kronecker substitution to a given circuit and then choose a sufficiently large integer as evaluation point.

Lemma 2.6.4 (Cauchy's bound, [HM97, Theorem 2])**.** *Let* $f = \sum_{i=0}^{d} c_i x^i \in \mathbb{C}[x]$ *be a univariate polynomial with* $c_d \neq 0$*, and let* $a \in \mathbb{C}$ *be a root of* f*. Then we have*

$$|a| < 1 + \max_{0 \leq i \leq d-1} |c_i / c_d|.$$

Proof of Theorem 2.6.3. The problem $\mathsf{Eval}_{\mathbb{Q}}$ clearly reduces to $\mathsf{PIT}_{\mathbb{Q}}$, because evaluation of an arithmetic circuit is the same as identity testing of a variable-free arithmetic circuit.

To show that $\mathsf{PIT}_{\mathbb{Q}}$ reduces to $\mathsf{Eval}_{\mathbb{Q}}$, let C be an arithmetic circuit over $\mathbb{Q}[\boldsymbol{x}]$. Set $s := \max\{\mathrm{size}(C), n, 5\}$, set $D := s^s + 1$, and consider the univariate polynomial

$$C\big(z^{D^0}, z^{D^1}, \ldots, z^{D^{n-1}}\big) \in \mathbb{Q}[z].$$

Using repeated squaring, this polynomial can be computed by an arithmetic circuit C' with $\mathrm{size}(C') = \mathrm{poly}(s)$. By Lemma 2.2.4, we have $\mathrm{fdeg}(C) < D$, therefore, by Lemma 2.6.2, we have $C = 0$ if and only if $C' = 0$.

Now set $B := 2^{s^2}$. By Lemma 2.2.7, we have $|\mathrm{num}(c)| \leq 2^s$ and $\mathrm{den}(c) \leq 2^s$ for all constants $c \in \mathbb{Q}$ of C. Now let $c, d \in \mathbb{Q}$ be coefficients of C with $d \neq 0$. Since c and d are polynomials in the constants of C of degree at most

$\operatorname{fdeg}(C) \leq s^s$, we obtain

$$\begin{aligned} |c| \cdot |d|^{-1} &\leq |c| \cdot \operatorname{den}(d) \\ &\leq \left(\tbinom{n+s^s}{s^s} \cdot (2^s)^{s^s} \right) \cdot \left((2^s)^s \right)^{s^s} \\ &\leq \left((s+1)^{s^s} \cdot 2^{s^{s+1}} \right) \cdot 2^{s^{s+2}} \\ &\leq 2^{3s^{s+2}} \\ &\leq 2^B - 1. \end{aligned}$$

Consider the univariate polynomial $C'\big((2z)^B\big) \in \mathbb{Q}[z]$. Again, using repeated squaring, this polynomial can be computed by an arithmetic circuit C'' with $\operatorname{size}(C'') = \operatorname{poly}(s)$. Since C and C' have the same coefficients, Lemma 2.6.4 yields $C' = 0$ if and only if $C''(1) = 0$.

Given C, the arithmetic circuit C'' can be computed in polynomial time, and we have $C \in \mathsf{PIT}_{\mathbb{Q}}$ if and only if $(C'', 1) \in \mathsf{Eval}_{\mathbb{Q}}$. □

Agrawal's paradigm

Agrawal introduced a general paradigm for derandomizing polynomial identity testing [Agr03, Agr05]. His idea is to reduce univariate circuits of high degree (for instance, obtained by a Kronecker substitution) modulo several low-degree polynomials. One hopes that in this way a non-zero circuit will remain non-zero for some reduction. The following conjecture, if true, would imply a polynomial-time identity test for constant-depth circuits.

Conjecture 2.6.5. *Let K be a field and let C be a constant-depth arithmetic circuit over $K[\boldsymbol{x}]$. Then $C \neq 0$ if and only if*

$$C\big(z^{D^0}, z^{D^1}, \ldots, z^{D^{n-1}}\big) \neq 0 \pmod{\langle z^r - 1 \rangle_{K[z]}} \qquad \text{for some } r \in [N],$$

where $D := \operatorname{fdeg}(C) + 1$ and $N = \operatorname{poly}(|C|)$.

Agrawal's approach was successfully employed to obtain a deterministic polynomial-time primality test [AKS04]. It also works for sparse polynomials [Agr05, BHLV09], see Section 3.2.2.

Isolation of terms

Another possibility to obtain a multivariate to univariate reduction of polynomials is via isolating weight vectors [MVV87, CRS95, KS01, AM08]. For a weight vector $w \in \mathbb{N}^n$ and a vector $\alpha \in \mathbb{R}^n_{\geq 0}$, we define $|\alpha|_w := w_1\alpha_1 + \cdots + w_n\alpha_n$ (see Appendix A.3.2).

Definition 2.6.6. Let $A \subseteq \mathbb{R}^n_{\geq 0}$ be a subset and let $w \in \mathbb{N}^n$ be a weight vector.

(a) Let $\alpha \in A$. If $|\alpha|_w < |\beta|_w$ for all $\beta \in A \setminus \{\alpha\}$, then we say that w **isolates** α in A.

(b) If there exists $\alpha \in A$ such that w isolates α in A, then w is called **isolating** for A.

Let $d \geq 0$ and let $f \in K[\boldsymbol{x}]$ be a non-zero polynomial of degree at most d. Then the logarithmic support $A := \mathrm{LSupp}(f) \subset \mathbb{N}^n$ is non-empty. If a weight vector $w \in \mathbb{N}^n$ isolates some $\alpha \in A$, then the univariate polynomial

$$f\big(z^{w_1}, \ldots, z^{w_n}\big) \in K[z],$$

is non-zero, because it has a non-zero monomial of degree $|\alpha|_w$. Note that the Kronecker substitution (2.6.1) yields a weight vector $w := \big(1, D, \ldots, D^{n-1}\big)$ for A, though, with entries exponential in d. We are interested in weights of magnitude $\mathrm{poly}(n, d)$. The following lemma demonstrates that a weight vector which is randomly chosen from $[2nd]^n$ is isolating for A with high probability.

Lemma 2.6.7 (Isolating Lemma, [KS01, Lemma 4])**.** *Let $d, N \geq 1$, and let $A \subset \mathbb{N}^n$ such that $|\alpha| \leq d$ for all $\alpha \in A$. Then we have*

$$\Pr_{w \in [N]^n}\big[w \text{ is isolating for } A\big] \geq 1 - \frac{nd}{N}.$$

A suitable derandomization of the Isolating Lemma (see for example [AM08]) would imply a deterministic polynomial-time identity test for arithmetic circuits of polynomial degree.

Finally, we remark that it is easy to obtain an isolating weight vector for $A \subset \mathbb{N}^n$ if the convex polytope $\mathrm{Conv}(A)$ has few vertices. We will exploit this fact in Section 3.2.3.

2.7 Hitting Sets

To be sure of hitting the target, shoot first,
and call whatever you hit the target.
(Ashleigh Brilliant)

The randomized PIT algorithms given in Section 2.5 work by evaluation, where the query points are determined without "looking inside" the

given arithmetic circuit. Algorithms of this kind are referred to as *blackbox* algorithms. Blackbox algorithms require the computation of a hitting set according to the following definition.

Definition 2.7.1. Let $\mathcal{C} \subseteq K[\boldsymbol{x}]$ be a set of polynomials. A set $\mathcal{H} \subseteq K^n$ is called a **hitting set** for $\mathcal{C}$ if for all non-zero $C \in \mathcal{C}$ there exists $\boldsymbol{a} \in \mathcal{H}$ such that $C(\boldsymbol{a}) \neq 0$.

Example 2.7.2. Let us give two examples of hitting sets.

(a) Let $d \geq 0$ and let $S \subseteq K$ be a subset such that $|S| \geq d+1$. Then S^n is a hitting set for $K[\boldsymbol{x}]_{\leq d}$ by Theorem 2.5.4. The size of this hitting set is exponential in the general setting. However, for polynomial-degree circuits with constantly many variables, we obtain a polynomial-size hitting set.

(b) Let $K = \mathbb{Q}$ and let $\mathcal{C}_{n,s}$ be the set of arithmetic circuits C over $\mathbb{Q}[\boldsymbol{x}]$ such that $\operatorname{size}(C) \leq s$. Then the proof of Theorem 2.6.3 yields a hitting set for $\mathcal{C}_{n,s}$ consisting of a single point. The coordinates of this point have bit-size exponential in s.

Existence of small hitting sets

The existence of small hitting sets was proven by Heintz & Schnorr [HS80a] (in their paper, hitting sets are called "correct test sequences") for fields of characteristic zero. Here we reproduce their proof, but replace a result they use from [HS80b] by a simpler argument that works for arbitrary fields. This argument is inspired by the proof of [SY10, Theorem 3.1]. We will require some machinery from algebraic geometry which we cover in Appendix A.4.

Theorem 2.7.3. *Let $1 \leq n \leq s$ and let $d \geq 1$. Let K be a field and let $S \subseteq K$ be an arbitrary subset with $|S| \geq (2sd+2)^2$. Denote by $\mathcal{C}_{n,d,s}$ the set of arithmetic circuits C over $K[\boldsymbol{x}]$ such that $\operatorname{fdeg}(C) \leq d$ and $|C| \leq s$. Then there exists a hitting set $\mathcal{H}_{n,d,s} \subseteq S^n$ for $\mathcal{C}_{n,d,s}$ such that $|\mathcal{H}_{n,d,s}| \leq 9s$.*

Proof. Let $\boldsymbol{y} = \{y_1, \ldots, y_s\}$ be new variables and let $\mathcal{S}_{n,d,s}$ be the set of constant-free arithmetic circuits C over $K[\boldsymbol{x}, \boldsymbol{y}]$ such that $\operatorname{fdeg}(C) \leq d$ and $|C| \leq s$. Obviously, every circuit in $\mathcal{C}_{n,d,s}$ can be obtained from a circuit in $\mathcal{S}_{n,d,s}$ by substituting constants for the $\boldsymbol{y}$-variables. There are at most s^{2s} connected, directed multigraphs C with $V(C) \subseteq [s]$ and $|C| \leq s$, and the vertices of each such multigraph can be labeled by the symbols $\{+, \times, x_1, \ldots, x_n, y_1, \ldots, y_s\}$ in at most $(2s+2)^s$ different ways. Therefore, we have $|\mathcal{S}_{n,d,s}| \leq (2s+2)^{3s}$.

Set $t := \binom{n+d}{d}$ and let $\boldsymbol{x}^{\alpha_1}, \ldots \boldsymbol{x}^{\alpha_t} \in \mathbb{T}(\boldsymbol{x})$ be the terms of degree at most d. We identify a polynomial $f = \sum_{i=1}^{t} c_i \cdot \boldsymbol{x}^{\alpha_i} \in K[\boldsymbol{x}]_{\leq d}$ with its vector of

coefficients $(c_1, \dots, c_t) \in K^t$, hence $\mathcal{C}_{n,d,s} \subseteq K^t$. Let $C \in \mathcal{S}_{n,d,s}$ be a constant-free circuit. Write $C = \sum_{i=1}^{t} c_i \cdot \boldsymbol{x}^{\alpha_i}$ with $c_i \in K[\boldsymbol{y}]$. The coefficients c_i define a morphism

$$\varphi_C \colon \overline{K}^s \to \overline{K}^t, \quad \boldsymbol{a} \mapsto (c_1(\boldsymbol{a}), \dots, c_t(\boldsymbol{a}))$$

with $\deg(\varphi_C) \leq d$. Let $Y_C \subseteq \overline{K}^t$ be the Zariski closure of $\varphi_C(\overline{K}^s)$. Since $\dim(\overline{K}^s) = s$, we have $\dim(Y_C) \leq s$. By Lemma 2.7.4 below, we obtain $\deg_{\overline{K}^t}(Y_C) \leq d^s$. The affine variety

$$Y_{n,d,s} := \bigcup_{C \in \mathcal{S}_{n,d,s}} Y_C \subseteq \overline{K}^t$$

contains $\mathcal{C}_{n,d,s}$ and satisfies $\dim(Y_{n,d,s}) \leq \max\{\dim(Y_C) \mid C \in \mathcal{S}_{n,d,s}\} \leq s$ and

$$\begin{aligned} \deg_{\overline{K}^t}(Y_{n,d,s}) &\leq \sum_{C \in \mathcal{S}_{n,d,s}} \deg_{\overline{K}^t}(Y_C) \\ &\leq |\mathcal{S}_{n,d,s}| \cdot \max\bigl\{\deg_{\overline{K}^t}(Y_C) \mid C \in \mathcal{S}_{n,d,s}\bigr\} \\ &\leq (2s+2)^{3s} d^s. \end{aligned}$$

Set $m := 9s$. We want to show that there exists a tuple of points $(\boldsymbol{a}_1, \dots, \boldsymbol{a}_m) \in S^{mn}$ such that for all non-zero $C \in \mathcal{C}_{n,d,s}$ there exists $i \in [m]$ such that $C(\boldsymbol{a}_i) \neq 0$. This tuple will then constitute a desired hitting set.

Consider the affine variety

$$X := \bigl\{(f, \boldsymbol{a}_1, \dots, \boldsymbol{a}_m) \in \overline{K}^{t+mn} \mid f \in Y_{n,d,s} \text{ and } f(\boldsymbol{a}_i) = 0 \text{ for all } i \in [m]\bigr\}.$$

For $i \in [t]$ and $(j,k) \in [m] \times [n]$, let z_i and $z_{j,k}$ be the coordinates of $\overline{K}^{t+mn}$. Then X is defined by the polynomial equations for $Y_{n,d,s}$ and

$$\sum_{i=1}^{t} z_i \cdot z_{j,1}^{\alpha_{i,1}} \cdots z_{j,n}^{\alpha_{i,n}}, \quad j \in [m].$$

By Theorem A.4.7, we have

$$\deg_{\overline{K}^{t+mn}}(X) \leq \deg_{\overline{K}^{t+mn}}(Y_{n,d,s}) \cdot (d+1)^m \leq (2s+2)^{3s} d^s (d+1)^m.$$

Define the projections $\pi_1 \colon \overline{K}^{t+mn} \twoheadrightarrow \overline{K}^t$ and $\pi_2 \colon \overline{K}^{t+mn} \twoheadrightarrow \overline{K}^{mn}$ to the first t and last mn coordinates, respectively. Let $C_1, \dots, C_\ell \subseteq \overline{K}^{t+mn}$ be all irreducible components $C \subseteq X$ such that $\pi_1(C)$ contains a non-zero polynomial, and set $C := \bigcup_{i=1}^{\ell} C_i$. Then $\pi_2(C) \cap S^{mn}$ contains all tuples $(\boldsymbol{a}_1, \dots, \boldsymbol{a}_m) \in S^{mn}$ that do not constitute a hitting set for $\mathcal{C}_{n,d,s}$.

Let $i \in [\ell]$ and let $f \in \pi_1(C_i)$ such that $f \neq 0$. Then

$$\pi_1^{-1}(f) = \{f\} \times \underbrace{\mathcal{V}_{\overline{K}^n}(f) \times \cdots \times \mathcal{V}_{\overline{K}^n}(f)}_{m \text{ times}},$$

hence $\dim(\pi_1^{-1}(f)) = m(n-1)$. Applying Lemma A.4.2 to the morphism $\pi_1 \colon C_i \to Y_{n,d,s}$, we obtain

$$\dim(C_i) \leq \dim(\pi_1^{-1}(f)) + \dim(Y_{n,d,s}) \leq m(n-1) + s.$$

This implies $\dim(C) \leq \max\{\dim(C_i) \mid i \in [\ell]\} \leq m(n-1) + s$.

Now define the hypersurfaces

$$H_{j,k} := \mathcal{V}_{\overline{K}^{t+mn}}\big(\textstyle\prod_{c \in S}(z_{j,k} - c)\big)$$

for all $j \in [m]$ and $k \in [n]$, and set $H := \bigcap_{(j,k) \in [m] \times [n]} H_{j,k}$. Then we have

$$\begin{aligned}
|\pi_2(C) \cap S^{mn}| &= |\pi_2(C \cap H)| \\
&\leq \deg_{\overline{K}^{t+mn}}(C \cap H) \\
&\leq \deg_{\overline{K}^{t+mn}}(C) \cdot \max\{\deg_{\overline{K}^{t+mn}}(H_{j,k}) \mid j \in [m],\, k \in [n]\}^{\dim(C)} \\
&\leq \deg_{\overline{K}^{t+mn}}(X) \cdot |S|^{\dim(C)} \\
&\leq (2s+2)^{3s} d^s (d+1)^m \cdot |S|^{m(n-1)+s} \\
&\leq |S|^{2s+m/2} \cdot |S|^{m(n-1)+s} \\
&= |S|^{-m/6} \cdot |S|^{mn},
\end{aligned}$$

where the second inequality follows from Corollary A.4.8. This implies the existence of a tuple $(\boldsymbol{a}_1, \ldots, \boldsymbol{a}_m) \in S^{mn}$ that constitutes a hitting set for $\mathcal{C}_{n,d,s}$. □

In the proof of Theorem 2.7.3 we used the following lemma for bounding the degree of the image of a morphism.

Lemma 2.7.4. *Let $X \subseteq \overline{K}^s$ be an irreducible affine variety, let $Y \subseteq \overline{K}^t$ be an affine variety, and let $\varphi \colon X \to Y$ be a dominant morphism. Then we have*

$$\deg_{\overline{K}^t}(Y) \leq \deg_{\overline{K}^s}(X) \cdot \deg(\varphi)^{\dim(Y)}.$$

Proof. The following argument is contained in the proof of [HS80b, Lemma 1]. Set $r := \dim(Y)$. Since φ is dominant, Y is irreducible. By Theorem A.4.4, $\varphi(X)$ is a constructible set, so by Lemma A.4.3 it contains a non-empty open subset of Y. Therefore, by Lemma A.4.6, there exist affine hyperplanes $H_1, \ldots, H_r \subset \overline{K}^t$ such that $\deg_{\overline{K}^t}(Y) = |\varphi(X) \cap H_1 \cap \cdots \cap H_r|$.

Then $\varphi^{-1}(H_i) \subset \overline{K}^s$ is an affine hypersurface with $\deg_{\overline{K}^s}(\varphi^{-1}(H_i)) \leq \deg(\varphi)$ for all $i \in [r]$. By Theorem A.4.7, we obtain

$$\deg_{\overline{K}^s}\big(X \cap \varphi^{-1}(H_1) \cap \cdots \cap \varphi^{-1}(H_r)\big) \leq \deg_{\overline{K}^s}(X) \cdot \deg(\varphi)^r.$$

Let $C_1, \ldots, C_m \subseteq \overline{K}^s$ be the irreducible components of the affine variety $X \cap \varphi^{-1}(H_1) \cap \cdots \cap \varphi^{-1}(H_r)$. Since the map

$$\varphi\colon X \cap \varphi^{-1}(H_1) \cap \cdots \cap \varphi^{-1}(H_r) \to \varphi(X) \cap H_1 \cap \cdots \cap H_r$$

is surjective and $\varphi(C_i)$ is a singleton for all $i \in [m]$, we get

$$\begin{aligned}
\deg_{\overline{K}^t}(Y) &= |\varphi(X) \cap H_1 \cap \cdots \cap H_r| \\
&\leq m \\
&\leq \sum_{i=1}^{m} \deg_{\overline{K}^s}(C_i) \\
&= \deg_{\overline{K}^s}\big(X \cap \varphi^{-1}(H_1) \cap \cdots \cap \varphi^{-1}(H_r)\big) \\
&\leq \deg_{\overline{K}^s}(X) \cdot \deg(\varphi)^r,
\end{aligned}$$

finishing the proof. □

Polynomial-space computation of hitting sets

Using quantifier elimination, the proof of Theorem 2.7.3 can be turned into a polynomial-space algorithm for the computation of small hitting sets. For an introduction to quantifier elimination, see [BPR06, Chapter 1].

Theorem 2.7.5. *Let $K = \mathbb{Q}$ or $K = \mathbb{F}_q$ for some prime power q. Then there exists a Turing machine that, given $1 \leq n \leq s$ and $d \geq 1$, computes in $\mathrm{poly}(s)$-space a hitting set $\mathcal{H}_{n,d,s} \subseteq S^n$ for $\mathcal{C}_{n,d,s}$ of size $|\mathcal{H}_{n,d,s}| \leq 9s$, where $S \subset \overline{K}$ is a subset such that $\mathrm{bs}(c) = \mathrm{poly}(\log s, \log d)$ for all $c \in S$.*

Proof sketch. The description of the asserted Turing machine M is as follows. If $K = \mathbb{Q}$, then M sets $S \leftarrow [(2sd+2)^2] \subset K$. If $K = \mathbb{F}_q$ for some prime power q, then M constructs the smallest field extension L/K such that $|L| \geq (2sd+2)^2$ and picks a subset $S \subseteq L$ of size $|S| = (2sd+2)^2$. In both cases, we obtain a subset $S \subseteq \overline{K}$ such that $|S| = (2sd+2)^2$ and $\mathrm{bs}(c) = \mathrm{poly}(\log s, \log d)$ for all $c \in S$.

Next, M sets $m \leftarrow 9s$ and checks for all m-subsets $\mathcal{H} \subseteq S^n$ whether $\mathcal{H}$ is a hitting set for $\mathcal{C}_{n,d,s}$ as follows. As in the proof of Theorem 2.7.3, let $\boldsymbol{y} = \{y_1, \ldots, y_s\}$ be new variables and let $\mathcal{S}_{n,d,s}$ be the set of all constant-free arithmetic circuits C over $K[\boldsymbol{x}, \boldsymbol{y}]$ such that $\mathrm{fdeg}(C) \leq d$ and $|C| \leq s$. Let

$\overline{\mathcal{C}}_{n,d,s}$ be the set of arithmetic circuits C over $\overline{K}[\boldsymbol{x}]$ such that $\operatorname{fdeg}(C) \leq d$ and $|C| \leq s$, thus $\mathcal{C}_{n,d,s} \subseteq \overline{\mathcal{C}}_{n,d,s}$. Then $\mathcal{H}$ is a hitting set for $\overline{\mathcal{C}}_{n,d,s}$ if and only if the sentence

$$\bigwedge_{C \in \mathcal{S}_{n,d,s}} \left(\forall\, \boldsymbol{c} \in \overline{K}^s \left(\forall\, \boldsymbol{b} \in \overline{K}^n \; C(\boldsymbol{b}, \boldsymbol{c}) = 0 \right) \vee \bigvee_{\boldsymbol{a} \in \mathcal{H}} C(\boldsymbol{a}, \boldsymbol{c}) \neq 0 \right)$$

(in the first-order theory of algebraically closed fields) is true. Note that the sentence in the innermost parentheses is just another way of saying that $C(\boldsymbol{x}, \boldsymbol{c}) \in \overline{K}[\boldsymbol{x}]$ is the zero polynomial. Using quantifier elimination, M checks the truth of the sentence

$$\forall\, \boldsymbol{c} \in \overline{K}^s \left(\forall\, \boldsymbol{b} \in \overline{K}^n \; C(\boldsymbol{b}, \boldsymbol{c}) = 0 \right) \vee \bigvee_{\boldsymbol{a} \in \mathcal{H}} C(\boldsymbol{a}, \boldsymbol{c}) \neq 0$$

for all $C \in \mathcal{S}_{n,d,s}$. Since the number of quantifier alternations is constant, this can be done in $\operatorname{poly}(s)$-space [Ier89].

By Theorem 2.7.3, M will eventually find a hitting set $\mathcal{H}_{n,d,s} \subseteq S^n$ for $\overline{\mathcal{C}}_{n,d,s}$ of size $|\mathcal{H}_{n,d,s}| \leq 9s$. By reusing space, the algorithm can be implemented to run in $\operatorname{poly}(s)$-space. □

Connections to lower bounds

The following simple theorem demonstrates that small hitting sets imply lower bounds (cf. [HS80a, Theorem 4.5]). See also [Agr05] for a similar result.

Theorem 2.7.6. *Let $1 \leq n \leq s$ and let $d \geq 1$. Let K be a field, let $S \subseteq K$ be a subset, and let $K_0 \subseteq K$ be the prime field of K. Denote by $\mathcal{C}_{n,d,s}$ the set of arithmetic circuits C over $K[\boldsymbol{x}]$ such that $\operatorname{fdeg}(C) \leq d$ and $|C| \leq s$. Assume that $\mathcal{H}_{n,d,s} \subseteq S^n$ is a hitting set for $\mathcal{C}_{n,d,s}$ of size $m := |\mathcal{H}_{n,d,s}|$.*

If $m \leq \binom{n+d}{d} - 1$, then there exists a non-zero polynomial $f \in K_0(S)[\boldsymbol{x}]_{\leq d}$ with $\operatorname{sp}(f) \leq m + 1$ such that $f \notin \mathcal{C}_{n,d,s}$.

Proof. The proof is by interpolation. Denote $\mathcal{H}_{n,d,s} = \{\boldsymbol{a}_1, \ldots, \boldsymbol{a}_m\}$, let $t_1, \ldots, t_{m+1} \in \mathbb{T}(\boldsymbol{x})_{\leq d}$ be distinct terms, and let $\boldsymbol{y} = \{y_1, \ldots, y_{m+1}\}$ be new variables. Consider the homogeneous system of linear equations

$$t_1(\boldsymbol{a}_i) \cdot y_1 + \cdots + t_{m+1}(\boldsymbol{a}_i) \cdot y_{m+1} = 0, \quad i \in [m],$$

with indeterminates $\boldsymbol{y}$ and coefficients in $K_0(S)$. Since this system has more variables than equations, there exists a non-zero solution $(c_1, \ldots, c_{m+1}) \in K_0(S)^{m+1}$. The polynomial $f := \sum_{i=1}^{m+1} c_i \cdot t_i$ has the desired properties. □

Chapter 3

Linear Independence Techniques

This chapter deals with the theme of linear independence. First we present the Alternant Criterion for linear independence of polynomials. Using techniques from the existing literature, we give constructions of rank-preserving homomorphisms for linear forms, sparse polynomials, and products of linear forms. On the way, we encounter hitting set constructions for sparse polynomials and $\Sigma\Pi\Sigma$-circuits with constant top fan-in. Using isolating weight vectors, we generalize the hitting sets for sparse polynomials to polynomials whose Newton polytope can be decomposed into sparse polytopes. All constructions will be independent of the field of constants. Finally, we outline that linear independence testing and the computation of linear relations is (more or less) equivalent to PIT. In this context, we extend the polynomial-time PIT algorithm [RS05] for set-multilinear $\Sigma\Pi\Sigma$-circuits (with unbounded top fan-in) to an algorithm for computing the linear relations of set-multilinear $\Pi\Sigma$-circuits.

Chapter outline

This chapter is organized as follows. Section 3.1 contains a criterion for linear independence of polynomials. In Section 3.2 we define rank-preserving homomorphisms and give explicit constructions of rank-preserving homomorphisms and hitting sets for several circuit classes. We summarize those results in Section 3.2.5. Section 3.3 deals with the linear independence testing problem. Finally, in Section 3.4, we investigate the complexity of computing linear relations.

3.1 Linear Independence

In this section we introduce a bit of notation connected with linear independence and present a criterion for linear independence of polynomials.

Let K be a field, let A be a K-vector space, and let $a_1, \dots, a_m \in A$. Then

$$\mathrm{LinRel}_K(a_1, \dots, a_m) := \big\{\lambda \in K^m \mid \lambda_1 a_1 + \cdots + \lambda_m a_m = 0\big\} \tag{3.1.1}$$

is a K-subspace of K^m and is called the **subspace of linear relations of** $a_1, \dots, a_m$ **over** K. It is the kernel of the K-linear epimorphism

$$K^m \to \langle a_1, \dots, a_m\rangle_K, \quad \lambda \mapsto \lambda_1 a_1 + \cdots + \lambda_m a_m.$$

For a subset $S \subseteq A$, we define the **rank of** S **over** K as

$$\mathrm{rk}_K(S) := \dim_K\big(\langle S\rangle_K\big) \in \mathbb{N} \cup \{\infty\}. \tag{3.1.2}$$

We are primarily interested in the case where A is a polynomial ring over K.

3.1.1 The Alternant Criterion

Let K be a field and let $K[\boldsymbol{x}] = K[x_1, \dots, x_n]$ be a polynomial ring over K. The following theorem contains a criterion for linear independence of polynomials in $K[\boldsymbol{x}]$ if the field K is sufficiently large.

Theorem 3.1.1 (Alternant Criterion)**.** *Let K be an infinite field and let $f_1, \dots, f_m \in K[\boldsymbol{x}]$ be polynomials. Then $f_1, \dots, f_m$ are K-linearly independent if and only if there exist points $\boldsymbol{a}_1, \dots, \boldsymbol{a}_m \in K^n$ such that*

$$\det\big(f_i(\boldsymbol{a}_j)\big)_{1\le i,j\le m} \neq 0.$$

Proof. By Theorem 2.5.4, this follows from Lemma 3.1.2 below. □

The Alternant Criterion is based on the following assertion which appeared in the proof of [Kay10, Lemma 8].

Lemma 3.1.2. *Let $f_1, \dots, f_m \in K[\boldsymbol{x}]$ be polynomials. Define the matrix*

$$A := \begin{pmatrix} f_1(t_{1,1}, \dots, t_{1,n}) & \cdots & f_m(t_{1,1}, \dots, t_{1,n}) \\ \vdots & & \vdots \\ f_1(t_{m,1}, \dots, t_{m,n}) & \cdots & f_m(t_{m,1}, \dots, t_{m,n}) \end{pmatrix} \in K[\boldsymbol{t}]^{m\times m},$$

where $\boldsymbol{t} = \{t_{i,j} \mid i \in [m] \text{ and } j \in [n]\}$ are new variables. Then $f_1, \dots, f_m$ are K-linearly independent if and only if $\det(A) \neq 0$.

Proof. By a linear algebra argument, $f_1, \ldots, f_m$ are K-linearly independent if and only if they are $\overline{K}$-linearly independent. Therefore, we may assume that K is infinite.

First let $f_1, \ldots, f_m$ be K-linearly dependent. Then the columns of A are $K(\boldsymbol{t})$-linearly dependent, hence $\det(A) = 0$.

Conversely, assume that $f_1, \ldots, f_m$ are K-linearly independent. We show $\det(A) \neq 0$ by induction on m. The case $m = 1$ is obvious, so let $m \geq 2$. Expanding $\det(A)$ by the last row, we get

$$\det(A) = \sum_{j=1}^{m} (-1)^{j+m} \cdot f_j(t_{m,1}, \ldots, t_{m,n}) \cdot \det(A_{m,j}), \tag{3.1.3}$$

where $A_{m,j} \in K[\boldsymbol{t} \setminus \{t_{m,1}, \ldots, t_{m,n}\}]^{(m-1)\times(m-1)}$ is obtained from A by deleting the m-th row and j-th column. By induction hypothesis, we have $\det(A_{m,1}) \neq 0$. Since K is infinite, Theorem 2.5.4 implies that there exist $c_{i,k} \in K$ for $i \in [m-1]$ and $j \in [n]$ such that $(\det(A_{m,1}))(\boldsymbol{c}) \neq 0$, where $\boldsymbol{c} = (c_{i,k})$. Since $f_1(t_{m,1}, \ldots, t_{m,n}), \ldots, f_m(t_{m,1}, \ldots, t_{m,n})$ are K-linearly independent, (3.1.3) implies $(\det(A))(\boldsymbol{c}) \neq 0$, hence $\det(A) \neq 0$. □

3.2 Rank-Preserving Homomorphisms

Let $n, r \geq 1$, let K be a field, and let $K[\boldsymbol{x}] = K[x_1, \ldots, x_n]$ and $K[\boldsymbol{z}] = K[z_1, \ldots, z_r]$ be polynomial rings over K. In this section we investigate K-algebra homomorphisms that preserve the rank of a given set of polynomials.

Definition 3.2.1. Let $\varphi\colon K[\boldsymbol{x}] \to K[\boldsymbol{z}]$ be a K-algebra homomorphism and let $f_1, \ldots, f_m \in K[\boldsymbol{x}]$ be polynomials. If

$$\mathrm{rk}_K(\varphi(f_1), \ldots, \varphi(f_m)) = \mathrm{rk}_K(f_1, \ldots, f_m),$$

then φ is called **rank-preserving for** $\{f_1, \ldots, f_m\}$.

Existence of rank-preserving homomorphisms

The following theorem shows that toric rank-preserving homomorphisms exist for every set of polynomials and for $r = 1$. The proof is based on a Kronecker substitution (see Section 2.6).

Theorem 3.2.2. *Let $f_1, \ldots, f_m \in K[\boldsymbol{x}]$ be polynomials. Then there exists a toric K-algebra homomorphism $\varphi\colon K[\boldsymbol{x}] \to K[z]$ which is rank-preserving for $\{f_1, \ldots, f_m\}$.*

Proof. Let $d_1, \dots, d_n \geq 0$ such that $\deg_{x_i}(f_j) \leq d_i$ for all $i \in [n]$ and $j \in [m]$. Set $D_i := \prod_{j=1}^{i-1}(d_j+1)$ for $i \in [n+1]$ and define the K-algebra homomorphism

$$\varphi\colon K[\boldsymbol{x}] \to K[z], \quad x_i \mapsto z^{D_i},$$

where $i \in [n]$. Let $V := \left\langle f \in K[\boldsymbol{x}] \setminus \{0\} \mid \deg_{x_i}(f) \leq d_i \text{ for all } i \in [n] \right\rangle_K$. By Lemma 2.6.2, the map

$$V \to K[z]_{\leq D_{n+1}-1}, \quad f \mapsto \varphi(f)$$

is an isomorphism of K-vector spaces. Since $f_1, \dots, f_m \in V$, the assertion follows. □

The homomorphism in the proof of Theorem 3.2.2 is of exponential degree and in fact rank-preserving for the whole subspace V. The following theorem proves the existence of rank-preserving homomorphisms with more interesting parameter settings. Given polynomials $f_1, \dots, f_m \in K[\boldsymbol{x}]$ of rank at most ρ and assuming that the field K is sufficiently large, this theorem demonstrates that rank-preserving homomorphisms $\varphi\colon K[\boldsymbol{x}] \to K[\boldsymbol{z}]$ for $\{f_1, \dots, f_m\}$ exist such that $r = 1$ and φ is of degree $< \rho$, or such that $r = \rho$ and φ is graded of degree 1. The proof relies on the Alternant Criterion and uses an idea from [FS12b] based on interpolation.

Theorem 3.2.3. *Let K be an infinite field. Let $r \geq 1$ and let $f_1, \dots, f_m \in K[\boldsymbol{x}]$ be polynomials with $\operatorname{rk}_K(f_1, \dots, f_m) \leq r$.*

(a) There exists a K-algebra homomorphism $\varphi\colon K[\boldsymbol{x}] \to K[z]$ with $\deg(\varphi) < r$ which is rank-preserving for $\{f_1, \dots, f_m\}$.

(b) There exists a graded K-algebra homomorphism $\varphi\colon K[\boldsymbol{x}] \to K[\boldsymbol{z}] = K[z_1, \dots, z_r]$ of degree 1 which is rank-preserving for $\{f_1, \dots, f_m\}$.

Proof. We may assume that $f_1, \dots, f_r$ are K-linearly independent (if the rank is less than r, we can append linearly independent monomials). Since K is infinite, Lemma 3.1.2 and Theorem 2.5.4 imply that there exist $\boldsymbol{a}_1, \dots, \boldsymbol{a}_r \in K^n$ such that the matrix $\big(f_i(\boldsymbol{a}_j)\big)_{i,j} \in K^{r \times r}$ is non-singular.

To show (a), pick distinct $b_1, \dots, b_r \in K$. By interpolation, there exist univariate polynomials $g_1, \dots, g_n \in K[z]$ such that $\deg(g_k) < r$ and $g_k(b_j) = a_{j,k}$ for all $j \in [r]$ and $k \in [n]$. Define the K-algebra homomorphism

$$\varphi\colon K[\boldsymbol{x}] \to K[z], \quad x_k \mapsto g_k,$$

where $k \in [n]$. Since $\big((\varphi(f_i))(b_j)\big)_{i,j} = \big(f_i(\boldsymbol{a}_j)\big)_{i,j}$ is non-singular, the polynomials $\varphi(f_1), \dots, \varphi(f_r)$ are K-linearly independent by Lemma 3.1.2, hence φ is rank-preserving for $\{f_1, \dots, f_m\}$.

To show (b), define the K-algebra homomorphism

$$\varphi\colon K[\boldsymbol{x}] \to K[\boldsymbol{z}], \quad x_k \mapsto a_{1,k} \cdot z_1 + \cdots + a_{r,k} \cdot z_r,$$

where $k \in [n]$. Then $\big((\varphi(f_i))(\boldsymbol{e}_j)\big)_{i,j} = \big(f_i(\boldsymbol{a}_j)\big)_{i,j}$ is non-singular, where $\boldsymbol{e}_1, \ldots, \boldsymbol{e}_r \in K^r$ are the standard basis vectors of K^r. By Lemma 3.1.2, the polynomials $\varphi(f_1), \ldots, \varphi(f_r)$ are K-linearly independent, hence φ is rank-preserving for $\{f_1, \ldots, f_m\}$. □

Reducing the number of variables

Polynomial identity testing of constant-variable polynomial-degree circuits is easy by the Combinatorial Nullstellensatz. Therefore, we are interested in homomorphisms of polynomial degree that reduce the number of variables. To be useful for identity testing, those homomorphisms should preserve the non-zeroness of the circuit under consideration. Usually it is not possible to find a single map that does the job, but a family of homomorphisms where one homomorphism is guaranteed to work. We formalize this idea in the following simple theorem.

Theorem 3.2.4. *Let $n, r, d, \delta \geq 1$ and let $\mathcal{C} \subseteq K[\boldsymbol{x}]$ be a set of polynomials of degree at most δ. Let I be an index set and let $\Phi_i\colon K[\boldsymbol{x}] \to K[\boldsymbol{z}]$ be a K-algebra homomorphism of degree at most d for all $i \in I$. Denote $\Phi_i^{(j)} := \Phi_i(x_j) \in K[\boldsymbol{z}]$ for all $i \in I$ and $j \in [n]$. Let $S \subseteq K$ be a subset such that $|S| \geq \delta d + 1$.*

Assume that for all non-zero $f \in \mathcal{C}$ there exists $i \in I$ such that $\Phi_i(f) \neq 0$. Then

$$\mathcal{H} := \left\{ \big(\Phi_i^{(1)}(\boldsymbol{a}), \ldots, \Phi_i^{(n)}(\boldsymbol{a})\big) \;\middle|\; i \in I \text{ and } \boldsymbol{a} \in S^r \right\} \subseteq K^n$$

is a hitting set for $\mathcal{C}$ with $|\mathcal{H}| \leq |I| \cdot |S|^r$.

Proof. Let $f \in \mathcal{C}$ be non-zero. Then there exists $i \in I$ such that $\Phi_i(f) \neq 0$. We have $\deg(\Phi_i(f)) \leq \delta d < |S|$. By Theorem 2.5.4, there exists $\boldsymbol{a} \in S^r$ such that

$$f\big(\Phi_i^{(1)}(\boldsymbol{a}), \ldots, \Phi_i^{(n)}(\boldsymbol{a})\big) = \big(\Phi_i(f)\big)(\boldsymbol{a}) \neq 0.$$

This implies that $\mathcal{H}$ is a hitting set for $\mathcal{C}$. □

The following lemma demonstrates that a homomorphism that is rank-preserving for $\{f_1, \ldots, f_m\} \subset K[\boldsymbol{x}]$ preserves the non-zeroness of polynomials $\lambda_1 f_1 + \cdots + \lambda_m f_m$ in the K-subspace $\langle f_1, \ldots, f_m \rangle_K$.

Lemma 3.2.5. *Let $\varphi\colon K[\boldsymbol{x}] \to K[\boldsymbol{z}]$ be a K-algebra homomorphism, let $f_1, \dots, f_m \in K[\boldsymbol{x}]$ be polynomials and let $\varphi_V := \varphi|_V\colon V \to K[\boldsymbol{z}]$ be the (K-linear) restriction of φ to the K-subspace $V := \langle f_1, \dots, f_m\rangle_K \subset K[\boldsymbol{x}]$. Then φ is rank-preserving for $\{f_1, \dots, f_m\}$ if and only if φ_V is injective.*

Proof. This is clear by linear algebra. □

Let $m \geq 1$ and let $\mathcal{C} \subset K[\boldsymbol{x}]$ be a set of polynomials. Define the subset

$$\Sigma_m\mathcal{C} := \left\{ \lambda_1 f_1 + \cdots + \lambda_m f_m \;\middle|\; \begin{array}{l} \lambda_1, \dots, \lambda_m \in K, \\ f_1, \dots, f_m \in \mathcal{C} \end{array} \right\} \subseteq K[\boldsymbol{x}]$$

By Lemma 3.2.5, an efficient construction of rank-preserving homomorphisms for m-subsets of $\mathcal{C}$ yields an efficient construction for homomorphisms that preserve the non-zeroness of polynomials in $\Sigma_m\mathcal{C}$. Conversely, it is not clear how to efficiently obtain rank-preserving homomorphisms for $\mathcal{C}$ given non-zeroness preserving homomorphisms for $\Sigma_m\mathcal{C}$. In this sense, rank-preserving homomorphisms can be considered the stronger notion.

In Sections 3.2.1 to 3.2.4 we will present explicit constructions of homomorphisms preserving non-zeroness of restricted circuit classes to which Theorem 3.2.4 can be applied. Except for Section 3.2.3, we also give explicit constructions of rank-preserving homomorphisms for the corresponding classes. A summary of those results will be given in Section 3.2.5.

3.2.1 Linear Forms

We start with the construction of rank-preserving homomorphisms for sets of linear forms. Linear forms are instances of sparse polynomials which are covered in Section 3.2.2. Here we are interested in obtaining rank-preserving homomorphisms of degree 1. This is motivated, amongst other things, by Lemma 3.2.8 below. The following theorem is based on a lemma by Gabizon & Raz [GR08].

Theorem 3.2.6. *Let $1 \leq r \leq n$. For $c \in K$, define the K-algebra homomorphism*

$$\Phi_c\colon K[\boldsymbol{x}] \to K[\boldsymbol{z}], \quad x_i \mapsto \sum_{j=1}^{r} c^{(i-1)(j-1)} z_j, \tag{3.2.1}$$

where $i \in [n]$. There exists an effectively computable $N \in \mathbb{N}$ with $N = \mathrm{poly}(n)$ such that for all N-subsets $S \subseteq K$ we have the following: For all linear forms $\ell_1, \dots, \ell_m \in K[\boldsymbol{x}]_1$ with $\mathrm{rk}_K(\ell_1, \dots, \ell_m) \leq r$ there exists $c \in S$ such that Φ_c is rank-preserving for $\{\ell_1, \dots, \ell_m\}$.

Proof. The theorem is a direct consequence of Lemma 3.2.7 below. □

For the proof, we translate this theorem into the language of matrices. Let $1 \leq r \leq n$ and $m \geq 1$. Let $A \in K^{m \times n}$ be a matrix with $\mathrm{rk}_K(A) \leq r$. We say that a matrix $B \in K^{n \times r}$ is **rank-preserving** for A if $\mathrm{rk}_K(AB) = \mathrm{rk}_K(A)$. If $\ell_1, \ldots, \ell_m \in K[\boldsymbol{x}]_1$ are given by the rows of A and if $\varphi\colon K[\boldsymbol{x}] \to K[\boldsymbol{z}]$ is given by $x_i \mapsto \sum_{j=1}^{r} b_{i,j} \cdot z_j$ for $i \in [n]$, then $B = \big(b_{i,j}\big)$ is rank-preserving for A if and only if φ is rank-preserving for $\{\ell_1, \ldots, \ell_m\}$.

A construction of rank-preserving matrices inspired by Vandermonde matrices was given in [GR08, Lemma 6.1]. We present this lemma here with a proof similar to that of Theorem 4.1 in the full version of [FS12a]. In Lemma 4.2.13 we will propose another construction for rank-preserving matrices.

Lemma 3.2.7. *Let $1 \leq r \leq n$ and $m \geq 1$. Let $A \in K^{m \times n}$ be a matrix with $\mathrm{rk}_K(A) \leq r$. For $c \in K$, define $V_c := \big(c^{(i-1)(j-1)}\big)_{i,j} \in K^{n \times r}$. Then there exists a set $B \subseteq K$ with $|B| \leq \binom{r}{2}(n-1)$ such that*

$$\mathrm{rk}_K(AV_c) = \mathrm{rk}_K(A)$$

for all $c \in K \setminus B$.

Proof. Let t be a variable and define $V := \big(t^{(i-1)(j-1)}\big)_{i,j} \in K[t]^{n \times r}$. By removing rows of A and columns of V (from the right), we may assume $m = r = \mathrm{rk}_K(A)$. Then it suffices to show that $f := \det(AV) \in K[t]$ is a non-zero polynomial with $\deg(f) \leq \binom{r}{2}(n-1)$. By the Cauchy–Binet Formula (see Lemma A.3.2), we have

$$f = \sum_{I \in \mathcal{I}} \det(A_{[r],I}) \cdot \det(V_{I,[r]}),$$

where $\mathcal{I} := \big\{ I \in \binom{[n]}{r} \mid \det(A_{[r],I}) \neq 0 \big\}$. Since $\mathrm{rk}_K(A) = r$, the set $\mathcal{I}$ is non-empty. Therefore, it suffices to show that

(a) the polynomial $f_I := \det(V_{I,[r]}) \in K[t]$ is non-zero and $\deg(f_I) \leq \binom{r}{2}(n-1)$ for all $I \in \binom{[n]}{r}$, and

(b) there exists $I \in \mathcal{I}$ such that $\deg(f_I) > \deg(f_J)$ for all $J \in \mathcal{I} \setminus \{I\}$.

To show (a), let $I = \{i_1 < \cdots < i_r\} \in \binom{[n]}{r}$. We have $f_I = \sum_{\sigma \in \mathfrak{S}_r} \mathrm{sgn}(\sigma) \cdot t^{d_{\sigma,I}}$, where $d_{\sigma,I} := (i_1 - 1)(\sigma(1) - 1) + \cdots + (i_r - 1)(\sigma(r) - 1) \in \mathbb{N}$. It is not hard to show that $d_{\mathrm{id},I} > d_{\sigma,I}$ for all $\sigma \in \mathfrak{S}_r \setminus \{\mathrm{id}\}$, hence $f_I \neq 0$ and $\deg(f_I) = d_{\mathrm{id},I} \leq \binom{r}{2}(n-1)$.

To show (b), let $I \in \mathcal{I}$ such that $\deg(f_I) \geq \deg(f_J)$ for all $J \in \mathcal{I}$. Assume for the sake of contradiction that there exists $J \in \mathcal{I} \setminus \{I\}$ such that

$\deg(f_I) = \deg(f_J)$. Let $i \in (I \setminus J) \cup (J \setminus I)$ be minimal. We may assume $i \in I$. Then, by the Steinitz Exchange Lemma, there exists $j \in J \setminus I$ such that $I' := (I \setminus \{i\}) \cup \{j\} \in \mathcal{I}$. Since $j > i$, we obtain $\deg(f_{I'}) = d_{\mathrm{id},I'} > d_{\mathrm{id},I} = \deg(f_I)$, a contradiction. □

To conclude this section, we would like to point out that a graded homomorphism $\varphi\colon K[\boldsymbol{x}] \to K[\boldsymbol{z}]$ of degree 1, such as (3.2.1), which is rank-preserving for $\{\ell_1, \ldots, \ell_m\} \subseteq K[\boldsymbol{x}]_1$ is not only injective on the K-subspace $\langle \ell_1, \ldots, \ell_m \rangle_K$, but also on the K-subalgebra $K[\ell_1, \ldots, \ell_m]$. Homomorphisms that are injective on subalgebras $K[f_1, \ldots, f_m]$ for arbitrary polynomials $f_1, \ldots, f_m \in K[\boldsymbol{x}]$ will be the subject of Section 4.2.

Lemma 3.2.8. *Let $\ell_1, \ldots, \ell_m \in K[\boldsymbol{x}]_1$ be linear forms, let $\varphi\colon K[\boldsymbol{x}] \to K[\boldsymbol{z}] = K[z_1, \ldots, z_r]$ be a graded K-algebra homomorhism of degree 1, and let $\varphi|_{K[\ell_1,\ldots,\ell_m]}$ be the restriction of φ to the K-subalgebra $K[\ell_1, \ldots, \ell_m]$.*

If φ is rank-preserving for $\{\ell_1, \ldots, \ell_m\}$, then $\varphi|_{K[\ell_1,\ldots,\ell_m]}$ is injective. If, in addition, $\mathrm{rk}_K(\ell_1, \ldots, \ell_m) = r$, then $\varphi|_{K[\ell_1,\ldots,\ell_m]}$ is bijective.

Proof. We may assume that $\ell_1, \ldots, \ell_m$ are K-linearly independent. Let φ be rank-preserving for $\{\ell_1, \ldots, \ell_m\}$. Since $\varphi(\ell_i) \in K[\boldsymbol{z}]_1$ for all $i \in [m]$, we have $m \leq r$. After an invertible linear change of the $\boldsymbol{z}$-variables, we may assume that $\varphi(\ell_i) = z_i$ for all $i \in [m]$. Now let $F \in K[y_1, \ldots, y_m]$ be a polynomial such that $\varphi(F(\ell_1, \ldots, \ell_m)) = 0$. This implies $0 = \varphi(F(\ell_1, \ldots, \ell_m)) = F(\varphi(\ell_1), \ldots, \varphi(\ell_m)) = F(z_1, \ldots, z_m)$, thus $F = 0$. This demonstrates that $\varphi|_{K[\ell_1,\ldots,\ell_m]}$ is injective. If $\mathrm{rk}_K(\ell_1, \ldots, \ell_m) = r$, then $\varphi(K[\ell_1, \ldots, \ell_m]) = K[\boldsymbol{z}]$, hence $\varphi|_{K[\ell_1,\ldots,\ell_m]}$ is bijective. □

3.2.2 Sparse Polynomials

It was so sparse out there
they didn't get close enough to each other
to collide and form a planet.
(Andrew Puckett)

In this section we present PIT algorithms and rank-preserving homomorphisms for sparse polynomials. Blackbox identity testing and blackbox interpolation of sparse polynomials have received a lot of attention in the literature [GK87, BT88, Zip90, GKS90, CDGK91, KS01, AHT07, BHLV09, BE11].

Identity testing of sparse polynomials

We use the sparse PIT algorithm that appeared in [Agr05, BHLV09] and stands out due to its simplicity. The main idea of the algorithm is to make

the sparse polynomial univariate by a Kronecker substitution and then apply Agrawal's paradigm in order to reduce the high degree (see Section 2.6). The following lemma (cf. [BHLV09, Lemma 13]) makes Agrawal's paradigm work for sparse polynomials. It bounds the number of primes q for which a non-zero polynomial $f \in K[z]$ vanishes modulo $\langle z^q - 1 \rangle$.

Lemma 3.2.9. *Let R be a ring, let $d, s \geq 1$, and let $f \in R[z]$ be a non-zero polynomial of sparsity at most s and degree at most d. Then*

$$\#\big\{q \in \mathbb{P} \mid f \in \langle z^q - 1 \rangle_{R[z]}\big\} \leq (s-1)\lfloor \log_2 d \rfloor.$$

Proof. Let $S := \mathrm{LSupp}(f) \subseteq [0, d]$ be the logarithmic support of f and let $i \in S$ be minimal. Assume that $q \in \mathbb{P}$ is a prime such that $f \in \langle z^q - 1 \rangle$. Then $|S| \geq 2$ and there exists $j \in S \setminus \{i\}$ such that $q \mid (j - i)$. Since $j - i$ has at most $\lfloor \log_2(j-i) \rfloor \leq \lfloor \log_2 d \rfloor$ prime divisors, we conclude

$$\#\big\{q \in \mathbb{P} \mid f \in \langle z^q - 1 \rangle\big\} \leq (|S| - 1)\lfloor \log_2 d \rfloor \leq (s-1)\lfloor \log_2 d \rfloor,$$

as required. □

Let $D \geq 1$ and let $q \geq 1$. For $a \in \mathbb{Z}$, we denote by $\lfloor a \rfloor_q$ the integer $b \in \mathbb{Z}$ satisfying $0 \leq b < q$ and $a = b \pmod q$. Define the K-algebra homomorphisms

$$\begin{aligned} \Phi_D &\colon K[\boldsymbol{x}] \to K[z], \quad x_i \mapsto z^{D^{i-1}}, \\ \Phi_{D,q} &\colon K[\boldsymbol{x}] \to K[z], \quad x_i \mapsto z^{\lfloor D^{i-1} \rfloor_q}, \end{aligned} \tag{3.2.2}$$

where $i \in [n]$. We have $\Phi_D(f) = \Phi_{D,q}(f) \pmod{\langle z^q - 1 \rangle_{K[z]}}$ for all $f \in K[\boldsymbol{x}]$. For almost all $D \geq 1$ and $q \in \mathbb{P}$ the homomorphism $\Phi_{D,q}$ preserves the non-zeroness of a given polynomial. The following lemma bounds the number of bad primes q. Note that the homomorphism $\Phi_{D,q}$ is toric, hence it is sparsity-preserving as well.

Lemma 3.2.10. *Let $\delta, s \geq 1$ and let $D \geq \delta + 1$. For $q \geq 1$, let $\Phi_{D,q} \colon K[\boldsymbol{x}] \to K[z]$ be defined as in (3.2.2). Let $f \in K[\boldsymbol{x}]$ be a non-zero polynomial of sparsity at most s and degree at most δ.*

Then there exists a set $B \subset \mathbb{P}$ of primes with $|B| \leq (s-1)\lfloor n \log_2 D \rfloor$ such that $\Phi_{D,q}(f) \neq 0$ for all $q \in \mathbb{P} \setminus B$.

Proof. By Lemma 2.6.2, the polynomial $g := \Phi_D(f) \in K[z]$ satisfies $g \neq 0$, $\mathrm{sp}(g) = \mathrm{sp}(f) \leq s$ and $\deg(g) \leq D^n - 1$. By Lemma 3.2.9, there exists a set $B \subset \mathbb{P}$ with $|B| \leq (s-1)\lfloor \log_2(D^n - 1) \rfloor \leq (s-1)\lfloor n \log_2 D \rfloor$ such that $g \notin \langle z^q - 1 \rangle_{K[z]}$ for all $q \in \mathbb{P} \setminus B$. Since $g - \Phi_{D,q}(f) \in \langle z^q - 1 \rangle_{K[z]}$, we obtain $\Phi_{D,q}(f) \neq 0$ for all $q \in \mathbb{P} \setminus B$. □

By Corollary A.1.2 (b), we will hit a good prime q for a given non-zero polynomial by trying every integer in an interval of polynomial size. Thus we obtain the following theorem.

Theorem 3.2.11. *Let $\delta, s \geq 1$. Set $D := \delta + 1$. For $q \geq 1$, let $\Phi_{D,q} \colon K[\boldsymbol{x}] \to K[z]$ be defined as in (3.2.2).*

There exists an effectively computable $N \in \mathbb{N}$ with $N = \operatorname{poly}(n, s, \log \delta)$ such that we have the following: For every non-zero polynomial $f \in K[\boldsymbol{x}]$ of sparsity at most s and degree at most δ, there exists $q \in [N]$ such that $\Phi_{D,q}(f) \neq 0$.

Proof. Using Corollary A.1.2 (b), the assertion follows from Lemma 3.2.10. □

Preserving the rank of sparse polynomials

Preserving the rank of sparse polynomials $f_1, \ldots, f_m \in K[\boldsymbol{x}]$ works similar to the PIT algorithm. Here it suffices to find $D, q \geq 1$ such that $\Phi_{D,q}$ sends the terms in the supports of $f_1, \ldots, f_m$ to different terms.

Theorem 3.2.12. *Let $\delta, m, r, s \geq 1$. Set $D := \delta + 1$. For $q \geq 1$, define $\Phi_{D,q} \colon K[\boldsymbol{x}] \to K[z]$ as in (3.2.2).*

There exists an effectively computable $N \in \mathbb{N}$ with $N = \operatorname{poly}(n, r, s, \log \delta)$ such that we have the following: For all polynomials $f_1, \ldots, f_m \in K[\boldsymbol{x}]$ of sparsity at most s, degree at most δ, and $\operatorname{rk}_K(f_1, \ldots, f_m) \leq r$, there exists $q \in [N]$ such that $\Phi_{D,q}$ is rank-preserving for $\{f_1, \ldots, f_m\}$.

Proof. Using Corollary A.1.2 (b), the assertion follows from Lemma 3.2.13 below. □

The following lemma constitutes the proof of Theorem 3.2.12. It demonstrates that, for almost all $D \geq 1$ and $q \in \mathbb{P}$, the homomorphism $\Phi_{D,q}$ is rank-preserving for a given set of polynomials, and it bounds the number of bad primes q.

Lemma 3.2.13. *Let $\delta, r, s \geq 1$ and let $D \geq \delta + 1$. For $q \geq 1$, define $\Phi_{D,q} \colon K[\boldsymbol{x}] \to K[z]$ as in (3.2.2). Let $f_1, \ldots, f_m \in K[\boldsymbol{x}]$ be polynomials of sparsity at most s, degree at most δ, and $\operatorname{rk}_K(f_1, \ldots, f_m) \leq r$.*

Then there exists a set $B \subset \mathbb{P}$ of primes with $|B| \leq \binom{rs}{2} \lfloor n \log_2 D \rfloor$ such that $\Phi_{D,q}$ is rank-preserving for $\{f_1, \ldots, f_m\}$ for all $q \in \mathbb{P} \setminus B$.

Proof. Assume that $f_1, \ldots, f_r$ are K-linearly independent (if the rank is less than r, we can append linearly independent monomials). Let $S := \operatorname{Supp}(f_1) \cup \cdots \cup \operatorname{Supp}(f_r) \subset \mathbb{T}(\boldsymbol{x})$. Then S is a K-basis of $V := \langle S \rangle_K \subset K[\boldsymbol{x}]$, and we

have $|S| \leq rs$. By Lemma 3.2.10, there exists a set $B \subset \mathbb{P}$ with $|B| \leq \binom{rs}{2} \lfloor n \log_2 D \rfloor$ such that $\Phi_{D,q}(t) \neq \Phi_{D,q}(t')$ for all $\{t, t'\} \in \binom{S}{2}$ and all $q \in \mathbb{P} \setminus B$. Let $q \in \mathbb{P} \setminus B$. Then the K-linear map $V \to K[z]$, $f \mapsto \Phi_{D,q}(f)$ is injective. Since $f_1, \ldots, f_m \in V$, this means that $\Phi_{D,q}$ is rank-preserving for $\{f_1, \ldots, f_m\}$. □

The next theorem shows how rank-preserving homomorphisms of low degree according to Theorem 3.2.3 can be found for sparse polynomials. The construction is a combination of Theorems 3.2.6 and 3.2.12, and uses additional ideas of [FS12b].

Theorem 3.2.14. *Let $\delta, m, r, s \geq 1$. Set $D := \delta + 1$. Let $a_1, \ldots, a_r \in K$ be distinct and let $g_1, \ldots, g_r \in K[z]$ such that $\deg(g_i) = r - 1$ and $g_i(a_j) = \delta_{i,j}$ for all $i, j \in [r]$. For $q \geq 1$ and $c \in K$, define the K-algebra homomorphisms*

$$\Phi_{D,q,c} \colon K[\boldsymbol{x}] \to K[z], \quad x_i \mapsto \sum_{j=1}^{r} c^{\lfloor D^{i-1} \rfloor_q \cdot (j-1)} \cdot g_j, \tag{3.2.3}$$

where $i \in [n]$, and

$$\Psi_{D,q,c} \colon K[\boldsymbol{x}] \to K[\boldsymbol{z}], \quad x_i \mapsto \sum_{j=1}^{r} c^{\lfloor D^{i-1} \rfloor_q \cdot (j-1)} \cdot z_j, \tag{3.2.4}$$

where $i \in [n]$ and $\boldsymbol{z} = \{z_1, \ldots, z_r\}$.

There exists an effectively computable $N \in \mathbb{N}$ with $N = \operatorname{poly}(n, r, s, \delta)$ such that for all N-subsets $S \subseteq K$ we have the following: For all polynomials $f_1, \ldots, f_m \in K[\boldsymbol{x}]$ of sparsity at most s, degree at most δ, and $\operatorname{rk}_K(f_1, \ldots, f_m) \leq r$, there exist $q \in [N]$ and $c \in S$ such that both $\Phi_{D,q,c}$ and $\Psi_{D,q,c}$ are rank-preserving for $\{f_1, \ldots, f_m\}$.

Proof. Using Corollary A.1.2 (b), the assertion follows from Lemma 3.2.15 below. □

The following lemma constitutes the proof of Theorem 3.2.14. The main idea of the proof is as follows. By the Alternant Criterion and the proof of Theorem 3.2.3, it suffices to find points $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_r \in K^n$ such that $\big(f_i(\boldsymbol{b}_j)\big)_{i,j} \in K^{r \times r}$ is non-singular. Indeed, then we can interpolate those points by low degree polynomials (this idea was used in [FS12b]; cf. the proof of Theorem 3.2.3). In order to obtain the points $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_r$, we first apply the rank-preserving homomorphism (3.2.2) to $f_1, \ldots, f_r$ to make them univariate polynomials $h_1, \ldots, h_r \in K[z]$ of moderate degree $< d$. Subsequently, we evaluate those univariate polynomials at the powers $c^0, c^1, \ldots, c^{r-1}$ of an element $c \in K$. In [FS12b] it was observed that the matrix $\big(h_i(c^{j-1})\big)_{i,j} \in K^{r \times r}$

equals $A \cdot V_c$, where $A \in K^{r \times d}$ contains the coefficients of $h_1, \ldots, h_r$ and $V_c \in K^{d \times r}$ is the Vandermonde matrix from Lemma 3.2.7. Since V_c is rank-preserving for A for almost all $c \in K$, we obtain points $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_r$ with the desired properties.

Lemma 3.2.15. *Let $\delta, r, s \geq 1$ and let $D \geq \delta + 1$. Let $a_1, \ldots, a_r \in K$ be distinct and let $g_1, \ldots, g_r \in K[z]$ such that $\deg(g_i) = r - 1$ and $g_i(a_j) = \delta_{i,j}$ for all $i, j \in [r]$. For $q \geq 1$ and $c \in K$, define $\Phi_{D,q,c} \colon K[\boldsymbol{x}] \to K[z]$ and $\Psi_{D,q,c} \colon K[\boldsymbol{x}] \to K[\boldsymbol{z}]$ as in (3.2.3) and (3.2.4). Let $f_1, \ldots, f_m \in K[\boldsymbol{x}]$ be polynomials of sparsity at most s, degree at most δ, and $\mathrm{rk}_K(f_1, \ldots, f_m) \leq r$.*

Then there exists a set $B_1 \subset \mathbb{P}$ of primes with $|B_1| \leq \binom{rs}{2} \lfloor n \log_2 D \rfloor$ satisfying the following property: For all $q \in \mathbb{P} \setminus B_1$ there exists a set $B_2 \subseteq K$ with $|B_2| < q\delta\binom{r}{2}$ such that both $\Phi_{D,q,c}$ and $\Psi_{D,q,c}$ are rank-preserving for $\{f_1, \ldots, f_m\}$ for all $c \in K \setminus B_2$.

Proof. Assume that $f_1, \ldots, f_r$ are K-linearly independent (if the rank is less than r, we can append linearly independent monomials). By Lemma 3.2.13, there exists $B_1 \subset \mathbb{P}$ with $|B_1| \leq \binom{rs}{2} \lfloor n \log_2 D \rfloor$ such that the polynomials

$$h_{i,q} := f_i\big(t^{\lfloor D^0 \rfloor_q}, t^{\lfloor D^1 \rfloor_q}, \ldots, t^{\lfloor D^{n-1} \rfloor_q}\big) \in K[t], \quad i \in [r],$$

are K-linearly independent for all $q \in \mathbb{P} \setminus B_1$. Now fix $q \in \mathbb{P} \setminus B_1$. We have $\deg_t(h_{i,q}) < q\delta =: d$ for all $i \in [r]$. Let $A = \big(a_{i,j}\big)_{i,j} \in K^{r \times d}$, where $a_{i,j}$ is the coefficient of t^{j-1} in $h_{i,q}$ for all $i \in [r]$ and $j \in [d]$. Since $g_{1,q}, \ldots, g_{r,q}$ are K-linearly independent, we have $\mathrm{rk}_K(A) = r$. By Lemma 3.2.7, there exists $B_2 \subseteq K$ with $|B_2| < q\delta\binom{r}{2}$ such that $\det(AV_c) \neq 0$ for all $c \in K \setminus B_2$, where $V_c := \big(c^{(i-1)(j-1)}\big)_{i,j} \in K^{d \times r}$. Fix an element $c \in K \setminus B_2$. We have

$$\big((\Phi_{D,q,c}(f_i))(a_j)\big)_{1 \leq i,j \leq r} = \big((\Psi_{D,q,c}(f_i))(\boldsymbol{e}_j)\big)_{i,j} = \big(h_{i,q}(c^{j-1})\big)_{i,j} = AV_c,$$

where $\boldsymbol{e}_1, \ldots, \boldsymbol{e}_r \in K^r$ are the standard basis vectors of K^r. Since AV_c is non-singular, Lemma 3.1.2 implies that both $\Phi_{D,q,c}(f_1), \ldots, \Phi_{D,q,c}(f_r)$ and $\Psi_{D,q,c}(f_1), \ldots, \Psi_{D,q,c}(f_r)$ are K-linearly independent. Therefore, both $\Phi_{D,q,c}$ and $\Psi_{D,q,c}$ are rank-preserving for $\{f_1, \ldots, f_m\}$. □

3.2.3 Polynomials with Sparse Newton Polytope Decomposition

It is the weight, not numbers
of experiments that is to be regarded.
(Isaac Newton)

In this section, we generalize the identity test for sparse polynomials from Section 3.2.2 to polynomials whose Newton polytopes admits a certain sparse decomposition.

We start with a few definitions about convex polytopes. For more information on polytopes, we refer to the standard monographs [Grü03, Zie95]. A subset $P \subset \mathbb{R}^n$ is called **polytope** if it is the convex hull of a finite set of points, i. e. $P = \mathrm{Conv}(\alpha_1, \ldots, \alpha_m)$ for some $\alpha_1, \ldots, \alpha_m \in \mathbb{R}^n$. A point $\alpha \in P$ is a **vertex** of P, if $\alpha \notin \mathrm{Conv}(P \setminus \{\alpha\})$. The set of all vertices of P is denoted by $\mathrm{Vert}(P) \subset \mathbb{R}^n$. It is the unique minimal subset of $\mathbb{R}^n$ with convex hull P. We call the number $\mathrm{sp}(P) := \#\,\mathrm{Vert}(P) \in \mathbb{N}$ the **sparsity** of P. If $\mathrm{Vert}(P) \subset \mathbb{Z}^n$, then P is called **integral**. We are interested in the integral polytope that is spanned by the exponent vectors in the support of a polynomial.

Definition 3.2.16. Let $f \in K[\boldsymbol{x}]$ be a polynomial. The set

$$\mathrm{New}(f) := \mathrm{Conv}(\mathrm{LSupp}(f)) \subset \mathbb{R}^n_{\geq 0}$$

is called the **Newton polytope** of f.

By definition, we have $\mathrm{sp}(\mathrm{New}(f)) \leq \mathrm{sp}(f)$ for all $f \in K[\boldsymbol{x}]$. The following example demonstrates that the sparsity of a polynomial can be exponentially larger than the sparsity of its Newton polytope.

Example 3.2.17. Let $\delta \geq 1$, let K be a field with $\mathrm{char}(K) = 0$ or $\mathrm{char}(K) > \delta$, and consider the polynomial $f = (x_1 + \cdots + x_n + 1)^\delta \in K[\boldsymbol{x}]$. Then we have $\mathrm{Supp}(f) = \mathbb{T}(\boldsymbol{x})_{\leq \delta}$, hence $\mathrm{New}(f)$ is an n-dimensional simplex with vertices $\{\mathbf{0}, \delta\varepsilon_1, \ldots, \delta\varepsilon_n\}$, where $\varepsilon_i \in \mathbb{R}^n$ is the i-th standard basis vector for $i \in [n]$. Therefore, we have $\mathrm{sp}(\mathrm{New}(f)) = n + 1$ and $\mathrm{sp}(f) = \binom{n+\delta}{\delta} > (n/\delta)^\delta$.

Ostrowski [Ost75] observed that a factorization of a polynomial implies a decomposition of its Newton polytope as Minkowski sum. Recall that the **Minkowski sum** of subsets $P_1, \ldots, P_m \subseteq \mathbb{R}^n$ is defined as $P_1 + \cdots + P_m := \{\alpha_1 + \cdots + \alpha_m \mid \alpha_i \in P_i \text{ for } i \in [m]\} \subseteq \mathbb{R}^n$. If $P_1, \ldots, P_m$ are polytopes, then their Minkowski sum is again a polytope.

Lemma 3.2.18 ([Ost75, Theorem VI])**.** *Let $f, g \in K[\boldsymbol{x}]$ be polynomials. Then we have* $\mathrm{New}(f \cdot g) = \mathrm{New}(f) + \mathrm{New}(g)$.

Motivated by this lemma, we will consider polynomials whose Newton polytopes decompose into few sparse integral polytopes.

Definition 3.2.19. Let $\mathrm{New}_{s,\delta}$ be the set of all polynomials $f \in K[\boldsymbol{x}]$ of degree at most δ such that $\mathrm{New}(f) = P_1 + \cdots + P_m$ for some integral polytopes $P_1, \ldots, P_m \subset \mathbb{R}^n_{\geq 0}$ with $\sum_{i=1}^m |\mathrm{Vert}(P_i)| \leq s$.

The Newton polytope in the following example has exponential sparsity, but admits a sparse decomposition.

Example 3.2.20. Let K be an arbitrary field and consider the polynomial $f = (x_1 + 1) \cdots (x_n + 1) \in K[\boldsymbol{x}]$. Then $\mathrm{LSupp}(f) = \{0,1\}^n$, hence $\mathrm{New}(f)$ is an n-dimensional hypercube with vertices $\{0,1\}^n$. Therefore, we have $\mathrm{sp}(\mathrm{New}(f)) = \mathrm{sp}(f) = 2^n$. On the other hand, Lemma 3.2.18 implies $\mathrm{New}(f) = \mathrm{Conv}(\mathbf{0}, \varepsilon_1) + \cdots + \mathrm{Conv}(\mathbf{0}, \varepsilon_n)$, thus we have $f \in \mathrm{New}_{2n,n}$.

Now we can state the main result of this section. Note that this is a generalization of Theorem 3.2.11.

Theorem 3.2.21. *Let $\delta, s \geq 1$. Set $D := \delta + 1$. For $q \geq 1$, let $\Phi_{D,q} \colon K[\boldsymbol{x}] \to K[z]$ be defined as in* (3.2.2).

There exists an effectively computable $N \in \mathbb{N}$ with $N = \mathrm{poly}(n, s, \log \delta)$ such that we have the following: For every non-zero $f \in \mathrm{New}_{s,\delta} \cap K[\boldsymbol{x}]$ there exists $q \in [N]$ such that $\Phi_{D,q}(f) \neq 0$.

Proof. Using Corollary A.1.2 (b), the assertion follows from Lemma 3.2.24 below. □

In the proof we use the theme of isolating terms which was introduced in Section 2.6. We first observe that, in order to obtain an isolating weight vector (recall Definition 2.6.6) for a polytope, it suffices to isolate one of its vertices.

Lemma 3.2.22. *Let $P \subset \mathbb{R}^n_{\geq 0}$ be a polytope and let $w \in \mathbb{N}^n$ be a weight vector. Then the following statements are equivalent:*

(a) The weight vector w is isolating for P.

(b) Some $\alpha \in \mathrm{Vert}(P)$ is isolated by w in P.

(c) The weight vector w is isolating for $\mathrm{Vert}(P)$.

Proof. Denote $\mathrm{Vert}(P) = \{\alpha_1, \ldots, \alpha_m\}$. First we assume (a). Then some $\alpha \in P$ is isolated by w in P. Write $\alpha = \sum_{i=1}^m \lambda_i \alpha_i$ for some $\lambda_1, \ldots, \lambda_m \in \mathbb{R}_{\geq 0}$ with $\sum_{i=1}^m \lambda_i = 1$. We have

$$|\alpha|_w = \sum_{i=1}^m \lambda_i \cdot |\alpha_i|_w \geq \Big(\min_{1 \leq i \leq m} |\alpha_i|_w \Big) \cdot \sum_{i=1}^m \lambda_i = \min_{1 \leq i \leq m} |\alpha_i|_w.$$

Since w isolates α in P, we get $\alpha = \alpha_j$ for some $j \in [m]$, so we have shown (b). Part (b) contains (c) as a special case. Finally, assume (c). Then there exists $j \in [m]$ such that w isolates α_j in $\mathrm{Vert}(P)$. Let $\beta \in P \setminus \{\alpha_j\}$. Write

$\beta = \sum_{i=1}^{m} \lambda_i \alpha_i$ for some $\lambda_1, \ldots, \lambda_m \in \mathbb{R}_{\geq 0}$ with $\sum_{i=1}^{m} \lambda_i = 1$. We have $\lambda_j < 1$, hence $\lambda_i > 0$ for some $i \neq j$, so we obtain

$$|\alpha_j|_w = \sum_{i=1}^{m} \lambda_i \cdot |\alpha_j|_w < \sum_{i=1}^{m} \lambda_i \cdot |\alpha_i|_w = |\beta|_w.$$

This shows (a). □

The following lemma demonstrates that a weight vector is isolating for a Minkowski sum of polytopes if and only if it is isolating for every summand.

Lemma 3.2.23. *Let $P_1, \ldots, P_m \subset \mathbb{R}^n_{\geq 0}$ be polytopes and let $w \in \mathbb{N}^n$ be a weight vector. Then w is isolating for $P_1 + \cdots + P_m$ if and only if w is isolating for P_i for all $i \in [m]$.*

Proof. Denote $P := P_1 + \cdots + P_m$. Assume that w is isolating for P. Then some $\alpha \in P$ is isolated by w in P. Write $\alpha = \alpha_1 + \cdots + \alpha_m$ with $\alpha_i \in P_i$ for $i \in [m]$. Now let $i \in [m]$. We want to show that w isolates α_i in P_i. To this end, let $\beta_i \in P_i \setminus \{\alpha_i\}$ and consider $\beta := \alpha - \alpha_i + \beta_i \in P \setminus \{\alpha\}$. Since w isolates α in P, we obtain $|\alpha|_w < |\beta|_w = |\alpha|_w - |\alpha_i|_w + |\beta_i|_w$, hence $|\alpha_i|_w < |\beta_i|_w$. This shows that w is isolating for P_i for all $i \in [m]$.

Conversely, assume that w is isolating for P_i for all $i \in [m]$. Then some $\alpha_i \in P_i$ is isolated by w in P_i for all $i \in [m]$. We want to show that $\alpha := \alpha_1 + \cdots + \alpha_m \in P$ is isolated by w in P. To this end, let $\beta \in P \setminus \{\alpha\}$. Write $\beta = \beta_1 + \cdots + \beta_m$ with $\beta_i \in P_i$ for $i \in [m]$. We have $|\alpha_i|_w \leq |\beta_i|_w$ for all $i \in [m]$. Since $\alpha \neq \beta$, there exits $j \in [m]$ such that $\alpha_j \neq \beta_j$, hence $|\alpha_j|_w < |\beta_j|$. This yields

$$|\alpha|_w = \sum_{i=1}^{m} |\alpha_i|_w < \sum_{i=1}^{m} |\beta_i|_w = |\beta|_w,$$

showing that w isolates α in P. □

The following lemma constitutes the proof of Theorem 3.2.21. It gives a bound on the number of primes $q \in \mathbb{P}$ for which the homomorphism $\Phi_{D,q}$ does not preserve the non-zeroness of a polynomial whose Newton polytope has a sparse decomposition. In view of Lemmas 3.2.22 and 3.2.23, it suffices to isolate the terms corresponding to the vertices of the decomposition from each other.

Lemma 3.2.24. *Let $\delta \geq 1$ and let $D \geq \delta + 1$. For $q \geq 1$, let $\Phi_{D,q} \colon K[\boldsymbol{x}] \to K[z]$ be defined as in (3.2.2). Let $f \in K[\boldsymbol{x}]$ be a non-zero polynomial of*

degree at most δ such that $\mathrm{New}(f) = P_1 + \cdots + P_m$ *for some integral polytopes* $P_1, \ldots, P_m \subset \mathbb{R}^n_{\geq 0}$ *with* $|\mathrm{Vert}(P_i)| \leq s$ *for all* $i \in [m]$.

Then there exists a set $B \subset \mathbb{P}$ *of primes with* $|B| \leq m\binom{s}{2}\lfloor n \log_2 D \rfloor$ *such that* $\Phi_{D,q}(f) \neq 0$ *for all* $q \in \mathbb{P} \setminus B$.

Proof. Denote $V_i := \mathrm{Vert}(P_i) \subset \mathbb{N}^n$ for all $i \in [m]$. For $q \geq 1$, define the weight vector

$$w_q := \left(\lfloor D^0 \rfloor_q, \lfloor D^1 \rfloor_q, \ldots, \lfloor D^{n-1} \rfloor_q\right) \in \mathbb{N}^n.$$

Now let $i \in [m]$ and let $\{\alpha, \beta\} \in \binom{V_i}{2}$. By Lemma 3.2.10, there exists a set $B_{i,\{\alpha,\beta\}} \subset \mathbb{P}$ of primes with $|B_{i,\{\alpha,\beta\}}| \leq \lfloor n \log_2 D \rfloor$ such that $\Phi_{D,q}(\boldsymbol{x}^\alpha) \neq \Phi_{D,q}(\boldsymbol{x}^\beta)$ for all $q \in \mathbb{P} \setminus B_{i,\{\alpha,\beta\}}$. This implies $|\alpha|_{w_q} \neq |\beta|_{w_q}$ for all $q \in \mathbb{P} \setminus B_{i,\{\alpha,\beta\}}$. Now set

$$B := \bigcup_{i=1}^{m} \bigcup_{\{\alpha,\beta\} \in \binom{V_i}{2}} B_{i,\{\alpha,\beta\}} \subset \mathbb{P}$$

and let $q \in \mathbb{P} \setminus B$. Then w_q is isolating for V_i for all $i \in [m]$. By Lemma 3.2.22, this implies that w_q is isolating for P_i for all $i \in [m]$. Therefore, by Lemma 3.2.23, w_q is isolating for $\mathrm{New}(f)$. We conclude that $\Phi_{D,q}(f) \neq 0$. □

3.2.4 Products of Linear Forms

Knowing + and × is good enough,
understanding their interaction is ideal.
(Bruno Buchberger)

In this section we give a construction of rank-preserving homomorphisms for sets of products of linear forms. A related topic are PIT algorithms for ΣΠΣ-circuits which are sums of products of linear forms.

Definition 3.2.25. Let $n, k, \delta \geq 1$ and consider the arithmetic circuit

$$C = \sum_{i=1}^{k} \prod_{j=1}^{\delta} \ell_{i,j}, \tag{3.2.5}$$

where $\ell_{i,j} \in K[\boldsymbol{x}]_1 \setminus \{0\}$ are linear forms (in sparse Σ-representation). The parameter k is called the **top fan-in** of C. For $i \in [k]$, the product $T_i := \prod_{j=1}^{\delta} \ell_{i,j}$ is called a **multiplication term** of C. The set of all circuits as in (3.2.5) is denoted by $\Sigma_k\Pi_\delta\Sigma$.

This class of circuits has been subject to a long line of research. For ΣΠΣ-circuits with constant top fan-in, polynomial-time algorithms are known. The first non-blackbox polynomial-time algorithm was given by Kayal & Saxena [KS07] (see also [AM10] for a different formulation of this algorithm).

The quest for blackbox algorithms was initiated by Karnin & Shpilka [KS11a] who turned the quasipolynomial-time algorithm of Dvir & Shpilka [DS07] into a hitting set. Their rank-based construction was gradually improved in the works [SS11a, KS09, SS10], so that polynomial-time blackbox algorithms could be obtained over ordered fields such as $\mathbb{Q}$. We will address this approach in Section 4.2.5, where we generalize it to ΣΠΣΠ-circuits with constant top and bottom fan-in.

Saxena & Seshadhri [SS11b] finally found a field-independent polynomial-time blackbox identity test for ΣΠΣ-circuits with constant top fan-in. Their algorithm can be interpreted as a blackbox version of [KS07], but uses also tools developed in [KS11a, SS10]. We will present these methods here and show how they can be used to obtain rank-preserving homomorphisms for products of linear forms.

Ideal decomposition

The results of this section are based on decompositions of ideals generated by products of linear forms. This method was used in [SS10] (see the full version of the paper for details). Let $S \subset K[\boldsymbol{x}]$ be a set of products of linear forms. We define the K-subspace

$$\mathrm{Lin}_K(S) := \big\langle \ell \in K[\boldsymbol{x}]_1 \mid \ell \text{ divides some } f \in S \big\rangle_K \subseteq K[\boldsymbol{x}]_1.$$

The following lemma gives a sufficient condition for a linear form being a non-zero divisor modulo an ideal generated by products of linear forms (cf. [SS11b, Lemma 10]).

Lemma 3.2.26. *Let $f_1, \ldots, f_m \in K[\boldsymbol{x}]$ be products of linear forms and let $\ell \in K[\boldsymbol{x}]_1 \setminus \mathrm{Lin}(f_1, \ldots, f_m)$. Then ℓ is a non-zerodivisor modulo $\langle f_1, \ldots, f_m \rangle_{K[\boldsymbol{x}]}$.*

Proof. After an invertible linear change of variables, we may assume that $\ell = x_n$ and $\mathrm{Lin}(f_1, \ldots, f_m) \subseteq K[\boldsymbol{x}_{[n-1]}]_1$. Then $f_1, \ldots, f_m \in K[\boldsymbol{x}_{[n-1]}]$ and it is easy to see that ℓ is a non-zerodivisor modulo $\langle f_1, \ldots, f_m \rangle_{K[\boldsymbol{x}]}$. □

Non-zerodivisors can be used to split ideals generated by products of linear forms.

Lemma 3.2.27. *Let $f_1, \dots, f_m, g_1, g_2 \in K[\boldsymbol{x}]$ be products of linear forms such that $\operatorname{Lin}(g_1) \cap \operatorname{Lin}(f_1, \dots, f_m, g_2) = \{0\}$. Denote $I := \langle f_1, \dots, f_m \rangle_{K[\boldsymbol{x}]}$ and $g := g_1 \cdot g_2$. Then we have*

$$I + \langle g \rangle_{K[\boldsymbol{x}]} = \big(I + \langle g_1 \rangle_{K[\boldsymbol{x}]}\big) \cap \big(I + \langle g_2 \rangle_{K[\boldsymbol{x}]}\big).$$

Proof. It is clear that the left-hand side is contained in the right-hand side. Conversely, let $h = f + q_1 g_1 = f' + q_2 g_2$, where $f, f' \in I$ and $q_1, q_2 \in K[\boldsymbol{x}]$. Then $q_1 g_1 = f' - f + q_2 g_2 \in I + \langle g_2 \rangle$. By Lemma 3.2.26, g_1 is a non-zerodivisor modulo $I + \langle g_2 \rangle$, hence $q_1 \in I + \langle g_2 \rangle$. This implies $q_1 g_1 \in I + \langle g \rangle$, thus $h = f + q_1 g_1 \in I + \langle g \rangle$. □

Repeating the splitting procedure, we obtain an ideal decomposition with control over the dimension of the Lin-spaces of the generators.

Lemma 3.2.28. *Let $f_1, \dots, f_m, g \in K[\boldsymbol{x}]$ be products of linear forms and let $I := \langle f_1, \dots, f_m \rangle_{K[\boldsymbol{x}]}$. Then there exist products of linear forms $g_1, \dots, g_s \in K[\boldsymbol{x}]$ with $g = g_1 \cdots g_s$ such that*

$$I + \langle g \rangle_{K[\boldsymbol{x}]} = \bigcap_{i=1}^{s} \big(I + \langle g_i \rangle_{K[\boldsymbol{x}]}\big)$$

and $\dim_K \operatorname{Lin}(f_1, \dots, f_m, g_i) \leq \dim_K \operatorname{Lin}(f_1, \dots, f_m) + 1$ for all $i \in [s]$.

Proof. Apply Lemma 3.2.27 repeatedly. □

We conclude this section by showing how the rank-preserving homomorphism from Section 3.2.1 can be used to preserve non-membership in ideals generated by products of linear forms (cf. [SS11b, Lemma 8]).

Lemma 3.2.29. *Let $f, f_1, \dots, f_m \in K[\boldsymbol{x}]$ be products of linear forms and let $I := \langle f_1, \dots, f_m \rangle_{K[\boldsymbol{x}]}$. Let $\varphi\colon K[\boldsymbol{x}] \to K[\boldsymbol{z}]$ be a graded K-algebra homomorphism of degree 1. Assume that for all $\ell \in K[\boldsymbol{x}]_1$ with $\ell \mid f$ there exist linearly independent $\ell_1, \dots, \ell_r$ with $\operatorname{Lin}(\ell, f_1, \dots, f_m) \subseteq \langle \ell_1, \dots, \ell_r \rangle_K$ such that φ is rank-preserving for $\{\ell_1, \dots, \ell_r\}$. Then we have*

(a) $\varphi(I) = \langle \varphi(f_1), \dots, \varphi(f_m) \rangle_{K[\boldsymbol{z}]}$, and

(b) $f \in I$ if and only if $\varphi(f) \in \varphi(I)$.

Proof. By assumption and Lemma 3.2.8, the homomorphism φ is surjective, hence $\varphi(I) = \langle \varphi(f_1), \dots, \varphi(f_m) \rangle_{K[\boldsymbol{z}]}$. If $f \in I$, then clearly $\varphi(f) \in \varphi(I)$. Conversely, let $f \notin I$. Write $f = g_1 \cdot g_2$ with $g_1, g_2 \in K[\boldsymbol{x}]$ such that $\ell \notin \operatorname{Lin}(f_1, \dots, f_m)$ for all $\ell \in K[\boldsymbol{x}]_1$ with $\ell \mid g_1$ and $\operatorname{Lin}(g_2) \subseteq \operatorname{Lin}(f_1, \dots, f_m)$.

By Lemma 3.2.26, g_1 is a non-zerodivisor modulo I, hence $g_2 \notin I$. By assumption and Lemma 3.2.8, there exist linearly independent $\ell_1, \dots, \ell_r \in K[\boldsymbol{x}]_1$ such that $g_2, f_1, \dots, f_m \in K[\ell_1, \dots, \ell_r]$ and $\varphi|_{K[\ell_1,\dots,\ell_r]}$ is an isomorphism. This implies $\varphi(g_2) \notin \varphi(I)$. Now let $\ell \in K[\boldsymbol{x}]_1$ such that $\ell \mid g_1$, hence $\ell \notin \operatorname{Lin}(f_1, \dots, f_m)$. Again by assumption and Lemma 3.2.8, there exist $\ell_1, \dots, \ell_r \in K[\boldsymbol{x}]_1$ such that $\ell, f_1, \dots, f_m \in K[\ell_1, \dots, \ell_r]$ and $\varphi|_{K[\ell_1,\dots,\ell_r]}$ is an isomorphism. This implies $\varphi(\ell) \notin \operatorname{Lin}(\varphi(f_1), \dots, \varphi(f_m))$. By Lemma 3.2.26, $\varphi(g_1)$ is a non-zerodivisor modulo $\varphi(I)$, therefore $\varphi(f) = \varphi(g_1) \cdot \varphi(g_2) \notin \varphi(I)$. □

Identity testing of ΣΠΣ-circuits with bounded top fan-in

Now we can state the main result of [SS11b]. It shows how to reduce the number of variables of a $\Sigma_k\Pi\Sigma$-circuit from n to k while preserving non-zeroness.

Theorem 3.2.30. *Let $n, k, \delta \geq 1$. For $c \in K$, let $\Phi_c \colon K[\boldsymbol{x}] \to K[\boldsymbol{z}]$ be defined as in* (3.2.1).

There exists an effectively computable $N \in \mathbb{N}$ with $N = \operatorname{poly}(n, k, \delta)$ such that for all N-subsets $S \subseteq K$ we have the following: For all non-zero $C \in \Sigma_k\Pi_\delta\Sigma$ there exists $c \in S$ such that $\Phi_c(C) \neq 0$.

The proof of this theorem, given below, is based on the following lemma which provides a low-rank certificate for the non-zeroness of a ΣΠΣ-circuit (cf. [SS11b, Theorem 6]).

Lemma 3.2.31. *Let $f_1, \dots, f_m \in K[\boldsymbol{x}]$ be products of linear forms of the same degree such that $f := \sum_{i=1}^m f_i$ is non-zero. Then there exist $i \in [m]$ and polynomials $g_1, \dots, g_{i-1} \in K[\boldsymbol{x}]$ such that*

(a) $g_j \mid f_j$ for all $j \in [i-1]$,

(b) $\dim_K \operatorname{Lin}(g_1, \dots, g_j) \leq j$ for all $j \in [i-1]$,

(c) $f \notin \langle g_1, \dots, g_{i-1} \rangle_{K[\boldsymbol{x}]}$, and

(d) $f - \lambda f_i \in \langle g_1, \dots, g_{i-1} \rangle_{K[\boldsymbol{x}]}$ for some $\lambda \in K^*$.

Proof. Let $i \in [m]$ be maximal such that there exist $g_1, \dots, g_{i-1} \in K[\boldsymbol{x}]$ satisfying (a)–(c). This maximal index exists, because $f \notin \langle 0 \rangle$, thus $i = 1$ is possible. Now assume for the sake of contradiction that $f \notin \langle g_1, \dots, g_{i-1}, f_i \rangle$. This implies $i < m$. By Lemma 3.2.28, there exists $g_i \in K[\boldsymbol{x}]$ with $g_i \mid f_i$ such that $f \notin \langle g_1, \dots, g_i \rangle$ and $\dim_K \operatorname{Lin}(g_1, \dots, g_i) \leq (i-1) + 1 = i$. This is a contradiction to the maximality of i, therefore $f \in \langle g_1, \dots, g_{i-1}, f_i \rangle$. By homogeneity, there exists $\lambda \in K$ such that $f - \lambda f_i \in \langle g_1, \dots, g_{i-1} \rangle$, and by (c), we have $\lambda \neq 0$. □

Proof of Theorem 3.2.30. Let $C = \sum_{i=1}^{k} T_i$ be a non-zero $\Sigma_k\Pi_\delta\Sigma$-circuit. By Lemma 3.2.31, there exist $i \in [k]$, $g_1, \ldots, g_{i-1} \in K[\boldsymbol{x}]$, and $\lambda \in K^*$ such that $g_j \mid T_j$ for all $j \in [i-1]$, $\dim_K \operatorname{Lin}(g_1, \ldots, g_{i-1}) \leq i-1$, and $C = \lambda T_i \neq 0 \pmod{\langle g_1, \ldots, g_{i-1}\rangle}$. By Lemmas 3.2.7 and 3.2.29, there exists $N \in \mathbb{N}$ with $N = \operatorname{poly}(n, k, \delta)$ such that for all N-subsets $S \subseteq K$ we have $\Phi_c(\lambda T_i) \notin \langle \Phi_c(g_1), \ldots, \Phi_c(g_{i-1})\rangle$ for some $c \in S$. Since $\Phi_c(C) - \Phi_c(\lambda T_i) \in \langle \Phi_c(g_1), \ldots, \Phi_c(g_{i-1})\rangle$, this implies $\Phi_c(C) \neq 0$, as required. □

Preserving the rank of products of linear forms

Finally, we can state the main result of this section. Using arguments from [SS10], we show how to find rank-preserving homomorphisms for products of linear forms. For products of linear forms of rank at most ρ, the homomorphism under consideration reduces the number of variables from n to ρ^2.

Theorem 3.2.32. *Let $n, \rho, \delta \geq 1$ and let $r := \rho^2$. For $c \in K$, let $\Phi_c \colon K[\boldsymbol{x}] \to K[\boldsymbol{z}] = K[z_1, \ldots, z_r]$ be defined as in* (3.2.1).

There exists an effectively computable $N \in \mathbb{N}$ with $N = \operatorname{poly}(n, \rho, \delta)$ such that for all N-subsets $S \subseteq K$ we have the following: For all products of linear forms $f_1, \ldots, f_m \in K[\boldsymbol{x}]$ of degree at most δ and $\operatorname{rk}_K(f_1, \ldots, f_m) \leq \rho$ there exists $c \in S$ such that Φ_c is rank-preserving for $\{f_1, \ldots, f_m\}$.

The proof of this theorem, given below, is based on a criterion for linear independence of products of linear forms. A prototype of this characterization for general homogeneous polynomials is provided by the following lemma.

Lemma 3.2.33. *Let $f_1, \ldots, f_m \in K[\boldsymbol{x}]$ be homogeneous polynomials of the same degree. Then $f_1, \ldots, f_m$ are K-linearly independent if and only if for every $i \in [m]$ there exist polynomials $g_1, \ldots, g_{i-1} \in K[\boldsymbol{x}]$ such that $g_j \mid f_j$ for all $j \in [i-1]$ and $f_i \notin \langle g_1, \ldots, g_{i-1}\rangle_{K[\boldsymbol{x}]}$.*

Proof. Let $f_1, \ldots, f_m$ be K-linearly independent. Set $g_i := f_i$ for $i \in [m-1]$. Since $f_1, \ldots, f_m$ are homogeneous of the same degree, we obtain $f_i \notin \langle g_1, \ldots, g_{i-1}\rangle$ for all $i \in [m]$.

Conversely, let $f_1, \ldots, f_m$ be K-linearly dependent. Then there exist $\lambda_1, \ldots, \lambda_m \in K$, not all zero, such that $\lambda_1 f_1 + \cdots + \lambda_m f_m = 0$. Let $i \in [m]$ be maximal such that $\lambda_i \neq 0$, and let $g_1, \ldots, g_{i-1} \in K[\boldsymbol{x}]$ such that $g_j \mid f_j$ for all $j \in [i-1]$. Then $f_i = (-\lambda_1/\lambda_i) f_1 + \cdots + (-\lambda_{i-1}/\lambda_i) f_{i-1} \in \langle g_1, \ldots, g_{i-1}\rangle$. □

For products of linear forms, the polynomials $g_1, \ldots, g_{i-1}$ can be chosen such that the dimension of their Lin-space is small (cf. the full version of the paper [SS10]; note that they state this result in a slightly different language).

Lemma 3.2.34. *Let $f_1, \dots, f_r \in K[\boldsymbol{x}]$ be K-linearly independent products of linear forms of the same degree. Then there exist products of linear forms $g_1, \dots, g_{r-1} \in K[\boldsymbol{x}]$ with $g_i \mid f_i$ for $i \in [r-1]$ such that $f_i \notin \langle g_1, \dots, g_{i-1} \rangle_{K[\boldsymbol{x}]}$ for all $i \in [r]$ and $\dim_K \operatorname{Lin}(g_1, \dots, g_{r-1}) \leq \binom{r}{2}$.*

Proof. The proof is by double induction. We start with induction on r. For $r = 1$ the statement is true, because $f_1 \notin \langle 0 \rangle$. Now let $r \geq 2$. By induction hypothesis, we have $g'_1, \dots, g'_{r-2} \in K[\boldsymbol{x}]$ with $g'_i \mid f_i$ for $i \in [r-2]$ such that $f_i \notin \langle g'_1, \dots, g'_{i-1} \rangle$ for all $i \in [r-1]$ and $\dim_K \operatorname{Lin}(g'_1, \dots, g'_{r-2}) \leq \binom{r-1}{2}$.

> Now we want to prove the following claim: For all $j \in [0, r-2]$ there exist $g_1, \dots, g_j \in K[\boldsymbol{x}]$ with $g'_i \mid g_i$ and $g_i \mid f_i$ for $i \in [j]$ such that
>
> (a) $f_r \notin \langle g_1, \dots, g_j, f_{j+1}, \dots, f_{r-1} \rangle$, and
>
> (b) $\dim_K \operatorname{Lin}(g_1, \dots, g_j, g'_{j+1}, \dots, g'_{r-2}) \leq \binom{r-1}{2} + j$.
>
> We prove this statement by induction on j. Since $f_1, \dots, f_r$ are linearly independent and homogeneous of the same degree, we have $f_r \notin \langle f_1, \dots, f_{r-1} \rangle$, so the claim holds for $j = 0$. Now let $j \in [1, r-2]$. By induction hypothesis, we have $g_1, \dots, g_{j-1} \in K[\boldsymbol{x}]$ with $g'_i \mid g_i$ and $g_i \mid f_i$ for $i \in [j-1]$ such that $f_r \notin \langle g_1, \dots, g_{j-1}, f_j, \dots, f_{r-1} \rangle$ and
>
> $$\dim_K \operatorname{Lin}(g_1, \dots, g_{j-1}, g'_j, \dots, g'_{r-2}) \leq \binom{r-1}{2} + (j-1).$$
>
> Let us assume that $f_r \in \langle g_1, \dots, g_{j-1}, g'_j, f_{j+1}, \dots, f_{r-1} \rangle$, because otherwise we can set $g_j := g'_j$ and are done. By homogeneity, there exist $\lambda_{j+1}, \dots, \lambda_{r-1} \in K$ such that
>
> $$f_r - \sum_{i=j+1}^{r-1} \lambda_i f_i \in \langle g_1, \dots, g_{j-1}, g'_j \rangle. \tag{3.2.6}$$
>
> Also by homogeneity, we have $f_r - \sum_{i=j+1}^{r-1} \lambda_i f_i \notin \langle g_1, \dots, g_{j-1}, f_j \rangle$. By Lemma 3.2.28, there exists $g''_j \in K[\boldsymbol{x}]$ with $g''_j \mid f_j$ such that $f_r - \sum_{i=j+1}^{r-1} \lambda_i f_i \notin \langle g_1, \dots, g_{j-1}, g''_j \rangle$ and
>
> $$\dim_K \operatorname{Lin}(g_1, \dots, g_{j-1}, g''_j) \leq \dim_K \operatorname{Lin}(g_1, \dots, g_{j-1}) + 1.$$
>
> Set $g_j := \operatorname{lcm}(g'_j, g''_j)$. Then we have
>
> $$f_r - \sum_{i=j+1}^{r-1} \lambda_i f_i \notin \langle g_1, \dots, g_j \rangle \tag{3.2.7}$$

and $\dim_K \operatorname{Lin}(g_1, \ldots, g_j, g'_{j+1}, \ldots, g'_{r-2}) \leq \binom{r-1}{2} + j$. In order to finish the argument, we assume for the sake of contradiction that $f_r \in \langle g_1, \ldots, g_j, f_{j+1}, \ldots, f_{r-1} \rangle$. Then, again by homogeneity, there exist $\mu_{j+1}, \ldots, \mu_{r-1} \in K$ such that

$$f_r - \sum_{i=j+1}^{r-1} \mu_i f_i \in \langle g_1, \ldots, g_j \rangle \subseteq \langle g_1, \ldots, g_{j-1}, g'_j \rangle. \tag{3.2.8}$$

By (3.2.7), there exists a maximal index $i \in [j+1, r-1]$ such that $\lambda_i \neq \mu_i$. By (3.2.6) and (3.2.8), this implies

$$f_i \in \langle g_1, \ldots, g_{j-1}, g'_j, f_{j+1}, \ldots, f_{i-1} \rangle \subseteq \langle g'_1, \ldots, g'_{i-1} \rangle,$$

contradicting the hypothesis of the outer induction. Therefore, we have $f_r \notin \langle g_1, \ldots, g_j, f_{j+1}, \ldots, f_{r-1} \rangle$ and the claim is proved.

The case $j = r-2$ of the claim yields polynomials $g_1, \ldots, g_{r-2} \in K[\boldsymbol{x}]$ with $g'_i \mid g_i$ and $g_i \mid f_i$ for $i \in [r-2]$ such that $f_r \notin \langle g_1, \ldots, g_{r-2}, f_{r-1} \rangle$ and $\dim_K \operatorname{Lin}(g_1, \ldots, g_{r-2}) \leq \binom{r-1}{2} + (r-2)$. By Lemma 3.2.28, there exists $g_{r-1} \in K[\boldsymbol{x}]$ with $g_{r-1} \mid f_{r-1}$ such that $f_r \notin \langle g_1, \ldots, g_{r-1} \rangle$ and

$$\dim_K \operatorname{Lin}(g_1, \ldots, g_{r-1}) \leq \binom{r-1}{2} + (r-2) + 1 = \binom{r}{2}.$$

Since $f_i \notin \langle g'_1, \ldots, g'_{i-1} \rangle$ for all $i \in [r-1]$, we also have $f_i \notin \langle g_1, \ldots, g_{i-1} \rangle$ for all $i \in [r-1]$. This finishes the proof. □

Proof of Theorem 3.2.32. Let $f_1, \ldots, f_\rho \in K[\boldsymbol{x}]$ be K-linearly independent products of linear forms. We may assume that $f_1, \ldots, f_\rho$ are of degree δ (by homogeneity, we can treat each degree separately). By Lemma 3.2.34, there exist $g_1, \ldots, g_{\rho-1} \in K[\boldsymbol{x}]$ such that $g_i \mid f_i$ for all $i \in [\rho-1]$, $\operatorname{Lin}(g_1, \ldots, g_{\rho-1}) \leq \binom{\rho}{2}$, and $f_i \notin \langle g_1, \ldots, g_{i-1} \rangle$ for all $i \in [\rho]$. We have $\binom{\rho}{2} + 1 \leq \rho^2 = r$. By Lemmas 3.2.7 and 3.2.29, there exists $N \in \mathbb{N}$ with $N = \operatorname{poly}(n, \rho, \delta)$ such that for all N-subsets $S \subseteq K$ there exists $c \in S$ such that $\Phi_c(f_i) \notin \langle \Phi_c(g_1), \ldots, \Phi_c(g_{i-1}) \rangle$ for all $i \in [\rho]$. By Lemma 3.2.33, this implies that $\Phi_c(f_1), \ldots, \Phi_c(f_\rho)$ are K-linearly independent. □

3.2.5 Summary

We summarize the results of Sections 3.2.1 to 3.2.4. First we list the constructions of rank-preserving homomorphisms, then the obtained hitting sets.

Rank-preserving homomorphisms

We considered several circuit classes $\mathcal{C}$ depending on a subset of the parameters $n, s, \delta \geq 1$. For $\rho \geq 1$ and $\mathcal{C}$, we constructed families of K-algebra homomorphisms

$$\Phi_i \colon K[\boldsymbol{x}] \to K[z_1, \ldots, z_r], \quad i \in I,$$

where I is an index set, with the following property: For all arithmetic circuits $C_1, \ldots, C_m \in \mathcal{C} \cap K[\boldsymbol{x}]$ with $\operatorname{rk}_K(C_1, \ldots, C_m) \leq \rho$ there exists $i \in I$ such that Φ_i is rank-preserving for $\{C_1, \ldots, C_m\}$. The following table presents an overview of the respective constructions.

#	Circuit class	r	$\deg(\Phi_i)$	$\lvert I\rvert$	Remark
(a)	Σ	ρ	1	$\operatorname{poly}\big(n, \rho\big)$	
(b)	$\Sigma_s\Pi_\delta$	1	$\operatorname{poly}\big(n, \rho, s, \log\delta\big)$	$\operatorname{poly}\big(n, \rho, s, \log\delta\big)$	toric
(c)		1	$\rho - 1$	$\operatorname{poly}\big(n, \rho, s, \delta\big)$	
(d)		ρ	1	$\operatorname{poly}\big(n, \rho, s, \delta\big)$	
(e)	$\Pi_\delta\Sigma$	ρ^2	1	$\operatorname{poly}\big(n, \rho, \delta\big)$	

Item (a) on linear forms is proven by Theorem 3.2.6, items (b)–(d) on sparse polynomials are contained in Theorems 3.2.12 and 3.2.14, and item (e) on products of linear forms is Theorem 3.2.32.

Hitting sets

We presented hitting sets for the circuit classes listed in the following table.

#	Circuit class	Hitting set size
(a)	$\Sigma_s\Pi_\delta$	$\operatorname{poly}\big(n, s, \delta\big)$
(b)	$\mathrm{New}_{s,\delta}$	$\operatorname{poly}\big(n, s, \delta\big)$
(c)	$\Sigma_k\Pi_\delta\Sigma$	$\operatorname{poly}\big(n, \delta^k\big)$

Items (a)–(c) follow from Theorem 3.2.4 in conjunction with Theorems 3.2.11, 3.2.21, and 3.2.30, respectively. Note that Theorem 3.2.30 also uses the concept of rank-preserving homomorphisms.

To apply Theorems 3.2.4 and 3.2.30 the field K has to be of polynomial cardinality. Small finite fields can be efficiently replaced by a sufficiently large extension field by Lemma 2.2.9. Then, for both $K = \mathbb{Q}$ or K a finite field, the hitting sets can be chosen to consist of points of polynomial bit-size.

3.3 Linear Independence Testing

In this section we study the complexity of testing linear independence of arithmetic circuits.

Problem 3.3.1. Let K be a computable field and let $\mathcal{C}$ be a circuit class over K. Then the **linear independence testing** problem $\mathsf{LinIndep}_K(\mathcal{C})$ is defined as follows: Given circuits $C_1, \ldots, C_m \in \mathcal{C}$, decide whether the polynomials $C_1, \ldots, C_m$ are K-linearly independent. We set $\mathsf{LinIndep}_K := \mathsf{LinIndep}_K(\mathcal{C}_{\text{all}})$.

By the Alternant Criterion (see Theorem 3.1.1), testing linear independence reduces to (the complement of) PIT (cf. [CKW11, Lemma 14.4]).

Theorem 3.3.2. *Let K be a computable field. Then the problems $\mathsf{LinIndep}_K$ and $\overline{\mathsf{PIT}}_K$ are polynomial-time equivalent.*

Proof. Let C be an arithmetic circuit over $K[\boldsymbol{x}]$. Then $C \neq 0$ if and only if C is K-linearly dependent. Therefore, $\overline{\mathsf{PIT}}_K$ reduces to $\mathsf{LinIndep}_K$.

Conversely, let $C_1, \ldots, C_m$ be arithmetic circuits over $K[\boldsymbol{x}]$. Consider the polynomial

$$\det \begin{pmatrix} C_1(t_{1,1}, \ldots, t_{1,n}) & \cdots & C_m(t_{1,1}, \ldots, t_{1,n}) \\ \vdots & & \vdots \\ C_1(t_{m,1}, \ldots, t_{m,n}) & \cdots & C_m(t_{m,1}, \ldots, t_{m,n}) \end{pmatrix} \in K[\boldsymbol{t}],$$

where $\boldsymbol{t} = \{t_{i,j} \mid i \in [m] \text{ and } j \in [n]\}$ are new variables. By the Berkowitz algorithm (see Lemma A.3.1), an arithmetic circuit C for this polynomial can be computed in polynomial time. By Lemma 3.1.2, $C_1, \ldots, C_m$ are K-linearly independent if and only if $C \neq 0$. Therefore, $\mathsf{LinIndep}_K$ reduces to $\overline{\mathsf{PIT}}_K$. □

As a consequence of Theorem 3.3.2, we obtain efficient randomized algorithms for the linear independence testing problem.

Corollary 3.3.3. *Let $K = \mathbb{Q}$ or $K = \mathbb{F}_q$ for some prime power q. Then we have $\mathsf{LinIndep}_K \in \mathbf{RP}$.*

Proof. This follows from Theorems 3.3.2, 2.5.5, and 2.5.7. □

3.4 Computation of Linear Relations

In the final section of this chapter we investigate the complexity of computing the linear relations of arithmetic circuits. This problem can be considered

as a search version of the linear independence testing problem and was dealt with in [Kay10, CKW11].

Let K be a field and let $K[\boldsymbol{x}] = K[x_1, \ldots, x_n]$ be a polynomial ring over K. We say that a K-basis $\{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_r\}$ of a K-subspace $V \subseteq K^m$ is **canonical** if the matrix $M \in K^{m \times r}$ with columns $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_r$ is in reduced column echelon form. Every subspace $V \subseteq K^m$ has a unique canonical basis.

Given arithmetic circuits $C_1, \ldots, C_m$ over $K[\boldsymbol{x}]$, we want to compute the canonical K-basis $B \subset K^m$ of $\mathrm{LinRel}_K(C_1, \ldots, C_m)$. We restrict ourselves to polynomial-degree circuits, because otherwise B could have bit-size exponential in the encoding size of the circuits. For instance, if we are given the circuits $C_1 = 2^{2^s}$ and $C_2 = 1$ of encoding size $O(s)$ over $\mathbb{Q}$, then the canonical basis $B = \{(1, -2^{2^s})\}$ of $\mathrm{LinRel}_{\mathbb{Q}}(C_1, C_2)$ has bit-size $\Omega(2^s)$.

The following theorem deals with the case of general polynomial-degree circuits. It is proven similarly to Theorem 3.3.2, see [CKW11, Lemma 14.4].

Theorem 3.4.1. *Let $K = \mathbb{Q}$ or $K = \mathbb{F}_q$ for some prime power q. Then there exists a randomized polynomial-time Turing machine that, given polynomial-degree arithmetic circuits $C_1, \ldots, C_m$ over $K[\boldsymbol{x}]$, computes a K-linearly independent set $B \subset K^m$ in canonical form such that, with probability $\geq 1/2$, B is a K-basis of $\mathrm{LinRel}_K(C_1, \ldots, C_m)$.*

Proof sketch. A basis for the linear relations can be computed as follows. First determine an upper bound $d \geq 1$ for the formal degrees of the input circuits $C_1, \ldots, C_m$. Next, choose a subset $S \subseteq K$ with $|S| = 2md$ whose elements have small bit-size (if $|K| < 2md$, replace K by a sufficiently large extension field). Then pick points $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_m \in S^n$ at random and consider the matrix $M := \big(C_j(\boldsymbol{a}_i)\big)_{i,j} \in K^{m \times m}$. We have $\mathrm{LinRel}_K(C_1, \ldots, C_m) \subseteq \ker(M)$. By Lemma 3.1.2, Lemma 2.5.1, and a dimension argument, this is an equality with probability $\geq 1/2$. Now the canonical K-basis B of $\ker(M)$ can be computed by linear algebra algorithms. If $K = \mathbb{Q}$, standard Gaussian elimination might produce rational numbers of exponential bit-size. Here a modular approach can be used (see also the proof of Theorem 3.4.5). If $K = \mathbb{F}_q$ for some prime power q and K has been replaced by a finite field extension L/K, then note that the canonical L-basis of $\mathrm{LinRel}_L(C_1, \ldots, C_m)$ coincides with the canonical K-basis of $\mathrm{LinRel}_K(C_1, \ldots, C_m)$. □

3.4.1 Kronecker Products of Vectors

Die ganzen Zahlen hat der liebe Gott gemacht,
alles andere ist Menschenwerk.
(Leopold Kronecker)

In this section we give a polynomial-time algorithm for computing the linear relations of Kronecker products of vectors. The algorithm can be seen as a generalization of the polynomial-time identity test for set-multilinear $\Sigma\Pi\Sigma$-circuits (with unbounded top fan-in) of Raz & Shpilka [RS05]. Note that for this circuit class there is no polynomial-time *blackbox* algorithm known. Recently, progress towards a solution of this problem was made in [ASS12, FS12b].

For convenience of notation, we use a vector notation here as it was done in [FS12a]. Let $m, n, D \geq 1$ and let K be a field. For $i \in [m]$ and $j \in [n]$, let $\boldsymbol{a}_{i,j} = (a_{i,j,0}, \ldots, a_{i,j,D})^\top \in K^{D+1}$ be a vector. Define the Kronecker products (see Appendix A.3.1 for a definition)

$$\boldsymbol{f}_i := \boldsymbol{a}_{i,1} \otimes \cdots \otimes \boldsymbol{a}_{i,n} \in K^{(D+1)^n}$$

for all $i \in [m]$. Given the $\boldsymbol{a}_{i,j}$, we want to compute a K-basis of

$$\mathrm{LinRel}_K(\boldsymbol{f}_1, \ldots, \boldsymbol{f}_m) \subseteq K^m.$$

Note that we cannot compute the vectors $\boldsymbol{f}_1, \ldots, \boldsymbol{f}_m$ explicitly, since they have exponential dimensions.

Related circuit classes

Before we state the algorithm, we indicate the circuit classes to which Kronecker products of vectors relate. For $i \in [m]$, define the **products of univariates**

$$f_i := \prod_{j=1}^{n} \Big(\sum_{d=0}^{D} a_{i,j,d} \cdot x_j^d \Big) \in K[\boldsymbol{x}],$$

where $\boldsymbol{x} = \{x_1, \ldots, x_n\}$, and define the **set-multilinear products of linear forms**

$$g_i := \prod_{j=1}^{n} \Big(\sum_{d=0}^{D} a_{i,j,d} \cdot x_{j,d} \Big) \in K[\boldsymbol{x}],$$

where $\boldsymbol{x} = \{x_{j,d} \mid j \in [n] \text{ and } d \in [0, D]\}$. It is easy to see that

$$\mathrm{LinRel}_K(\boldsymbol{f}_1, \ldots, \boldsymbol{f}_m) = \mathrm{LinRel}_K(f_1, \ldots, f_m) = \mathrm{LinRel}_K(g_1, \ldots, g_m).$$

Note that the circuits $\sum_{i=1}^m f_i$ and $\sum_{i=1}^m g_i$ are zero if and only if $(1, \ldots, 1) \in \mathrm{LinRel}_K(\boldsymbol{f}_1, \ldots, \boldsymbol{f}_m)$.

Polynomial-time computation of $\mathrm{LinRel}_K(\boldsymbol{f}_1, \ldots, \boldsymbol{f}_m)$

Our approach is inspired by the algorithm in [CKW11, Theorem 14.8] for computing the linear relations of powers of sums of univariate polynomials. This problem is related to ours, because those powers can be transformed to sums of products of univariates [Sax08, SSS11, FS12b]. Note that the algorithm in [CKW11] uses partial derivatives and therefore works only in characteristic zero or sufficiently large characteristic, whereas our method works for any field.

Our algorithm is based on the following simple lemma. It can be used to compute the linear relations of Kronecker products iteratively, adding one factor at a time.

Lemma 3.4.2. *Let* $m, s, t \geq 1$. *Let* $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_m \in K^s$ *and* $\boldsymbol{w}_1, \ldots, \boldsymbol{w}_m \in K^t$ *be vectors. Then we have*

$$\mathrm{LinRel}_K(\boldsymbol{v}_1 \otimes \boldsymbol{w}_1, \ldots, \boldsymbol{v}_m \otimes \boldsymbol{w}_m) = \bigcap_{j=1}^{t} \mathrm{LinRel}_K(w_{1,j} \cdot \boldsymbol{v}_1, \ldots, w_{m,j} \cdot \boldsymbol{v}_m).$$

Proof. Let $\lambda_1, \ldots, \lambda_m \in K$. Then, by definition of the Kronecker product, we have $\sum_{i=1}^{m} \lambda_i \, \boldsymbol{v}_i \otimes \boldsymbol{w}_i = 0$ if and only if $\sum_{i=1}^{m} \lambda_i \, w_{i,j} \cdot \boldsymbol{v}_i = 0$ for all $j \in [t]$. □

The following lemma demonstrates how $\mathrm{LinRel}_K(w_1\boldsymbol{v}_1, \ldots, w_m\boldsymbol{v}_m)$ can be computed from $w_1, \ldots, w_m \in K$ and a K-basis of $\mathrm{LinRel}_K(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_m)$.

First we require some notation. Let V, W be finite-dimensional K-vector spaces with ordered bases $B \subset V$ and $C \subset W$. Then the matrix of a K-linear map $\varphi\colon V \to W$ with respect to B and C will be denoted by $M_C^B(\varphi) \in K^{|C| \times |B|}$.

Lemma 3.4.3. *Let* $m, s \geq 1$. *Let* $A \in K^{m \times m}$, *let* $F \in K^{s \times m}$ *and let* $U := \ker(F) \subseteq K^m$. *Let* $Q := M_C^E(K^m \twoheadrightarrow K^m/U) \in K^{r \times m}$, *where* E *is the standard* K*-basis of* K^m, C *is some* K*-basis of* K^m/U, *and* $r := |C| \in [0, m]$. *Then we have* $\ker(FA) = \ker(QA)$.

Proof. Observe that $\ker(FA)$ is the kernel of the K-linear map

$$\varphi\colon K^m \to K^m/U, \quad \boldsymbol{v} \mapsto (A \cdot \boldsymbol{v}) + U,$$

and we have $M_C^E(\varphi) = QA$. Therefore, we obtain $\ker(FA) = \ker(\varphi) = \ker(QA)$. □

Lemmas 3.4.2 and 3.4.3 suggest an iterative algorithm for computing the linear relations of Kronecker products. In the description of the algorithm, we denote by $\mathrm{diag}(a_1, \ldots, a_m) \in K^{m \times m}$ the diagonal matrix with diagonal entries $a_1, \ldots, a_m \in K$.

Algorithm 3.4.4 (Linear relations of Kronecker products of vectors)**.**
Input: Vectors $\boldsymbol{a}_{i,j} \in K^{D+1}$ for $i \in [m]$ and $j \in [n]$ over a computable field K.
Output: A K-basis B of $\mathrm{LinRel}_K(\boldsymbol{f}_1, \ldots, \boldsymbol{f}_m) \subseteq K^m$, where

$$\boldsymbol{f}_i := \boldsymbol{a}_{i,1} \otimes \cdots \otimes \boldsymbol{a}_{i,n} \in K^{(D+1)^n}$$

for $i \in [m]$.

(1) Compute a K-basis B of $\mathrm{LinRel}_K(\boldsymbol{a}_{1,1}, \ldots, \boldsymbol{a}_{m,1}) \subseteq K^m$.

(2) For $j \leftarrow 2, \ldots, n$, repeat steps (3) to (5).

(3) Compute a K-basis C of $K^m/\langle B\rangle_K$ and set $r \leftarrow |C|$. Compute

$$Q \leftarrow M_C^E\big(K^m \twoheadrightarrow K^m/\langle B\rangle_K\big) \in K^{r\times m},$$

where E denotes the standard K-basis of K^m.

(4) For $d \leftarrow 0, \ldots, D$, set $A_d \leftarrow \mathrm{diag}(a_{1,j,d}, \ldots, a_{m,j,d}) \in K^{m\times m}$.

(5) Compute a K-basis of $\bigcap_{d=0}^{D} \ker(QA_d)$ and replace B with it.

(6) Output B.

Theorem 3.4.5. *Algorithm 3.4.4 works correctly. If $K = \mathbb{Q}$ or $K = \mathbb{F}_q$ for some prime power q, then it can be implemented to run in polynomial time.*

Proof. For $i \in [m]$ and $j \in [n]$, define the partial Kronecker products

$$\boldsymbol{f}_{i,j} := \boldsymbol{a}_{i,1} \otimes \cdots \otimes \boldsymbol{a}_{i,j} \in K^{(D+1)^j}.$$

Denote by $B_1 \subset K^m$ the K-basis computed in step (1) of the algorithm and, for $j \in [2, n]$, denote by $B_j \subset K^m$ the K-basis computed in step (5) of the j-th round of the algorithm. We claim that B_j is a generating set of $\mathrm{LinRel}_K(\boldsymbol{f}_{1,j}, \ldots, \boldsymbol{f}_{m,j})$ for all $j \in [m]$. We prove this claim by induction on j. For $j = 1$, this is clear by step (1) of the algorithm. Now let $j \in [2, n]$. By Lemma 3.4.2, we have

$$\mathrm{LinRel}_K(\boldsymbol{f}_{1,j}, \ldots, \boldsymbol{f}_{m,j}) = \bigcap_{d=0}^{D} \mathrm{LinRel}_K(a_{1,j,d} \cdot \boldsymbol{f}_{1,j-1}, \ldots, a_{m,j,d} \cdot \boldsymbol{f}_{m,j-1}).$$

Denote by $F \in K^{(D+1)^{j-1}\times m}$ the matrix with columns $\boldsymbol{f}_{1,j-1}, \ldots, \boldsymbol{f}_{m,j-1}$. By induction, B_{j-1} is a K-basis of

$$\mathrm{LinRel}_K(\boldsymbol{f}_{1,j-1}, \ldots, \boldsymbol{f}_{m,j-1}) = \ker(F).$$

By Lemma 3.4.3, we get

$$\mathrm{LinRel}_K(a_{1,j,d} \cdot \boldsymbol{f}_{1,j-1}, \ldots, a_{m,j,d} \cdot \boldsymbol{f}_{m,j-1}) = \ker(FA_d) = \ker(QA_d),$$

where $Q \in K^{r \times m}$ and $A_d \in K^{m \times m}$ are the matrices computed in steps (3) and (4) of the j-th round of the algorithm. This finishes the proof of the claim. Since B_n is output in step (6), the algorithm works correctly.

Using well-known linear algebra algorithms, we see that Algorithm 3.4.4 requires $\mathrm{poly}(m, n, D)$ arithmetic operations in K. If $K = \mathbb{F}_q$ for some prime power q, then this yields a polynomial-time algorithm.

Now let $K = \mathbb{Q}$. In this case, standard Gaussian elimination might produce rational numbers of exponential bit-size. However, a modular approach can be used which we will sketch below. Let $s \geq 1$ be an upper bound on the bit-sizes of the coordinates of $\boldsymbol{a}_{i,j}$ for all $i \in [m]$ and $j \in [n]$. Then, by Lemma 2.2.7, the bit-sizes of the coordinates of $\boldsymbol{f}_i$ are bounded by ns for all $i \in [m]$. Denote by $F \in K^{(D+1)^n \times m}$ the matrix with columns $\boldsymbol{f}_1, \ldots, \boldsymbol{f}_m$. Using Cramer's Rule and Hadamard's Inequality (Lemma A.3.3), we see that there exists $N \geq 1$ with $N = \mathrm{poly}(m, n, s)$ such that $|\det(F')| < 2^N$ for every square submatrix F' of F and the bit-size of the canonical K-basis $B \subset K^m$ of $\ker(F)$ is bounded by N. We call a prime p bad if it divides a denominator in F (i. e. a denominator in one of the $\boldsymbol{a}_{i,j}$) or if $\dim_{\mathbb{F}_p}(\ker(F_p)) > \dim_{\mathbb{Q}}(\ker(F))$, where $F_p \in \mathbb{F}_p^{(D+1)^n \times m}$ denotes the image of F modulo p. The number of bad primes is bounded by $\mathrm{poly}(N)$. Given a prime p, we can use Algorithm 3.4.4 to compute the canonical $\mathbb{F}_p$-basis $B_p \subset \mathbb{F}_p^m$ of $\ker(F_p)$ in $\mathrm{poly}(m, n, s, D, \log p)$-time. Repeating this computation $\mathrm{poly}(N)$ times while discarding bad primes detected during this process, we obtain bases $B_{p_1}, \ldots, B_{p_\ell}$ for good primes $p_1, \ldots, p_\ell$ such that $p_1 \cdots p_\ell > 2^{2N+1}$. Applying a rational number reconstruction algorithm and a Chinese Remainder Theorem for rational numbers (see [vzGG03, Theorem 5.26 and Excercise 5.44]) coordinate-wise to the B_{p_i}, we obtain B. □

Chapter 4

Algebraic Independence Techniques

This chapter deals with the theme of algebraic independence. It constitutes the main part of this thesis and expands on the papers [BMS11, BMS13] and [MSS12]. First we present effective characterizations of the algebraic independence of polynomials. These include degree bounds for annihilating polynomials, the classical Jacobian Criterion, and the new Witt-Jacobian Criterion. Using those criteria, often in connection with techniques from Chapter 3, we design faithful homomorphisms for linear forms, monomials, sparse polynomials, and products of constant degree polynomials (of transcendence degree 2). Depending on the employed criterion, the field of constants is subject to restrictions. Furthermore, we extend the rank-based approach for $\Sigma\Pi\Sigma$-circuits with constant top fan-in by [DS07, KS11a] to $\Sigma\Pi\Sigma\Pi$-circuits with constant top and bottom fan-in. We obtain a hitting set construction whose efficiency depends on proving a certain rank bound. This question we leave open. Finally, we improve the complexity bound of the algebraic independence testing problem over finite fields from **PSPACE** to $\mathbf{NP}^{\#\mathbf{P}}$ by an application of the Witt-Jacobian Criterion.

Chapter outline

This chapter is organized along the lines of Chapter 3. Section 4.1 contains criteria for algebraic independence of polynomials. In Section 4.2 we define faithful homomorphisms and give explicit constructions of faithful homomorphisms and hitting sets for several circuit classes. We summarize those results in Section 4.2.6. Section 4.3 deals with the algebraic independence testing problem. Finally, in Section 4.4, we investigate the complexity of computing algebraic relations.

4.1 Algebraic Independence

In this section we introduce the notion of algebraic independence and give criteria for algebraic independence of polynomials.

Let K be a field, let A be a K-algebra, and let $a_1, \ldots, a_m \in A$. Then

$$\mathrm{AlgRel}_{K[\boldsymbol{y}]}(a_1, \ldots, a_m) := \big\{ F \in K[\boldsymbol{y}] \mid F(a_1, \ldots, a_m) = 0 \big\} \tag{4.1.1}$$

is an ideal of the polynomial ring $K[\boldsymbol{y}] = K[y_1, \ldots, y_m]$ and is called the **ideal of algebraic relations of** $a_1, \ldots, a_m$ **over** K. It is the kernel of the K-algebra epimorphism

$$K[\boldsymbol{y}] \to K[a_1, \ldots, a_m], \quad F \mapsto F(a_1, \ldots, a_m).$$

If $\mathrm{AlgRel}_{K[\boldsymbol{y}]}(a_1, \ldots, a_m) = \{0\}$, then $\{a_1, \ldots, a_m\}$ is called **algebraically independent over** K. If $\mathrm{AlgRel}_{K[\boldsymbol{y}]}(a_1, \ldots, a_m)$ contains a non-zero polynomial $F \in K[\boldsymbol{y}]$, then $\{a_1, \ldots, a_m\}$ is called **algebraically dependent over** K and we say that F is an **annihilating polynomial** of $a_1, \ldots, a_m$ over K.

For a subset $S \subseteq A$, we define the **transcendence degree of** S **over** K as

$$\mathrm{trdeg}_K(S) := \sup\big\{ \#T \mid T \subseteq S \text{ finite and alg. indep. over } K \big\}. \tag{4.1.2}$$

We have $\mathrm{trdeg}_K(S) \in \{-1\} \cup \mathbb{N} \cup \{\infty\}$, where $\mathrm{trdeg}_K(S) = -1$ for $A = S = \{0\}$. If L/K is a field extension, then $\mathrm{trdeg}_K(L)$ coincides with the notion of transcendence degree in field theory, usually written as $\mathrm{trdeg}(L/K)$.

The following lemma demonstrates that the transcendence degree of a K-algebra can be computed from the generators. Moreover, it shows that the transcendence degree of an affine K-algebra is finite.

Lemma 4.1.1. *Let A be a K-algebra generated by $S \subseteq A$. Then* $\mathrm{trdeg}_K(S) = \mathrm{trdeg}_K(A)$.

Proof. It suffices to show that for all algebraically independent $a_1, \ldots, a_r \in A$ we can find algebraically independent $s_1, \ldots, s_r \in S'$, where $S' \subseteq S$ is finite such that $a_1, \ldots, a_r \in K[S']$. Therefore we may assume that S is finite and A is an affine K-algebra.

Let $a_1, \ldots, a_r \in A$ be algebraically independent over K. By Lemma 4.1.2 below, there exists a prime ideal $\mathfrak{p} \subset A$ such that $a_1 + \mathfrak{p}, \ldots, a_r + \mathfrak{p} \in A/\mathfrak{p}$ are algebraically independent over K. Therefore, we have $\mathrm{trdeg}_K(A/\mathfrak{p}) \geq r$. Since $A/\mathfrak{p} = K[s + \mathfrak{p} \mid s \in S]$ is an affine K-domain, field theory (applied to the extension $\mathrm{Quot}(A/\mathfrak{p})/K$) tells us that there are $s_1, \ldots, s_r \in S$ such that $s_1 + \mathfrak{p}, \ldots, s_r + \mathfrak{p}$ are algebraically independent over K. This implies that $s_1, \ldots, s_r$ are algebraically independent over K. □

In the proof of Lemma 4.1.1, we used the following lemma. It shows how to transfer questions about the transcendence degree of affine K-algebras to affine domains, where results from field theory can be invoked (by passing to the quotient field).

Lemma 4.1.2. *Let A be an affine K-algebra and let $a_1, \ldots, a_r \in A$ be algebraically independent over K. Then there exists a minimal prime ideal $\mathfrak{p} \subset A$ such that $a_1 + \mathfrak{p}, \ldots, a_r + \mathfrak{p} \in A/\mathfrak{p}$ are algebraically independent over K.*

Proof. The following argument is contained in the proof of [Kem11, Theorem 5.9 and Proposition 5.10]. Since A is Noetherian (by [AM69, Corollary 7.7]), there exist only finitely many minimal prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_m \subset A$ (by [KR05, Proposition 5.6.15 b]). Assume for the sake of contradiction that, for all $i \in [m]$, the elements $a_1 + \mathfrak{p}_i, \ldots, a_r + \mathfrak{p}_i \in A/\mathfrak{p}_i$ are algebraically dependent over K. Then there are non-zero polynomials $F_i \in K[\boldsymbol{y}] = K[y_1, \ldots, y_r]$ such that $F_i(a_1, \ldots, a_r) \in \mathfrak{p}_i$. This implies that

$$a := \prod_{i=1}^{m} F_i(a_1, \ldots, a_r) \in \bigcap_{i=1}^{m} \mathfrak{p}_i = \sqrt{\langle 0 \rangle_A},$$

where the last equality holds by [KR05, Proposition 5.6.15 b]. Hence there is an $e \geq 1$ such that $a^e = 0$. Therefore, the polynomial $F := \prod_{i=1}^{m} F_i^e \in K[\boldsymbol{y}]$ is non-zero and satisfies $F(a_1, \ldots, a_r) = 0$, a contradiction. □

We are primarily interested in the case where $A = K[\boldsymbol{x}] = K[x_1, \ldots, x_n]$ is a polynomial ring. Let $f_1, \ldots, f_m \in K[\boldsymbol{x}]$. By Lemma 4.1.1, we have $0 \leq \operatorname{trdeg}_K(f_1, \ldots, f_m) \leq \operatorname{trdeg}_K(x_1, \ldots, x_n) = n$. Before we present effective characterizations of algebraic independence of polynomials in Sections 4.1.1 to 4.1.3, we give two sufficient conditions. For checking the condition of part (a) see Lemma 4.2.10.

Lemma 4.1.3. *Let $f_1, \ldots, f_n \in K[\boldsymbol{x}]$ be non-zero polynomials.*

(a) If $\operatorname{lt}_\sigma(f_1), \ldots, \operatorname{lt}_\sigma(f_n)$ are algebraically independent over K for some term ordering σ on $\mathbb{T}(\boldsymbol{x})$, then $f_1, \ldots, f_n$ are algebraically independent over K.

(b) If $f_i \in K[x_1, \ldots, x_i] \setminus K[x_1, \ldots, x_{i-1}]$ for all $i \in [n]$, then $f_1, \ldots, f_n$ are algebraically independent over K.

Proof. A proof of part (a) is implicitly contained in the proof of [KR05, Proposition 6.6.11]. Part (b) follows from (a) by considering the lexicographic term ordering $\sigma = \texttt{Lex}$ with $x_n >_{\texttt{Lex}} \cdots >_{\texttt{Lex}} x_1$ and using Lemma 4.2.10. □

4.1.1 Degree Bounds

Le degré de l'équation finale
résultante d'un nombre quelconque d'équations complettes,
refermant un pareil nombre d'inconnues, & de degrés quelconques,
est égal au produit des exposans des degrés de ces équations.
(Étienne Bézout)

Degree bounds for annihilating polynomials

Perron [Per27] established a degree bound for annihilating polynomials of $n+1$ polynomials in n variables.

Theorem 4.1.4 (Perron's Theorem, [Pło05, Theorem 1.1])**.** *Let $f_i \in K[\boldsymbol{x}]$ be a non-constant polynomial and let $\delta_i := \deg(f_i)$ for $i \in [n+1]$. Denote $w := (\delta_1, \ldots, \delta_{n+1}) \in \mathbb{N}_{>0}^{n+1}$. Then there exists a non-zero polynomial $F \in K[y_1, \ldots, y_{n+1}]$ with $\deg_w(F) \leq \delta_1 \cdots \delta_{n+1}$ such that $F(f_1, \ldots, f_{n+1}) = 0$. In particular, we have*

$$\deg(F) \leq \frac{\delta_1 \cdots \delta_{n+1}}{\min\{\delta_1, \ldots, \delta_{n+1}\}} \leq \big(\max\{\delta_1, \ldots, \delta_{n+1}\}\big)^n.$$

For fields of characteristic zero, Kayal [Kay09] deduced a degree bound for annihilating polynomials of an arbitrary number of polynomials. Moreover, this bound is in terms of the transcendence degree of the polynomials and independent of the number of variables. The following theorem is a generalization of this result for fields of arbitrary characteristic. In the proof, we use results from Section 4.2.

Theorem 4.1.5. *Let $f_1, \ldots, f_m \in K[\boldsymbol{x}]$ be polynomials of degree at most $\delta \geq 1$ and let $r := \operatorname{trdeg}_K(f_1, \ldots, f_m)$. If $m > r$, then there exists a non-zero polynomial $F \in K[y_1, \ldots, y_m]$ with*

$$\deg(F) \leq \delta^r$$

such that $F(f_1, \ldots, f_m) = 0$.

Proof. By a linear algebra argument, we may assume that K is infinite. Furthermore, we may assume that $m = r+1$ and $f_1, \ldots, f_r$ are algebraically independent over K. Let $F \in K[\boldsymbol{y}] = K[y_1, \ldots, y_m]$ be a non-zero irreducible polynomial such that $F(f_1, \ldots, f_m) = 0$. By Definition 4.2.1 and Theorem 4.2.2, there exists a K-algebra homomorphism $\varphi\colon K[\boldsymbol{x}] \to K[\boldsymbol{z}] = K[z_1, \ldots, z_r]$ such that the polynomials $g_i := \varphi(f_i) \in K[\boldsymbol{z}]$, $i \in [m]$, are of degree at most δ and $\operatorname{trdeg}_K(g_1, \ldots, g_m) = r$. By Theorem 4.1.4,

there exists a non-zero polynomial $G \in K[\boldsymbol{y}]$ with $\deg(G) \leq \delta^r$ such that $G(g_1, \ldots, g_m) = 0$. But since F is irreducible and satisfies

$$F(g_1, \ldots, g_m) = F(\varphi(f_1), \ldots, \varphi(f_m)) = \varphi(F(f_1, \ldots, f_m)) = 0,$$

Lemma 4.1.6 below implies that F divides G. Therefore, we have $\deg(F) \leq \deg(G) \leq \delta^r$. □

In the proof of Theorem 4.1.5 we used the following well-known lemma. It identifies a situation where annihilating polynomials are unique up to a non-zero scalar multiple. Due to the lack of a suitable reference, we present a proof here, following the instructions of [vdE00, Exercise 3.2.7].

Lemma 4.1.6. *Let* $f_1, \ldots, f_m \in K[\boldsymbol{x}]$ *such that* $\operatorname{trdeg}_K(f_1, \ldots, f_m) = m-1$. *Then* $\operatorname{AlgRel}_{K[\boldsymbol{y}]}(f_1, \ldots, f_m)$ *is a principal ideal of* $K[\boldsymbol{y}] = K[y_1, \ldots, y_m]$.

Proof. We may assume that $f_1, \ldots, f_{m-1}$ are algebraically independent over K. Now let $F_1, F_2 \in K[\boldsymbol{y}]$ be non-zero irreducible polynomials such that $F_i(f_1, \ldots, f_m) = 0$ for $i \in [2]$. It suffices to show that $F_1 = c \cdot F_2$ for some $c \in K^*$.

Since $f_1, \ldots, f_{m-1}$ are algebraically independent, we have $\deg_{y_m}(F_i) > 0$ for $i \in [2]$, so we may consider the y_m-resultant $g := \operatorname{res}_{y_m}(F_1, F_2) \in K[\boldsymbol{y}_{[m-1]}]$ of F_1 and F_2. By Lemma A.3.4 (a), there exist $g_1, g_2 \in K[\boldsymbol{y}]$ such that $g = g_1F_1 + g_2F_2$. Substituting $f_1, \ldots, f_m$, we obtain

$$\begin{aligned} &g(f_1, \ldots, f_{m-1}) \\ &\quad = g_1(f_1, \ldots, f_m) \cdot F_1(f_1, \ldots, f_m) + g_2(f_1, \ldots, f_m) \cdot F_2(f_1, \ldots, f_m) = 0. \end{aligned}$$

Since $f_1, \ldots, f_{m-1}$ are algebraically independent, this implies $g = 0$. Hence, by Lemma A.3.4 (b), F_1, F_2 have a non-constant common factor in $K[\boldsymbol{y}]$. Since we assumed that F_1, F_2 are irreducible, we obtain $F_1 = c \cdot F_2$ for some $c \in K^*$, as required. □

Definition 4.1.7. Let $f_1, \ldots, f_m \in K[\boldsymbol{x}]$ be polynomials. If

$$\operatorname{AlgRel}_{K[\boldsymbol{y}]}(f_1, \ldots, f_m) = \langle F \rangle_{K[\boldsymbol{y}]}$$

for some $F \in K[\boldsymbol{y}]$, then F is called a **minimal polynomial** of $f_1, \ldots, f_m$ over K.

Degree bound for field extensions

In Section 4.1.3 we will require bounds for the degree of finite extensions of function fields. It is possible to deduce such a bound from Perron's Theorem. However, for field extensions without primitive element, a stronger bound can be obtained from Bézout's Theorem. For homogeneous polynomials, this was shown in [Kem96]. By means of Lemma 4.1.9 below, we generalize this result to hold for arbitrary polynomials.

Theorem 4.1.8. *Let $f_1, \ldots, f_n \in K[\boldsymbol{x}]$ be algebraically independent over K and let $\delta_i := \deg(f_i)$ for $i \in [n]$. Then the extension $K(\boldsymbol{x})/K(f_1, \ldots, f_n)$ is finite and we have*

$$[K(\boldsymbol{x}) : K(f_1, \ldots, f_n)] \leq \delta_1 \cdots \delta_n.$$

Proof. By Lemma 4.1.9 below, we may assume that $f_1, \ldots, f_n$ are homogeneous. The homogeneous case of the statement is [Kem96, Corollary 1.8]. □

Lemma 4.1.9. *Let $f_1, \ldots, f_n \in K[\boldsymbol{x}]$ be algebraically independent over K, and let $f_i^{\mathrm{h}} \in K[x_0, \boldsymbol{x}]$ be the homogenization (with respect to the standard grading) of f_i for $i \in [n]$. Then $x_0, f_1^{\mathrm{h}}, \ldots, f_n^{\mathrm{h}}$ are algebraically independent over K and*

$$[K(\boldsymbol{x}) : K(f_1, \ldots, f_n)] = [K(x_0, \boldsymbol{x}) : K(x_0, f_1^{\mathrm{h}}, \ldots, f_n^{\mathrm{h}})].$$

Proof. Assume for the sake of contradiction that $x_0, f_1^{\mathrm{h}}, \ldots, f_n^{\mathrm{h}}$ are algebraically dependent over K. Then there exists a non-zero polynomial $F \in K[y_0, \ldots, y_n]$ such that $F(x_0, f_1^{\mathrm{h}}, \ldots, f_n^{\mathrm{h}}) = 0$. Since $x_0 - 1 \neq 0$, we may assume that $y_0 - 1$ does not divide F. This implies that the polynomial $G := F(1, y_1, \ldots, y_n) \in K[y_1, \ldots, y_n]$ is non-zero. We obtain

$$G(f_1, \ldots, f_n) = F(1, f_1, \ldots, f_n) = \big(F(x_0, f_1^{\mathrm{h}}, \ldots, f_n^{\mathrm{h}})\big)(1, \boldsymbol{x}) = 0,$$

a contradiction. Hence $x_0, f_1^{\mathrm{h}}, \ldots, f_n^{\mathrm{h}}$ are algebraically independent over K.

The field extensions $K(\boldsymbol{x})/K(f_1, \ldots, f_n)$ and $K(x_0, \boldsymbol{x})/K(x_0, f_1^{\mathrm{h}}, \ldots, f_n^{\mathrm{h}})$ are therefore finite. Note that both a $K(f_1, \ldots, f_n)$-basis of $K(\boldsymbol{x})$ and a $K(x_0, f_1^{\mathrm{h}}, \ldots, f_n^{\mathrm{h}})$-basis of $K(x_0, \boldsymbol{x})$ can be chosen from $\mathbb{T}(\boldsymbol{x})$. Therefore, in order to prove the assertion about the field extension degrees, it suffices to show that a set $B = \{\boldsymbol{x}^{\alpha_1}, \ldots, \boldsymbol{x}^{\alpha_s}\} \subset \mathbb{T}(\boldsymbol{x})$ is $K(f_1, \ldots, f_n)$-linearly independent if and only if it is $K(x_0, f_1^{\mathrm{h}}, \ldots, f_n^{\mathrm{h}})$-linearly independent.

First, let B be $K(f_1, \ldots, f_n)$-linearly independent. Assume for the sake of contradiction that B is $K(x_0, f_1^{\mathrm{h}}, \ldots, f_n^{\mathrm{h}})$-linearly dependent. Then there

exist polynomials $F_1, \dots, F_s \in K[y_0, \boldsymbol{y}] = K[y_0, y_1 \dots, y_n]$, not all zero, such that

$$F_1(x_0, f_1^{\mathrm{h}}, \dots, f_n^{\mathrm{h}}) \cdot \boldsymbol{x}^{\alpha_1} + \cdots + F_s(x_0, f_1^{\mathrm{h}}, \dots, f_n^{\mathrm{h}}) \cdot \boldsymbol{x}^{\alpha_s} = 0. \tag{4.1.3}$$

Denote $\delta_i := \deg(f_i^{\mathrm{h}}) \in \mathbb{N}_{>0}$ for $i \in [n]$ and $w := (1, \delta_1, \dots, \delta_n) \in \mathbb{N}_{>0}^{n+1}$. Now let $i \in [s]$ such that $F_i \neq 0$. Since $x_0, f_1^{\mathrm{h}}, \dots, f_n^{\mathrm{h}}$ are homogeneous and algebraically independent over K, we have $F_i(x_0, f_1^{\mathrm{h}}, \dots, f_n^{\mathrm{h}}) \neq 0$ and the homogeneous part of $F_i(x_0, f_1^{\mathrm{h}}, \dots, f_n^{\mathrm{h}})$ of degree $\deg(F_i(x_0, f_1^{\mathrm{h}}, \dots, f_n^{\mathrm{h}}))$ is given by $G_i(x_0, f_1^{\mathrm{h}}, \dots, f_n^{\mathrm{h}})$, where $G_i \in K[y_0, \boldsymbol{y}]$ is the w-homogeneous part of F_i of weighted degree $\deg_w(F_i)$. Considering only the leading forms of summands $F_i(x_0, f_1^{\mathrm{h}}, \dots, f_n^{\mathrm{h}}) \cdot \boldsymbol{x}^{\alpha_i}$ in (4.1.3) of maximal degree, we see that there exist w-homogeneous polynomials $G_1, \dots, G_s \in K[y_0, \boldsymbol{y}]$, not all zero, such that

$$G_1(x_0, f_1^{\mathrm{h}}, \dots, f_n^{\mathrm{h}}) \cdot \boldsymbol{x}^{\alpha_1} + \cdots + G_s(x_0, f_1^{\mathrm{h}}, \dots, f_n^{\mathrm{h}}) \cdot \boldsymbol{x}^{\alpha_s} = 0.$$

Let $i \in [s]$ such that $G_i \neq 0$. Since $G_i(x_0, f_1^{\mathrm{h}}, \dots, f_n^{\mathrm{h}})$ is homogeneous and non-zero, we have $\big(G_i(x_0, f_1^{\mathrm{h}}, \dots, f_n^{\mathrm{h}})\big)(1, \boldsymbol{x}) \neq 0$. Set $H_i := G_i(1, \boldsymbol{y}) \in K[\boldsymbol{y}]$ for all $i \in [s]$. Then we obtain

$$H_1(f_1, \dots, f_n) \cdot \boldsymbol{x}^{\alpha_1} + \cdots + H_s(f_1, \dots, f_n) \cdot \boldsymbol{x}^{\alpha_s} = 0,$$

where $H_i(f_1, \dots, f_n) = \big(G_i(x_0, f_1^{\mathrm{h}}, \dots, f_n^{\mathrm{h}})\big)(1, \boldsymbol{x}) \neq 0$ for some $i \in [s]$. This is a contradiction to the $K(f_1, \dots, f_n)$-linear independence of B.

Conversely, let B be $K(x_0, f_1^{\mathrm{h}}, \dots, f_n^{\mathrm{h}})$-linearly independent. Assume for the sake of contradiction that there exist $F_1, \dots, F_s \in K[\boldsymbol{y}]$, not all zero, such that

$$F_1(f_1, \dots, f_n) \cdot \boldsymbol{x}^{\alpha_1} + \cdots + F_s(f_1, \dots, f_n) \cdot \boldsymbol{x}^{\alpha_s} = 0.$$

Let $d \geq 1$ such that $\deg(F_i(f_1, \dots, f_n) \cdot \boldsymbol{x}^{\alpha_i}) \leq d$ for all $i \in [s]$ with $F_i \neq 0$. Then it is not hard to see that

$$0 = x_0^d \cdot \Big(\textstyle\sum_{i=1}^s F_i(f_1, \dots, f_n) \cdot \boldsymbol{x}^{\alpha_i}\Big)(\boldsymbol{x}/x_0) = \sum_{i=1}^s G_i(x_0, f_1^{\mathrm{h}}, \dots, f_n^{\mathrm{h}}) \cdot \boldsymbol{x}^{\alpha_i},$$

where $G_1, \dots, G_s \in K[y_0, \boldsymbol{y}]$ are polynomials such that $G_i(1, \boldsymbol{y}) = F_i$ for all $i \in [s]$. In particular, we have $G_i \neq 0$ for some $i \in [s]$. Since $x_0, f_1^{\mathrm{h}}, \dots, f_n^{\mathrm{h}}$ are algebraically independent over K, this implies $G_i(x_0, f_1^{\mathrm{h}}, \dots, f_n^{\mathrm{h}}) \neq 0$. This is a contradiction to the $K(x_0, f_1^{\mathrm{h}}, \dots, f_n^{\mathrm{h}})$-linear independence of B. □

A lower bound

The following construction is adapted from an example ascribed variously to Masser–Philippon [Bro87] and Lazard–Mora (see also [Płoo5, Example 3.2]). It demonstrates that the degree bounds featured in this section are essentially tight.

Example 4.1.10. Let $\delta_1, \dots, \delta_n \geq 1$ and consider the polynomials

$$f_1 := x_1^{\delta_1}, \quad f_2 := x_2^{\delta_2} - x_1, \quad \dots, \quad f_n := x_n^{\delta_n} - x_{n-1}, \quad f_{n+1} := x_n$$

in $K[\boldsymbol{x}]$. Then we have

(a) $\operatorname{trdeg}_K(f_1, \dots, f_n) = \operatorname{trdeg}_K(f_1, \dots, f_{n+1}) = n$,

(b) $\deg_w(F) \geq \deg(F) \geq \delta_1 \cdots \delta_n$ for all annihilating polynomials $F \in K[\boldsymbol{y}]$ of $f_1, \dots, f_{n+1}$, where $w = (\delta_1, \dots, \delta_n, 1)$, and

(c) $[K(\boldsymbol{x}) : K(f_1, \dots, f_n)] = \delta_1 \cdots \delta_n$.

Proof. Part (a) follows from Lemma 4.1.3. To prove (b), observe that the polynomial

$$F := \left(\cdots \left((y_{n+1}^{\delta_n} - y_n)^{\delta_{n-1}} - y_{n-1}\right)^{\delta_{n-2}} - \cdots\right)^{\delta_1} - y_1 \in K[\boldsymbol{y}]$$

is an annihilating polynomial of $f_1, \dots, f_{n+1}$ such that $\deg(F) = \deg_w(F) = \delta_1 \cdots \delta_n$. Thus, by Lemma 4.1.6, it suffices to show that F is irreducible. To this end, consider the K-algebra homomorphism

$$\varphi\colon K[\boldsymbol{y}] \to K[\boldsymbol{y}], \quad y_i \mapsto \begin{cases} -y_i + y_{i+1}^{\delta_i}, & \text{if } i \in [n], \\ y_i, & \text{if } i = n+1. \end{cases}$$

Note that φ is an automorphism of $K[\boldsymbol{y}]$ (by [KR00, Proposition 3.6.12], it suffices to check that φ is surjective). Since $\varphi(F) = y_1$ is irreducible, F is irreducible, too. Finally, (b) implies (c), because $K(f_1, \dots, f_{n+1}) = K(\boldsymbol{x})$. □

4.1.2 The Jacobian Criterion

Man muss immer umkehren.
(Carl G. J. Jacobi)

The classical Jacobian Criterion [Jac41] constitutes a more efficient test for algebraic independence of polynomials than Perron's Theorem. It is applicable to polynomials $f_1, \dots, f_m \in K[\boldsymbol{x}]$ for which $K(\boldsymbol{x})$ is a separable

extension of $K(f_1, \ldots, f_m)$, in particular in characteristic zero or sufficiently large prime characteristic (see Lemma 4.1.14). We prove the Jacobian Criterion in the spirit of the proof of the Witt-Jacobian Criterion presented in Section 4.1.3. For elementary proofs we refer to [Grö49, (116.25),(116.26)] or [ER93, DGW09, BMS13].

We state the Jacobian Criterion via the following differential form in the de Rham complex (see Appendix A.5).

Definition 4.1.11. Let R be a ring and let A be an R-algebra. Given $a_1, \ldots, a_m \in A$, we say that

$$\mathrm{J}_{A/R}(a_1, \ldots, a_m) := \mathrm{d}a_1 \wedge \cdots \wedge \mathrm{d}a_m \in \Omega^m_{A/R}$$

is the **Jacobian differential of** $a_1, \ldots, a_m$ **in** $\Omega^m_{A/R}$.

Under a separability hypothesis (for separability of field extensions, see Appendix A.3.3), polynomials $f_1, \ldots, f_m \in K[\boldsymbol{x}]$ are algebraically independent over K if and only if their Jacobian differential in $\Omega^m_{K[\boldsymbol{x}]/K}$ is non-zero.

Theorem 4.1.12 (Jacobian Criterion)**.** *Let $f_1, \ldots, f_m \in K[\boldsymbol{x}]$ be polynomials and assume that the extension $K(\boldsymbol{x})/K(f_1, \ldots, f_m)$ is separable. Then $f_1, \ldots, f_m$ are algebraically independent over K if and only if*

$$\mathrm{J}_{K[\boldsymbol{x}]/K}(f_1, \ldots, f_m) \neq 0.$$

By Lemma A.5.2, the zeroness of the Jacobian differential of $f_1, \ldots, f_m$ can be checked via their Jacobian matrix: we have $\mathrm{J}_{K[\boldsymbol{x}]/K}(f_1, \ldots, f_m) \neq 0$ if and only if $\mathrm{rk}_{K(\boldsymbol{x})} J_{\boldsymbol{x}}(f_1, \ldots, f_m) = m$.

We isolate the following special case of the Jacobian Criterion, because it holds without the separability condition.

Lemma 4.1.13. *Let $f_1, \ldots, f_m \in K[\boldsymbol{x}]$ be polynomials. If $f_1, \ldots, f_m$ are algebraically dependent over K, then $\mathrm{J}_{K[\boldsymbol{x}]/K}(f_1, \ldots, f_m) = 0$.*

Proof. Let $f_1, \ldots, f_m$ be algebraically dependent over K. Then they remain algebraically dependent over the algebraic closure $L := \overline{K}$. Since L is perfect, $L(f_1, \ldots, f_m)$ is separable over L. By Lemma A.5.6, we obtain

$$\dim_{L(f_1,\ldots,f_m)} \Omega^1_{L(f_1,\ldots,f_m)/L} = \mathrm{trdeg}(L(f_1, \ldots, f_m)/L) < m.$$

Thus $\mathrm{d}f_1, \ldots, \mathrm{d}f_m$ are linearly dependent, hence $\mathrm{J}_{L(f_1,\ldots,f_m)/L}(f_1, \ldots, f_m) = 0$. By Lemma A.5.4, this implies $\mathrm{J}_{L[f_1,\ldots,f_m]/L}(f_1, \ldots, f_m) = 0$. The inclusion $L[f_1, \ldots, f_m] \subseteq L[\boldsymbol{x}]$ induces an $L[f_1, \ldots, f_m]$-module homomorphism $\Omega^m_{L[f_1,\ldots,f_m]/L} \to \Omega^m_{L[\boldsymbol{x}]/L}$, hence $\mathrm{J}_{L[\boldsymbol{x}]/L}(f_1, \ldots, f_m) = 0$. Since $L[\boldsymbol{x}] = L \otimes_K K[\boldsymbol{x}]$, Lemma A.5.3 implies $\mathrm{J}_{K[\boldsymbol{x}]/K}(f_1, \ldots, f_m) = 0$. □

Proof of Theorem 4.1.12. If $f_1, \ldots, f_m$ are algebraically dependent over K, then, by Lemma 4.1.13, we have $\mathrm{J}_{K[\boldsymbol{x}]/K}(f_1, \ldots, f_m) = 0$.

Conversely, let $f_1, \ldots, f_m$ be algebraically independent over K. Since $K(\boldsymbol{x})/K(f_1, \ldots, f_m)$ is separable, there exist $f_{m+1}, \ldots, f_n \in \boldsymbol{x}$ such that $K(\boldsymbol{x})/K(f_1, \ldots, f_n)$ is algebraic and separable. Since $K[f_1, \ldots, f_n]$ is a polynomial ring, we have $\mathrm{J}_{K[f_1,\ldots,f_n]/K}(f_1, \ldots, f_n) \neq 0$. Lemmas A.5.4 and A.5.5 imply $\mathrm{J}_{K[\boldsymbol{x}]/K}(f_1, \ldots, f_n) \neq 0$, hence $\mathrm{J}_{K[\boldsymbol{x}]/K}(f_1, \ldots, f_m) \neq 0$. □

The separability hypothesis of the Jacobian Criterion is automatically satisfied in characteristic zero. In [DGW09], it is shown that the Jacobian Criterion is also valid in sufficiently large prime characteristic. As a consequence of Theorem 4.1.8, we can give a refined lower bound on the characteristic.

Lemma 4.1.14. *Let $f_1, \ldots, f_m \in K[\boldsymbol{x}]$ be polynomials of degree at most $\delta \geq 1$ and transcendence degree at most $r \geq 1$, and assume that* $\mathrm{char}(K) = 0$ *or* $\mathrm{char}(K) > \delta^r$. *Then the extension $K(\boldsymbol{x})/K(f_1, \ldots, f_m)$ is separable.*

Proof. In the case $\mathrm{char}(K) = 0$ there is nothing to prove, so let $p := \mathrm{char}(K) > \delta^r$. After renumbering polynomials and variables, we may assume that $f_1, \ldots, f_r, x_{r+1}, \ldots, x_n$ are algebraically independent over K. Then $\boldsymbol{x}_{[r+1,n]}$ is a transcendence basis of $K(\boldsymbol{x})/K(f_1, \ldots, f_m)$ and we claim that it is separating. Indeed, by Theorem 4.1.8 we have

$$[K(\boldsymbol{x}) : K(f_1, \ldots, f_m, \boldsymbol{x}_{[r+1,n]})] \leq [K(\boldsymbol{x}) : K(f_1, \ldots, f_r, \boldsymbol{x}_{[r+1,n]})] \leq \delta^r < p,$$

hence the minimal polynomial of x_i over $K(f_1, \ldots, f_m, \boldsymbol{x}_{[r+1,n]})$ has degree less than p for all $i \in [r]$. Therefore x_i is separable over $K(f_1, \ldots, f_m, \boldsymbol{x}_{[r+1,n]})$ for all $i \in [r]$. □

4.1.3 The Witt-Jacobian Criterion

Man muss immer generalisieren.
(Carl G. J. Jacobi)

In this section we propose a novel Jacobian-like criterion for algebraic independence of polynomials over fields of small prime characteristic. It builds on the de Rham-Witt complex constructed by Illusie [Ill79].

The abstract Witt-Jacobian criterion

The abstract Witt-Jacobian criterion is stated via the following differential form in the de Rham-Witt complex (see Appendix A.6.2).

Definition 4.1.15. Let $\ell \geq 0$ and let A be an $\mathbb{F}_p$-algebra. Given $a_1, \ldots, a_m \in A$, we say that

$$\mathrm{WJ}_{\ell+1,A}(a_1, \ldots, a_m) := \mathrm{d}[a_1]_{\leq \ell+1} \wedge \cdots \wedge \mathrm{d}[a_m]_{\leq \ell+1} \in \mathrm{W}_{\ell+1}\,\Omega^m_A$$

is the $(\ell+1)$**-th Witt-Jacobian differential of** $a_1, \ldots, a_m$ **in** $\mathrm{W}_{\ell+1}\,\Omega^m_A$.

The parameter ℓ will later be chosen according to a certain measure of inseparability. To this end, we extend the definition of the inseparable degree of finite field extensions to finitely generated field extensions.

Definition 4.1.16. Let Q/L be a finitely generated field extension. Then

$$[Q : L]_{\mathrm{insep}} := \min\big\{[Q : L(B)]_{\mathrm{insep}} \mid B \subset Q \text{ is a tr. basis of } Q/L\big\} \in \mathbb{N}_{>0}$$

is called the **inseparable degree** of Q/L.

If $\mathrm{char}(L) = 0$, then L is perfect, so $[Q : L]_{\mathrm{insep}} = 1$. If $\mathrm{char}(K) = p > 0$, then $[Q : L]_{\mathrm{insep}} = p^e$ for some $e \geq 0$, and $e = 0$ if and only if Q/L is separable.

As a consequence of Theorem 4.1.8, we obtain an effective bound for the inseparable degree of function field extensions.

Lemma 4.1.17. *Let K be a field and let $f_1, \ldots, f_m \in K[\boldsymbol{x}]$ be polynomials of degree at most $\delta \geq 1$. Then we have*

$$[K(\boldsymbol{x}) : K(f_1, \ldots, f_m)]_{\mathrm{insep}} \leq \delta^r,$$

where $r := \mathrm{trdeg}_K(f_1, \ldots, f_m)$.

Proof. After renumbering polynomials and variables, we may assume that $f_1, \ldots, f_r$, $x_{r+1}, \ldots, x_n$ are algebraically independent over K. Then $\boldsymbol{x}_{[r+1,n]}$ is a transcendence basis of $K(\boldsymbol{x})/K(f_1, \ldots, f_m)$, therefore

$$\begin{aligned}[K(\boldsymbol{x}) : K(f_1, \ldots, f_m)]_{\mathrm{insep}} &\leq [K(\boldsymbol{x}) : K(f_1, \ldots, f_m, \boldsymbol{x}_{[r+1,n]})]_{\mathrm{insep}} \\ &\leq [K(\boldsymbol{x}) : K(f_1, \ldots, f_r, \boldsymbol{x}_{[r+1,n]})] \\ &\leq \delta^r\end{aligned}$$

by Theorem 4.1.8. □

From now on, let p be a prime and let K be an algebraic extension of $\mathbb{F}_p$. In particular, note that K is a perfect field. Now we can state the abstract Witt-Jacobian Criterion.

Theorem 4.1.18 (Abstract Witt-Jacobian Criterion)**.** *Let $f_1, \dots, f_m \in K[\boldsymbol{x}]$ be polynomials and let $\ell \geq \log_p[K(\boldsymbol{x}) : K(f_1, \dots, f_m)]_{\text{insep}}$. Then $f_1, \dots, f_m$ are algebraically independent over K if and only if*

$$\mathrm{WJ}_{\ell+1,K[\boldsymbol{x}]}(f_1, \dots, f_m) \neq 0.$$

Remark 4.1.19. The bound for ℓ in Theorem 4.1.18 is tight. To see this, let $1 \leq m \leq n$ and let $e_i \geq 0$ and $f_i := x_i^{p^{e_i}}$ for $i \in [m]$. Then $f_1, \dots, f_m$ are algebraically independent over K, $[K(\boldsymbol{x}) : K(f_1, \dots, f_m)]_{\text{insep}} = p^e$, where $e = \sum_{i=1}^m e_i$, and we have

$$\mathrm{WJ}_{\ell+1,K[\boldsymbol{x}]}(f_1, \dots, f_m) = p^e \cdot [x_1]^{p^{e_1}-1} \cdots [x_m]^{p^{e_m}-1} \cdot \mathrm{WJ}_{\ell+1,K[\boldsymbol{x}]}(\boldsymbol{x}) \neq 0$$

if and only if $\ell \geq e$.

The following two lemmas constitute the proof of the abstract Witt-Jacobian Criterion.

Lemma 4.1.20. *Let $f_1, \dots, f_m \in K[\boldsymbol{x}]$ be algebraically dependent over K. Then $\mathrm{WJ}_{\ell+1,K[\boldsymbol{x}]}(f_1, \dots, f_m) = 0$ for all $\ell \geq 0$.*

Proof. Let $\ell \geq 0$ and let $r := \mathrm{trdeg}_K(f_1, \dots, f_m)$. Since K is perfect, the set $\{f_1, \dots, f_m\}$ contains a separating transcendence basis of $K(f_1, \dots, f_m)/K$, say $\{f_1, \dots, f_r\}$. This means that $K(f_1, \dots, f_m)$ is a finite separable extension of $K(f_1, \dots, f_r)$. Since $K[f_1, \dots, f_r]$ is isomorphic to a polynomial ring over K and $m > r$, we have $\mathrm{W}_{\ell+1}\,\Omega^m_{K[f_1,\dots,f_r]} = \{0\}$ (see Appendix A.6.3). By Lemma A.6.14, we infer $\mathrm{W}_{\ell+1}\,\Omega^m_{K(f_1,\dots,f_r)} = \{0\}$. Since $K(f_1, \dots, f_m)$ is finite and separable over $K(f_1, \dots, f_r)$, Lemma A.6.15 implies $\mathrm{W}_{\ell+1}\,\Omega^m_{K(f_1,\dots,f_m)} = \{0\}$. Again by Lemma A.6.14, we obtain $\mathrm{W}_{\ell+1}\,\Omega^m_{K[f_1,\dots,f_m]} = \{0\}$, in particular $\mathrm{WJ}_{\ell+1,K[f_1,\dots,f_m]}(f_1, \dots, f_m) = 0$. The inclusion $K[f_1, \dots, f_m] \subseteq K[\boldsymbol{x}]$ induces a homomorphism

$$\mathrm{W}_{\ell+1}\,\Omega^m_{K[f_1,\dots,f_m]} \to \mathrm{W}_{\ell+1}\,\Omega^m_{K[\boldsymbol{x}]},$$

hence $\mathrm{WJ}_{\ell+1,K[\boldsymbol{x}]}(f_1, \dots, f_m) = 0$. □

Lemma 4.1.21. *Let $f_1, \dots, f_m \in K[\boldsymbol{x}]$ be algebraically independent over K. Then $\mathrm{WJ}_{\ell+1,K[\boldsymbol{x}]}(f_1, \dots, f_m) \neq 0$ for all $\ell \geq \log_p[K(\boldsymbol{x}) : K(f_1, \dots, f_m)]_{\text{insep}}$.*

Proof. It suffices to consider the case $\ell = \log_p[K(\boldsymbol{x}) : K(f_1, \dots, f_m)]_{\text{insep}}$. By Definition 4.1.16, there exist $f_{m+1}, \dots, f_n \in K(\boldsymbol{x})$ such that $Q := K(\boldsymbol{x})$ is finite over $L := K(f_1, \dots, f_n)$ and $[Q : L]_{\text{insep}} = p^\ell$. Let L_{sep} be the separable closure of L in Q, thus Q/L_{sep} is purely inseparable. For $i \in [0, n]$, define the fields $L_i := L_{\text{sep}}[x_1, \dots, x_i]$, hence we have a tower

$$L \subseteq L_{\text{sep}} = L_0 \subseteq L_1 \subseteq \cdots \subseteq L_n = Q.$$

For $i \in [n]$, let $e_i \geq 0$ be minimal such that $x_i^{p^{e_i}} \in L_{i-1}$ (e_i exists, since L_i/L_{i-1} is purely inseparable), and set $q_i := p^{e_i}$. By the multiplicativity of field extension degrees, we have $\ell = \sum_{i=1}^n e_i$.

Since $\mathrm{WJ}_{1,K[\boldsymbol{x}]}(\boldsymbol{x}) \neq 0$, we have $p^\ell \cdot \mathrm{WJ}_{\ell+1,K[\boldsymbol{x}]}(\boldsymbol{x}) \neq 0$ by Lemma A.6.17. Lemma A.6.14 implies $p^\ell \cdot \mathrm{WJ}_{\ell+1,Q}(\boldsymbol{x}) \neq 0$. We conclude

$$\mathrm{WJ}_{\ell+1,Q}\big(x_1^{q_1}, \dots, x_n^{q_n}\big) = p^\ell \cdot [x_1]^{q_1-1} \cdots [x_n]^{q_n-1} \cdot \mathrm{WJ}_{\ell+1,Q}(\boldsymbol{x}) \neq 0, \quad (4.1.4)$$

since $[x_1]^{q_1-1} \cdots [x_n]^{q_n-1}$ is a unit in $\mathrm{W}_{\ell+1}(Q)$.

Now denote $\boldsymbol{f} := (f_1, \dots, f_n)$, and assume for the sake of contradiction that $\mathrm{WJ}_{\ell+1,Q}(\boldsymbol{f}) = 0$. For $i \in [0, n-1]$, we denote by

$$\Psi_i \colon \mathrm{W}_{\ell+1}\,\Omega^n_{L_i} \to \mathrm{W}_{\ell+1}\,\Omega^n_Q$$

the map induced by the inclusion $L_i \subseteq Q$. We want to show inductively, for $i = 0, \dots, n-1$, that the map Ψ_i satisfies

$$\Psi_i\big(\mathrm{d}[x_1^{q_1}] \wedge \cdots \wedge \mathrm{d}[x_i^{q_i}] \wedge \mathrm{d}[a_{i+1}] \wedge \cdots \wedge \mathrm{d}[a_n]\big) = 0 \quad (4.1.5)$$

for all $a_{i+1}, \dots, a_n \in L_i$. To prove this claim for $i = 0$, we first show that the map

$$\Psi \colon \mathrm{W}_{\ell+1}\,\Omega^n_{K[\boldsymbol{f}]} \to \mathrm{W}_{\ell+1}\,\Omega^n_Q,$$

induced by the inclusion $K[\boldsymbol{f}] \subseteq Q$, is zero. Let $\overline{\omega} \in \mathrm{W}_{\ell+1}\,\Omega^n_{K[\boldsymbol{f}]}$. By Lemma A.6.6, the element $\overline{\omega}$ is a $\mathbb{Z}$-linear combination of products of elements of the form $\mathrm{V}^j[c\boldsymbol{f}^\alpha]$ and $\mathrm{dV}^j[c\boldsymbol{f}^\alpha]$ for some $j \in [0, \ell]$, $c \in K$, and $\alpha \in \mathbb{N}^n$. Hence we may assume that

$$\overline{\omega} = \mathrm{V}^{j_0}[c_0\boldsymbol{f}^{\alpha_0}] \cdot \mathrm{dV}^{j_1}[c_1\boldsymbol{f}^{\alpha_1}] \wedge \cdots \wedge \mathrm{dV}^{j_n}[c_n\boldsymbol{f}^{\alpha_n}],$$

where $j_0, \dots, j_n \in [0, \ell]$, $c_0, \dots, c_n \in K$, and $\alpha_0, \dots, \alpha_n \in \mathbb{N}^n$. Let $\omega \in \mathrm{W}_{\ell+1+j}\,\Omega^n_{K[\boldsymbol{f}]}$ be a lift of $\overline{\omega}$, where $j \geq \ell + 1$. Using $\mathrm{F}\,\mathrm{dV} = \mathrm{d}$ and $\mathrm{F}\,\mathrm{d}[w] = [w]^{p-1}\,\mathrm{d}[w]$ for $w \in K[\boldsymbol{f}]$, we deduce

$$\mathrm{F}^{\ell+1}\,\omega = g \cdot \mathrm{d}[c_1\boldsymbol{f}^{\alpha_1}] \wedge \cdots \wedge \mathrm{d}[c_n\boldsymbol{f}^{\alpha_n}] \quad \text{for some } g \in \mathrm{W}_j(K[\boldsymbol{f}]).$$

By the Leibniz rule, we can simplify to

$$\mathrm{F}^{\ell+1}\,\omega = g' \cdot \mathrm{d}[f_1] \wedge \cdots \wedge \mathrm{d}[f_n] \quad \text{for some } g' \in \mathrm{W}_j(K[\boldsymbol{f}]).$$

Since $\mathrm{WJ}_{\ell+1,Q}(\boldsymbol{f}) = 0$ by assumption, we obtain $\mathrm{F}^{\ell+1}\,\Psi(\omega) = \Psi(\mathrm{F}^{\ell+1}\,\omega) \in \mathrm{Fil}^{\ell+1}\,\mathrm{W}_j\,\Omega^n_Q$, thus $\Psi(\omega) \in \mathrm{Fil}^{\ell+1}\,\mathrm{W}_{\ell+1+j}\,\Omega^n_Q$ by Lemma A.6.12. This shows $\Psi(\overline{\omega}) = 0$, so Ψ is zero. Lemmas A.6.14 and A.6.15 imply that Ψ_0 is zero, proving (4.1.5) for $i = 0$.

Now let $i \in [n-1]$ and let $\overline{\omega} = \mathrm{d}[x_1^{q_1}] \wedge \cdots \wedge \mathrm{d}[x_i^{q_i}] \wedge \mathrm{d}[a_{i+1}] \wedge \cdots \wedge \mathrm{d}[a_n] \in \mathrm{W}_{\ell+1}\,\Omega^n_{L_i}$, where $a_{i+1}, \ldots, a_n \in L_i$. Since $L_i = L_{i-1}[x_i]$, we may assume by Lemma A.6.6 that

$$\overline{\omega} = \mathrm{d}[x_1^{q_1}] \wedge \cdots \wedge \mathrm{d}[x_i^{q_i}] \wedge \mathrm{dV}^{j_{i+1}}[c_{i+1}x_i^{\alpha_{i+1}}] \wedge \cdots \wedge \mathrm{dV}^{j_n}[c_n x_i^{\alpha_n}],$$

where $j_{i+1}, \ldots, j_n \in [0, \ell]$, $c_{i+1}, \ldots, c_n \in L_{i-1}$, and $\alpha_{i+1}, \ldots, \alpha_n \geq 0$. Let $\omega \in \mathrm{W}_{\ell+1+j}\,\Omega^n_{L_i}$ be a lift of $\overline{\omega}$, where $j \geq \ell+1$. As above, we deduce

$$\mathrm{F}^{\ell+1}\,\omega = g \cdot \mathrm{d}[x_1^{q_1}] \wedge \cdots \wedge \mathrm{d}[x_i^{q_i}] \wedge \mathrm{d}[c_{i+1}x_i^{\alpha_{i+1}}] \wedge \cdots \wedge \mathrm{d}[c_n x_i^{\alpha_n}]$$

for some $g \in \mathrm{W}_j(L_i)$, and by the Leibniz rule, we can write

$$\mathrm{F}^{\ell+1}\,\omega = g' \cdot \mathrm{d}[x_1^{q_1}] \wedge \cdots \wedge \mathrm{d}[x_i^{q_i}] \wedge \mathrm{d}[c_{i+1}] \wedge \cdots \wedge \mathrm{d}[c_n]$$

for some $g' \in \mathrm{W}_j(L_i)$. Since $x_1^{q_1}, \ldots, x_i^{q_i}$, $c_{i+1}, \ldots, c_n \in L_{i-1}$, we obtain $\mathrm{F}^{\ell+1}\,\Psi_i(\omega) = \Psi_i(\mathrm{F}^{\ell+1}\,\omega) \in \mathrm{Fil}^{\ell+1}\,\mathrm{W}_j\,\Omega^n_Q$ by induction, hence we get $\Psi_i(\omega) \in \mathrm{Fil}^{\ell+1}\,\mathrm{W}_{\ell+1+j}\,\Omega^n_Q$ by Lemma A.6.12. This shows $\Psi_i(\overline{\omega}) = 0$, completing the induction.

Equation (4.1.5) for $i = n-1$ and $a_n = x_n^{q_n} \in L_{n-1}$ yields

$$\mathrm{WJ}_{\ell+1,Q}(x_1^{q_1}, \ldots, x_n^{q_n}) = 0,$$

contradicting (4.1.4). We conclude $\mathrm{WJ}_{\ell+1,Q}(\boldsymbol{f}) \neq 0$, thus

$$\mathrm{WJ}_{\ell+1,K[\boldsymbol{x}]}(f_1, \ldots, f_m) \neq 0$$

by Lemma A.6.14. □

The explicit Witt-Jacobian criterion

As before, let p be a prime and let K be an algebraic extension of $\mathbb{F}_p$. Let $R = \mathrm{W}(K)$ be the Witt ring of K. For the proof of the explicit Witt-Jacobian Criterion, we use Illusie's realization $\mathrm{E}^m_{\ell+1}$ of $\mathrm{W}_{\ell+1}\,\Omega^m_{K[\boldsymbol{x}]}$ which is described in Appendix A.6.3.

The explicit Witt-Jacobian Criterion is formulated as a divisibility condition on the coefficients of the following polynomials over R.

Definition 4.1.22. Let $\ell \geq 0$, let $g_1, \ldots, g_m \in R[\boldsymbol{x}]$, and let $\boldsymbol{u} \subseteq \boldsymbol{x}$ be an m-subset. We call

$$\mathrm{WJP}_{\ell+1,\boldsymbol{u}}(g_1, \ldots, g_m) := (g_1 \cdots g_m)^{p^\ell - 1}\big(\textstyle\prod_{x \in \boldsymbol{u}} x\big) \cdot \det J_{\boldsymbol{u}}(g_1, \ldots, g_m) \in R[\boldsymbol{x}]$$

the $(\ell+1)$**-th Witt-Jacobian polynomial of** $g_1, \ldots, g_m$ **with respect to** $\boldsymbol{u}$.

The divisibility condition is defined using the p-adic valuation v_p of $\mathbb{Q}$ (see Definition A.6.3).

Definition 4.1.23. Let $f \in R[\boldsymbol{x}]$ be a polynomial and let $\ell \geq 0$. Then f is called $(\ell+1)$**-degenerate** if the coefficient of $\boldsymbol{x}^\alpha$ in f is divisible by $p^{\min\{v_p(\alpha),\ell\}+1}$ for all $\alpha \in \mathbb{N}^n$.

Since K is perfect, we have $R/\langle p\rangle_R \cong K$ and $R[\boldsymbol{x}]/\langle p\rangle_{R[\boldsymbol{x}]} \cong K[\boldsymbol{x}]$. In the sequel, we will identify those rings. Now we can state the explicit Witt-Jacobian Criterion.

Theorem 4.1.24 (Explicit Witt-Jacobian Criterion)**.** *Let $f_1, \dots, f_m \in K[\boldsymbol{x}]$ be polynomials and let $\ell \geq \log_p[K(\boldsymbol{x}) : K(f_1, \dots, f_m)]_{\text{insep}}$. Let $g_1, \dots, g_m \in R[\boldsymbol{x}]$ be polynomials such that $f_i = g_i \pmod{\langle p\rangle_{R[\boldsymbol{x}]}}$ for all $i \in [m]$.*

Then $f_1, \dots, f_m$ are algebraically independent over K if and only if there exists $I \in \binom{[n]}{m}$ such that $\mathrm{WJP}_{\ell+1,\boldsymbol{x}_I}(g_1, \dots, g_m)$ is not $(\ell+1)$-degenerate.

Proof. Using Theorem A.6.16 (b) and Lemmas 4.1.26 and 4.1.30 below, the assertion follows from Theorem 4.1.18. □

Example 4.1.25. Let us revisit the example of Remark 4.1.19. Let $1 \leq m \leq n$ and let $e_i \geq 0$ and $f_i := x_i^{p^{e_i}} \in K[\boldsymbol{x}]$ for $i \in [m]$. Then $f_1, \dots, f_m$ are algebraically independent over K and $[K(\boldsymbol{x}) : K(f_1, \dots, f_m)]_{\text{insep}} = p^e$, where $e = \sum_{i=1}^m e_i$. We choose the lift $g_i := x_i^{p^{e_i}} \in R[\boldsymbol{x}]$ of f_i for all $i \in [m]$. Then we have

$$\mathrm{WJP}_{\ell+1,\boldsymbol{x}_{[m]}}(g_1, \dots, g_m) = p^e \cdot \big(x_1^{p^{e_1}} \cdots x_m^{p^{e_m}}\big)^{p^\ell}.$$

Since $v_p\big(p^{e_1+\ell}, \dots, p^{e_m+\ell}, 0, \dots, 0\big) \geq \ell$, this Witt-Jacobian polynomial is not $(\ell+1)$-degenerate if and only if $\ell \geq e$.

The following lemma shows how the Teichmüller lift of a polynomial can be realized in $\mathrm{E}^0_{\ell+1}$.

Lemma 4.1.26. *Let $\ell \geq 0$, let $f \in K[\boldsymbol{x}]$, and let $g \in R[\boldsymbol{x}]$ such that $f = g \pmod{\langle p\rangle_{R[\boldsymbol{x}]}}$. Then we have*

$$\tau([f]) = \big(\mathrm{F}^{-\ell}\, g\big)^{p^\ell} \quad \text{in } \mathrm{E}^0_{\ell+1},$$

where $\tau\colon \mathrm{W}_{\ell+1}(K[\boldsymbol{x}]) \to \mathrm{E}^0_{\ell+1}$ is the $\mathrm{W}(K)$-algebra isomorphism from Theorem A.6.16 (a).

Remark 4.1.27. Note that the intermediate expression $\mathrm{F}^{-\ell}\, g \in R[\boldsymbol{x}^{p^{-\infty}}]$ is in general not an element of E^0.

Proof of Lemma 4.1.26. Write $g = \sum_{i=1}^{s} c_i \boldsymbol{x}^{\alpha_i}$, where $c_i \in R$ and $\alpha_i \in \mathbb{N}^n$ for $i \in [s]$. By assumption, we have $[f] = \sum_{i=1}^{s} c_i [\boldsymbol{x}^{\alpha_i}]$ in $\mathrm{W}_1(K[\boldsymbol{x}])$. By Lemma A.6.2, we obtain

$$\mathrm{F}^{\ell}[f] = [f]^{p^{\ell}} = \left(\sum_{i=1}^{s} c_i [\boldsymbol{x}^{\alpha_i}]\right)^{p^{\ell}} = \sum_{|\boldsymbol{i}|=p^{\ell}} \binom{p^{\ell}}{\boldsymbol{i}} c_1^{i_1} [\boldsymbol{x}^{\alpha_1}]^{i_1} \cdots c_s^{i_s} [\boldsymbol{x}^{\alpha_s}]^{i_s} \quad (4.1.6)$$

in $\mathrm{W}_{\ell+1}(K[\boldsymbol{x}])$, where the last sum is over all $\boldsymbol{i} = (i_1, \ldots, i_s) \in \mathbb{N}^s$. Now define

$$w := \sum_{|\boldsymbol{i}|=p^{\ell}} p^{-\ell+v_p(\boldsymbol{i})} \binom{p^{\ell}}{\boldsymbol{i}} \mathrm{V}^{-\ell+v_p(\boldsymbol{i})} \mathrm{F}^{-v_p(\boldsymbol{i})} \big(c_1^{i_1} [\boldsymbol{x}^{\alpha_1}]^{i_1} \cdots c_s^{i_s} [\boldsymbol{x}^{\alpha_s}]^{i_s}\big) \in \mathrm{W}(K[\boldsymbol{x}]).$$

Since K is perfect, F is an automorphism of R. Moreover, $p^{-\ell+v_p(\boldsymbol{i})} \cdot \binom{p^{\ell}}{\boldsymbol{i}} \in \mathbb{N}$ by Lemma A.6.5, $v_p(\boldsymbol{i}) \le \ell$, and $p^{-v_p(\boldsymbol{i})} \cdot \boldsymbol{i} \in \mathbb{N}^s$ for all $\boldsymbol{i} \in \mathbb{N}^s$ with $|\boldsymbol{i}| = p^{\ell}$, so w is well-defined. Since $\mathrm{V}\,\mathrm{F} = \mathrm{F}\,\mathrm{V} = p$, we see that (4.1.6) is equal to $\mathrm{F}^{\ell} w$ in $\mathrm{W}_{\ell+1}(K[\boldsymbol{x}])$. The injectivity of F implies $[f] = w$ in $\mathrm{W}_{\ell+1}(K[\boldsymbol{x}])$.

Now denote $m_i := c_i \boldsymbol{x}^{\alpha_i} \in R[\boldsymbol{x}]$ for $i \in [s]$. By Theorem A.6.16 (a), we have $\tau([x_i]) = x_i$ for all $i \in [n]$ and $\tau\,\mathrm{V} = \mathrm{V}\,\tau$. Hence we have $\tau(c_i[\boldsymbol{x}^{\alpha_i}]) = m_i$ for all $i \in [s]$, therefore

$$\begin{aligned}
\tau([f]) &= \tau(w) \\
&= \sum_{|\boldsymbol{i}|=p^{\ell}} p^{-\ell+v_p(\boldsymbol{i})} \binom{p^{\ell}}{\boldsymbol{i}} \mathrm{V}^{-\ell+v_p(\boldsymbol{i})} \mathrm{F}^{-v_p(\boldsymbol{i})} (m_1^{i_1} \cdots m_s^{i_s}) \\
&= \sum_{|\boldsymbol{i}|=p^{\ell}} \binom{p^{\ell}}{\boldsymbol{i}} \mathrm{F}^{-\ell} (m_1^{i_1} \cdots m_s^{i_s}) = \sum_{|\boldsymbol{i}|=p^{\ell}} \binom{p^{\ell}}{\boldsymbol{i}} (\mathrm{F}^{-\ell} m_1)^{i_1} \cdots (\mathrm{F}^{-\ell} m_s)^{i_s} \\
&= \left(\sum_{i=1}^{s} \mathrm{F}^{-\ell} m_i\right)^{p^{\ell}} = \big(\mathrm{F}^{-\ell} g\big)^{p^{\ell}}
\end{aligned}$$

in $\mathrm{E}^0_{\ell+1}$. □

Let $Q = \mathrm{Quot}(R)$ be the quotient field of R. The algebra $Q[\boldsymbol{x}^{p^{-\infty}}]$, defined in Appendix A.6.3, is graded in a natural way by $G := \mathbb{N}[p^{-1}]^n$. The homogeneous elements of degree $\alpha \in G$ are of the form $c\boldsymbol{x}^{\alpha}$ for some $c \in Q$. This grading extends to $\Omega_{Q[\boldsymbol{x}^{p^{-\infty}}]}$ by defining $\omega \in \Omega^m_{Q[\boldsymbol{x}^{p^{-\infty}}]}$ to be homogeneous of degree $\alpha \in G$ if its coordinates in the representation (A.6.3) are. We denote the homogeneous part of degree α of ω by $(\omega)_{\alpha}$. For $\ell \ge 0$ and $\alpha \in G$, define

$$\nu(\ell+1, \alpha) := \min\big\{\max\{0, \ell+1+v_p(\alpha)\}, \ell+1\big\} \in [0, \ell+1]. \quad (4.1.7)$$

Using ν, the graded components of the filtration $\mathrm{Fil}^{\ell+1}\mathrm{E}$ can be described explicitly.

Lemma 4.1.28 ([Ill79, Proposition I.2.12])**.** *We have*

$$\big(\mathrm{Fil}^{\ell+1}\mathrm{E}\big)_\alpha = p^{\nu(\ell+1,\alpha)}\big(\mathrm{E}\big)_\alpha$$

for all $\ell \geq 0$ and $\alpha \in G$.

The following simple fact demonstrates how the degeneracy condition is related to ν.

Lemma 4.1.29. *Let $\ell \geq 0$ and let $f \in R[\boldsymbol{x}] \subset \mathrm{E}^0$. Then f is $(\ell+1)$-degenerate if and only if the coefficient of $\boldsymbol{x}^\alpha$ in $\mathrm{F}^{-\ell} f$ is divisible by $p^{\nu(\ell+1,\alpha)}$ for all $\alpha \in G$.*

Proof. Let $\alpha \in G$ and let $c \in R$ be the coefficient of $\boldsymbol{x}^\alpha$ in $\mathrm{F}^{-\ell} f$. Then $\mathrm{F}^\ell c$ is the coefficient of $\boldsymbol{x}^{p^\ell\alpha}$ in f. Since f is a polynomial, we may assume that $p^\ell\alpha \in \mathbb{N}^n$, hence $0 \leq v_p(p^\ell\alpha) = \ell + v_p(\alpha)$. We obtain

$$\nu(\ell+1,\alpha) = \min\{\ell+1+v_p(\alpha), \ell+1\} = \min\{v_p(p^\ell\alpha), \ell\} + 1.$$

Since K is perfect, F is an automorphism of R, hence c is divisible by $p^{\nu(\ell+1,\alpha)}$ if and only if $\mathrm{F}^{-\ell} c$ is divisible by $p^{\nu(\ell+1,\alpha)} = p^{\min\{v_p(p^\ell\alpha),\ell\}+1}$. □

The following lemma shows that the zeroness of a realization of a Witt-Jacobian differential in $\mathrm{E}^m_{\ell+1}$ is characterized by the $(\ell+1)$-degeneracy of the associated Witt-Jacobian polynomials.

Lemma 4.1.30. *Let $\ell \geq 0$, let $g_1, \ldots, g_m \in R[\boldsymbol{x}]$, and define*

$$\omega := \mathrm{d}\big(\mathrm{F}^{-\ell} g_1\big)^{p^\ell} \wedge \cdots \wedge \mathrm{d}\big(\mathrm{F}^{-\ell} g_m\big)^{p^\ell} \in \mathrm{E}^m.$$

Then we have $\omega \in \mathrm{Fil}^{\ell+1}\mathrm{E}^m$ if and only if $\mathrm{WJP}_{\ell+1,\boldsymbol{x}_I}(g_1, \ldots, g_m)$ is $(\ell+1)$-degenerate for all $I \in \binom{[n]}{m}$.

Proof. From the formula $\mathrm{d}\,\mathrm{F} = p\,\mathrm{F}\,\mathrm{d}$, we infer

$$\mathrm{F}^\ell\,\mathrm{d}\big(\mathrm{F}^{-\ell} g_i\big)^{p^\ell} = p^{-\ell}\,\mathrm{d}g_i^{p^\ell} = g_i^{p^\ell-1}\,\mathrm{d}g_i$$

for all $i \in [m]$, hence $\mathrm{F}^\ell\omega = (g_1 \cdots g_m)^{p^\ell} \cdot \mathrm{d}g_1 \wedge \cdots \wedge \mathrm{d}g_m$. A standard computation shows

$$\mathrm{d}g_1 \wedge \cdots \wedge \mathrm{d}g_m = \sum_I \big(\textstyle\prod_{j\in I} x_j\big) \cdot \det J_{x_I}(g_1, \ldots, g_m) \cdot \bigwedge_{j\in I} \mathrm{d}\log x_j,$$

where the sum is over all $I \in \binom{[n]}{m}$. This yields the unique representation

$$\omega = \sum_I \mathrm{F}^{-\ell} \operatorname{WJP}_{\ell+1,\boldsymbol{x}_I}(g_1, \ldots, g_m) \cdot \textstyle\bigwedge_{j \in I} \mathrm{d} \log x_j.$$

We have $\operatorname{Fil}^{\ell+1} \mathrm{E}^m = \bigoplus_{\alpha \in G} (\operatorname{Fil}^{\ell+1} \mathrm{E}^m)_\alpha = \bigoplus_{\alpha \in G} p^{\nu(\ell+1,\alpha)} (\mathrm{E}^m)_\alpha$ by Lemma 4.1.28, and for each $\alpha \in G$, the homogeneous part of ω of degree α has the unique representation

$$(\omega)_\alpha = \sum_I \big(\mathrm{F}^{-\ell} \operatorname{WJP}_{\ell+1,\boldsymbol{x}_I}(g_1, \ldots, g_m)\big)_\alpha \cdot \textstyle\bigwedge_{j \in I} \mathrm{d} \log x_j.$$

We conclude that $\omega \in \operatorname{Fil}^{\ell+1} \mathrm{E}^m$ if and only if $(\omega)_\alpha \in p^{\nu(\ell+1,\alpha)} (\mathrm{E}^m)_\alpha$ for all $\alpha \in G$ if and only if $p^{\nu(\ell+1,\alpha)}$ divides $\mathrm{F}^{-\ell} \operatorname{WJP}_{\ell+1,\boldsymbol{x}_I}(g_1, \ldots, g_m)$ for all $\alpha \in G$ and $I \in \binom{[n]}{m}$. By Lemma 4.1.29, this happens if and only if $\operatorname{WJP}_{\ell+1,\boldsymbol{x}_I}(g_1, \ldots, g_m)$ is $(\ell+1)$-degenerate for all $I \in \binom{[n]}{m}$. □

We conclude this section by pointing out a situation where degeneracy of polynomials is preserved under multiplication.

Lemma 4.1.31. *Let $g \in R[\boldsymbol{x}]$, let $\ell \geq 0$, and let $\alpha \in \mathbb{N}^n$ with $v_p(\alpha) \geq \ell$. Then g is $(\ell+1)$-degenerate if and only if $\boldsymbol{x}^\alpha \cdot g$ is $(\ell+1)$-degenerate.*

Proof. It suffices to show that $\min\{v_p(\beta), \ell\} = \min\{v_p(\alpha+\beta), \ell\}$ for all $\beta \in \mathbb{N}^n$. So let $\beta \in \mathbb{N}^n$. By assumption and Lemma A.6.4, we have $\min\{v_p(\beta), \ell\} = \min\{v_p(\alpha), v_p(\beta), \ell\} \leq \min\{v_p(\alpha+\beta), \ell\}$, with equality if $v_p(\alpha) \neq v_p(\beta)$. If $v_p(\alpha) = v_p(\beta)$, then $\min\{v_p(\beta), \ell\} = \min\{v_p(\alpha), \ell\} = \ell \geq \min\{v_p(\alpha+\beta), \ell\}$. □

4.2 Faithful Homomorphisms

Let $1 \leq r \leq n$, let K be a field, and let $K[\boldsymbol{x}] = K[x_1, \ldots, x_n]$ and $K[\boldsymbol{z}] = K[z_1, \ldots, z_r]$ be polynomial rings over K. In this section we investigate K-algebra homomorphisms $\varphi\colon K[\boldsymbol{x}] \to K[\boldsymbol{z}]$ that preserve the transcendence degree of given sets of polynomials. Since the expression "transcendence-degree-preserving" is a bit long, we will call these homomorphisms faithful.

Definition 4.2.1. Let $\varphi\colon K[\boldsymbol{x}] \to K[\boldsymbol{z}]$ be a K-algebra homomorphism and let $f_1, \ldots, f_m \in K[\boldsymbol{x}]$ be polynomials. If

$$\operatorname{trdeg}_K(\varphi(f_1), \ldots, \varphi(f_m)) = \operatorname{trdeg}_K(f_1, \ldots, f_m),$$

then φ is called **faithful to** $\{f_1, \ldots, f_m\}$.

Existence of faithful homomorphisms

The following theorem shows that faithful homomorphisms exist for arbitrary sets of polynomials, as long as the field is sufficiently large. Moreover, the faithful homomorphisms can even be chosen to be of degree 1.

Theorem 4.2.2. *Let K be an infinite field. Let $f_1, \dots, f_m \in K[\boldsymbol{x}]$ be polynomials such that $\operatorname{trdeg}_K(f_1, \dots, f_m) \leq r$. Then there exists a K-algebra homomorphism $\varphi\colon K[\boldsymbol{x}] \to K[\boldsymbol{z}] = K[z_1, \dots, z_r]$ of degree 1 which is faithful to $\{f_1, \dots, f_m\}$.*

Proof. After renumbering polynomials and variables, we may assume that $f_1, \dots, f_r, x_{r+1}, \dots, x_n$ are algebraically independent over K. Consequently, for $i \in [r]$, x_i is algebraically dependent on $f_1, \dots, f_r, x_{r+1}, \dots, x_n$, hence there exists a non-zero polynomial $G_i \in K[y_0, \boldsymbol{y}] = K[y_0, y_1, \dots, y_n]$ with $\deg_{y_0}(G_i) > 0$ such that

$$G_i(x_i, f_1, \dots, f_r, x_{r+1}, \dots, x_n) = 0. \tag{4.2.1}$$

Denote by $g_i \in K[\boldsymbol{y}]$ the (non-zero) leading term of G_i viewed as a polynomial in y_0 with coefficients in $K[\boldsymbol{y}]$. The algebraic independence of $f_1, \dots, f_r$, $x_{r+1}, \dots, x_n$ implies $g_i(f_1, \dots, f_r, x_{r+1}, \dots, x_n) \neq 0$. Since K is infinite, there exist $c_{r+1}, \dots, c_n \in K$ such that

$$\big(g_i(f_1, \dots, f_r, x_{r+1}, \dots, x_n)\big)(x_1, \dots, x_r, c_{r+1}, \dots, c_n) \neq 0 \tag{4.2.2}$$

for all $i \in [r]$ (by Lemma 2.5.1 or Theorem 2.5.4). Now define the K-algebra homomorphism

$$\varphi\colon K[\boldsymbol{x}] \to K[\boldsymbol{z}], \quad x_i \mapsto \begin{cases} z_i, & \text{if } i \in [r], \\ c_i, & \text{if } i \in [r+1, n]. \end{cases}$$

Applying φ to (4.2.1), we obtain $G_i(z_i, \varphi(f_1), \dots, \varphi(f_r), c_{r+1}, \dots, c_n) = 0$, and by (4.2.2) we have $G_i(y_0, \varphi(f_1), \dots, \varphi(f_r), c_{r+1}, \dots, c_n) \neq 0$ for all $i \in [r]$. This shows that z_i is algebraically dependent on $\varphi(f_1), \dots, \varphi(f_r)$ for all $i \in [r]$. It follows that $\operatorname{trdeg}_K(\varphi(f_1), \dots, \varphi(f_m)) = r = \operatorname{trdeg}_K(f_1, \dots, f_m)$, hence φ is faithful to $\{f_1, \dots, f_m\}$. □

Reducing the number of variables

The main motivation behind the definition of faithfulness is that faithful homomorphisms give rise to hitting sets as follows. Assume that we are given an m-variate arithmetic circuit F over $K[\boldsymbol{y}] = K[y_1, \dots, y_m]$ that

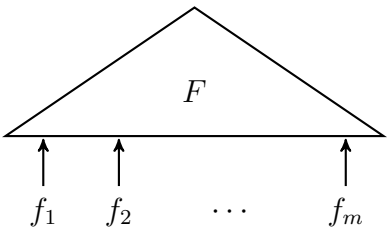


Figure 4.1: An arithmetic circuit F with subcircuits $f_1, \ldots, f_m$ computing the polynomial $F(f_1, \ldots, f_m)$.

takes arithmetic circuits $f_1, \ldots, f_m$ over $K[\boldsymbol{x}]$ as inputs. This composite circuit computes the polynomial $F(f_1, \ldots, f_m)$ which is an element of the K-subalgebra $K[f_1, \ldots, f_m]$ of $K[\boldsymbol{x}]$ (see Figure 4.1). Now let $\varphi\colon K[\boldsymbol{x}] \to K[\boldsymbol{z}] = K[z_1, \ldots, z_r]$ be a K-algebra homomorphism which is faithful to $\{f_1, \ldots, f_m\}$. If $F(f_1, \ldots, f_m) \neq 0$, then Lemma 4.2.7 implies that

$$F(\varphi(f_1), \ldots, \varphi(f_m)) = \varphi\big(F(f_1, \ldots, f_m)\big) \neq 0.$$

This means that φ reduces the number of variables from n to r, while preserving the non-zeroness of the circuit. If r is constant and φ can be constructed efficiently, then this yields a reduction to PIT of circuits with a constant number of variables. Finally, given that the transformed circuit has polynomial degree, the Combinatorial Nullstellensatz provides a polynomial-sized hitting set.

The following definition captures the circuit class for the composite circuits described above.

Definition 4.2.3. Let $\tau, D \geq 1$ and let $\mathcal{C} \subseteq K[\boldsymbol{x}]$ be a set of polynomials. Define the subset

$$\mathrm{Alg}_{\tau,D}\,\mathcal{C} := \left\{ F(f_1, \ldots, f_m) \;\middle|\; \begin{array}{l} m \geq 1,\ F \in K[y_1, \ldots, y_m],\ \deg(F) \leq D, \\ f_1, \ldots, f_m \in \mathcal{C},\ \mathrm{trdeg}_K(f_1, \ldots, f_m) \leq \tau \end{array} \right\}$$

of $K[\boldsymbol{x}]$.

The following theorem, proven below, describes the hitting set construction for $\mathrm{Alg}_{\tau,D}\,\mathcal{C}$. In Sections 4.2.1 to 4.2.5 we will explicitly construct families of faithful homomorphisms for several circuit classes $\mathcal{C}$ to which this theorem can be applied. A summary of those results will be given in Section 4.2.6.

Theorem 4.2.4. *Let $1 \leq r \leq n$, let $\tau, \delta, d, D \geq 1$, and let $\mathcal{C} \subseteq K[\boldsymbol{x}]$ be a set of polynomials of degree at most δ. Let I be an index set and let $\Phi_i\colon K[\boldsymbol{x}] \to K[\boldsymbol{z}]$ be a K-algebra homomorphism of degree at most d for all*

$i \in I$. Denote $\Phi_i^{(j)} := \Phi_i(x_j) \in K[\boldsymbol{z}]$ for all $i \in I$ and $j \in [n]$. Let $S \subseteq K$ be a set such that $|S| \geq \delta dD + 1$.

Assume that for all $f_1, \ldots, f_m \in \mathcal{C}$ with $\operatorname{trdeg}_K(f_1, \ldots, f_m) \leq \tau$ there exists $i \in I$ such that Φ_i is faithful to $\{f_1, \ldots, f_m\}$. Then

$$\mathcal{H} := \left\{ \left(\Phi_i^{(1)}(\boldsymbol{a}), \ldots, \Phi_i^{(n)}(\boldsymbol{a})\right) \mid i \in I \text{ and } \boldsymbol{a} \in S^r \right\} \subseteq K^n$$

is a hitting set for $\operatorname{Alg}_{\tau,D} \mathcal{C}$ with $|\mathcal{H}| \leq |I| \cdot |S|^r$.

The following lemma shows that the transcendence degree of a K-algebra is non-increasing under K-algebra homomorphisms.

Lemma 4.2.5. *Let A, B be K-algebras and let $\varphi\colon A \to B$ be a K-algebra homomorphism. Then $\operatorname{trdeg}_K(\varphi(A)) \leq \operatorname{trdeg}_K(A)$. If φ is injective, then $\operatorname{trdeg}_K(\varphi(A)) = \operatorname{trdeg}_K(A)$.*

Proof. Let $a_1, \ldots, a_r \in A$ such that $\varphi(a_1), \ldots, \varphi(a_r)$ are algebraically independent over K. For the sake of contradiction, assume that $a_1, \ldots, a_r$ are algebraically dependent over K. Then there exists a non-zero polynomial $F \in K[y_1, \ldots, y_r]$ such that $F(a_1, \ldots, a_r) = 0$. But this implies $0 = \varphi(F(a_1, \ldots, a_r)) = F(\varphi(a_1), \ldots, \varphi(a_r))$, a contradiction. Therefore $a_1, \ldots, a_r$ are algebraically independent over K.

Now let φ be injective and let $a_1, \ldots, a_r \in A$ be algebraically independent over K. For the sake of contradiction, assume that $\varphi(a_1), \ldots, \varphi(a_r)$ are algebraically dependent over K. Then there exists a non-zero polynomial $F \in K[y_1, \ldots, y_r]$ such that $F(\varphi(a_1), \ldots, \varphi(a_r)) = 0$. Hence, we have $\varphi(F(a_1, \ldots, a_r)) = 0$. Since φ is injective, this implies $F(a_1, \ldots, a_r) = 0$, a contradiction. Therefore $\varphi(a_1), \ldots, \varphi(a_r)$ are algebraically independent over K. □

The following lemma demonstrates that passing from an affine algebra to a quotient algebra modulo a non-zerodivisor strictly decreases the transcendence degree.

Lemma 4.2.6. *Let A be an affine K-algebra and let $g \in A \setminus \{0\}$ be a non-zerodivisor. Then $\operatorname{trdeg}_K(A/\langle g \rangle_A) \leq \operatorname{trdeg}_K(A) - 1$.*

Proof. The following argument is contained in the proof of [Kem11, Lemma 5.6]. Let $r := \operatorname{trdeg}_K(A) \in \mathbb{N}$ and assume that there exist $a_1, \ldots, a_r \in A$ such that $a_1 + \langle g \rangle, \ldots, a_r + \langle g \rangle$ are algebraically independent over K. Then $a_1, \ldots, a_r$ are also algebraically independent. By the definition of r, the elements $g, a_1, \ldots, a_r$ are algebraically dependent. Therefore, there exists a non-zero polynomial $F \in K[y_0, \boldsymbol{y}] = K[y_0, y_1, \ldots, y_r]$ such that $F(g, a_1, \ldots, a_r) =$

0. Since $a_1, \ldots, a_r$ are algebraically independent, we have $\delta := \deg_{y_0}(F) > 0$. Write $F = \sum_{i=0}^{\delta} f_i y_0^i$, where $f_i \in K[\boldsymbol{y}]$. Since g is a non-zerodivisor, we may assume that $f_0 \neq 0$. We have $f_0(a_1, \ldots, a_r) = -\sum_{i=1}^{\delta} f_i(a_1, \ldots, a_r) g^i \in \langle g \rangle$, therefore $f_0(a_1 + \langle g \rangle, \ldots, a_r + \langle g \rangle) = 0$, a contradiction. □

The following lemma is key to our hitting set construction, as it demonstrates that a homomorphism which is faithful to $\{f_1, \ldots, f_m\} \subset K[\boldsymbol{x}]$ preserves the non-zeroness of polynomials $F(f_1, \ldots, f_m)$ in the K-subalgebra $K[f_1, \ldots, f_m]$.

Lemma 4.2.7. *Let $\varphi\colon K[\boldsymbol{x}] \to K[\boldsymbol{z}]$ be a K-algebra homomorphism, let $f_1, \ldots, f_m \in K[\boldsymbol{x}]$ be polynomials and let $\varphi_A := \varphi|_A\colon A \to K[\boldsymbol{z}]$ be the restriction of φ to the K-subalgebra $A := K[f_1, \ldots, f_m] \subseteq K[\boldsymbol{x}]$. Then φ is faithful to $\{f_1, \ldots, f_m\}$ if and only if φ_A is injective.*

Proof. If φ_A is injective, then $\operatorname{trdeg}_K(\varphi(f_1), \ldots, \varphi(f_m)) = \operatorname{trdeg}_K(\varphi_A(A)) = \operatorname{trdeg}_K(A) = \operatorname{trdeg}_K(f_1, \ldots, f_m)$ by Lemmas 4.1.1 and 4.2.5, hence φ is faithful to $\{f_1, \ldots, f_m\}$.

Conversely, let φ be faithful to $\{f_1, \ldots, f_m\}$. For the sake of contradiction, assume that φ_A is not injective. Then there exists $g \in A \setminus \{0\}$ such that $\varphi_A(g) = 0$. Since $g \in \ker(\varphi_A)$, the K-algebra homomorhism $\overline{\varphi}_A\colon A/\langle g \rangle \to K[\boldsymbol{z}]$, $a + \langle g \rangle \mapsto \varphi_A(a)$ is well-defined, and φ_A factors as $\varphi_A = \overline{\varphi}_A \circ \eta$, where $\eta\colon A \twoheadrightarrow A/\langle g \rangle$ is the canonical surjection. We obtain

$$\begin{aligned}
\operatorname{trdeg}_K(f_1, \ldots, f_m) &= \operatorname{trdeg}_K(\varphi(f_1), \ldots, \varphi(f_m)) && \text{(by faithfulness of } \varphi) \\
&= \operatorname{trdeg}_K(\varphi_A(A)) && \text{(by Lemma 4.1.1)} \\
&= \operatorname{trdeg}_K(\overline{\varphi}_A(\eta(A))) \\
&\leq \operatorname{trdeg}_K(\eta(A)) && \text{(by Lemma 4.2.5)} \\
&= \operatorname{trdeg}_K(A/\langle g \rangle) \\
&\leq \operatorname{trdeg}_K(A) - 1 && \text{(by Lemma 4.2.6)} \\
&= \operatorname{trdeg}_K(f_1, \ldots, f_m) - 1 && \text{(by Lemma 4.1.1),}
\end{aligned}$$

a contradiction. Hence, φ_A is injective. □

Proof of Theorem 4.2.4. Let $f \in \operatorname{Alg}_{\tau,D} \mathcal{C}$ be a non-zero polynomial. Write $f = F(f_1, \ldots, f_m)$, where $F \in K[y_1, \ldots, y_m]$ is a polynomial with $\deg(F) \leq D$ and $f_1, \ldots, f_m \in \mathcal{C}$ are polynomials with $\operatorname{trdeg}_K(f_1, \ldots, f_m) \leq \tau$. We have $\deg(f) \leq \delta D$. By assumption, there exists $i \in I$ such that Φ_i is faithful to $\{f_1, \ldots, f_m\}$. Since $f \in K[f_1, \ldots, f_m]$, Lemma 4.2.7 implies $\Phi_i(f) \neq 0$. Now the assertion follows from Theorem 3.2.4. □

4.2.1 Linear Forms

Linear forms are situated where the theories of rank-preserving and faithful homomorphisms meet. The reason is that linear forms are algebraically independent if and only if they are linearly independent. This follows from the Jacobian Criterion, because the Jacobian matrix of linear forms is just the matrix of their coefficients. We rephrase Theorem 3.2.6 for faithful homomorphisms.

Theorem 4.2.8. *Let $1 \leq r \leq n$. For $c \in K$, let $\Phi_c \colon K[\boldsymbol{x}] \to K[\boldsymbol{z}]$ be defined as in* (3.2.1).

There exists an effectively computable $N \in \mathbb{N}$ with $N = \operatorname{poly}(n)$ such that for all N-subsets $S \subseteq K$ we have the following: For all linear forms $\ell_1, \ldots, \ell_m \in K[\boldsymbol{x}]_1$ of transcendence degree at most r, there exists $c \in S$ such that Φ_c is faithful to $\{\ell_1, \ldots, \ell_m\}$.

Proof. By Lemma 3.2.8 and Lemma 4.2.7, a graded K-algebra homomorphism $K[\boldsymbol{x}] \to K[\boldsymbol{z}]$ of degree 1 is rank-preserving for $\{\ell_1, \ldots, \ell_m\}$ if and only if it is faithful to $\{\ell_1, \ldots, \ell_m\}$. Therefore, this theorem is a direct consequence of Theorem 3.2.6. □

4.2.2 Monomials

In this section, we construct faithful homomorphisms for sets of monomials. Note that the homomorphism in the following theorem is toric, hence it is sparsity-preserving.

Theorem 4.2.9. *Let $1 \leq r \leq n$ and let $\delta \geq 1$. For $\lambda \in \mathbb{Z}$ and $q \geq 1$, define the K-algebra homomorphism*

$$\Phi_{\lambda,q} \colon K[\boldsymbol{x}] \to K[\boldsymbol{z}], \quad x_i \mapsto \prod_{j=1}^{r} z_j^{\lfloor \lambda^{(i-1)(j-1)} \rfloor_q}, \tag{4.2.3}$$

where $i \in [n]$.

There exists an effectively computable $N \in \mathbb{N}$ with $N = \operatorname{poly}\big(n, \log \delta\big)$ such that we have the following: For all monomials $f_1, \ldots, f_m \in K[\boldsymbol{x}]$ of degree at most δ and transcendence degree at most r, there exist $\lambda, q \in [N]$ such that $\Phi_{\lambda,q}$ is faithful to $\{f_1, \ldots, f_m\}$.

Proof. Using Corollary A.1.2 (b), the assertion follows from Lemma 4.2.11 below. □

Lemma 4.2.11 is based on the following characterization of algebraic independence of monomials (see also [Stu96, Lemma 4.1]). For the proof, it is convenient to introduce the following notation. For $\alpha \in \mathbb{Z}$, we set $\alpha^+ := \max\{\alpha, 0\} \in \mathbb{N}$ and $\alpha^- := \max\{-\alpha, 0\} \in \mathbb{N}$. For $\alpha \in \mathbb{Z}^n$, we define $\alpha^+ := (\alpha_1^+, \ldots, \alpha_n^+) \in \mathbb{N}^n$ and $\alpha^- := (\alpha_1^-, \ldots, \alpha_n^-) \in \mathbb{N}^n$. We have $\alpha = \alpha^+ - \alpha^-$.

Lemma 4.2.10. *Let $\alpha_1, \ldots, \alpha_m \in \mathbb{N}^n$. Then the terms $\boldsymbol{x}^{\alpha_1}, \ldots, \boldsymbol{x}^{\alpha_m}$ are algebraically independent over K if and only if $\alpha_1, \ldots, \alpha_m$ are $\mathbb{Z}$-linearly independent.*

Proof. Let $\alpha_1, \ldots, \alpha_m$ be $\mathbb{Z}$-linearly dependent. Then there exist integers $\lambda_1, \ldots, \lambda_m \in \mathbb{Z}$, not all zero, such that $\lambda_1\alpha_1 + \cdots + \lambda_m\alpha_m = 0$. This implies

$$(\boldsymbol{x}^{\alpha_1})^{\lambda_1^+} \cdots (\boldsymbol{x}^{\alpha_m})^{\lambda_m^+} = (\boldsymbol{x}^{\alpha_1})^{\lambda_1^-} \cdots (\boldsymbol{x}^{\alpha_m})^{\lambda_m^-},$$

hence $\boldsymbol{x}^{\alpha_1}, \ldots, \boldsymbol{x}^{\alpha_m}$ are algebraically dependent over K.

Conversely, let $\boldsymbol{x}^{\alpha_1}, \ldots, \boldsymbol{x}^{\alpha_m}$ be algebraically dependent over K. Then there exists a non-zero polynomial $F \in K[\boldsymbol{y}] = K[y_1, \ldots, y_m]$ such that $F(\boldsymbol{x}^{\alpha_1}, \ldots, \boldsymbol{x}^{\alpha_m}) = 0$. This means that there are two distinct terms $t_1 = \boldsymbol{y}^\lambda$ and $t_2 = \boldsymbol{y}^\mu$ (where $\lambda, \mu \in \mathbb{N}^m$) in the support of F such that

$$t_1(\boldsymbol{x}^{\alpha_1}, \ldots, \boldsymbol{x}^{\alpha_m}) = t_2(\boldsymbol{x}^{\alpha_1}, \ldots, \boldsymbol{x}^{\alpha_m}).$$

This implies $(\lambda_1 - \mu_1)\alpha_1 + \cdots + (\lambda_m - \mu_m)\alpha_m = 0$. Since $\lambda - \mu \neq 0$, it follows that $\alpha_1, \ldots, \alpha_m$ are $\mathbb{Z}$-linearly dependent. □

By Lemma 4.2.10, preserving the transcendence degree of monomials boils down to preserving the rank of their exponent vectors. For the latter, we can use Lemma 3.2.7. Since the resulting monomials would be of exponential degree, we will also reduce the transformed exponent vectors modulo various integers q.

Lemma 4.2.11. *Let $1 \leq r \leq n$ and let $\delta \geq 1$. For $\lambda \in \mathbb{Z}$ and $q \geq 1$, define $\Phi_{\lambda,q}$ as in (4.2.3). Let $\alpha_1, \ldots, \alpha_m \in \mathbb{N}^n$ such that $\boldsymbol{x}^{\alpha_1}, \ldots, \boldsymbol{x}^{\alpha_m}$ are of degree at most δ and transcendence degree at most r.*

Then there exists a set $B_1 \subset \mathbb{Z}$ with $|B_1| \leq \binom{r}{2}(n-1)$ satisfying the following property: For all $\lambda \in \mathbb{Z} \setminus B_1$ there exists a set $B_2 \subset \mathbb{P}$ with $|B_2| \leq r^2 n \log_2(r\delta(|\lambda| + 1))$ such that $\Phi_{\lambda,q}$ is faithful to $\{\boldsymbol{x}^{\alpha_1}, \ldots, \boldsymbol{x}^{\alpha_m}\}$ for all $q \in \mathbb{P} \setminus B_1$.

Proof. We may assume that $\boldsymbol{x}^{\alpha_1}, \ldots, \boldsymbol{x}^{\alpha_r}$ are algebraically independent over K (if the transcendence degree is less than r, we can append algebraically

independent variables). Denote by $A \in \mathbb{Z}^{r\times n}$ the matrix with rows $\alpha_1, \ldots, \alpha_r$. By Lemma 4.2.10, we have $\mathrm{rk}_{\mathbb{Q}}(A) = r$. By Lemma 3.2.7, there exists a set $B_1 \subset \mathbb{Z}$ with $|B_1| \leq \binom{r}{2}(n-1)$ such that $\mathrm{rk}_{\mathbb{Q}}(AV_\lambda) = r$ for all $\lambda \in \mathbb{Z} \setminus B_1$, where $V_\lambda := \left(\lambda^{(i-1)(j-1)}\right)_{i,j} \in \mathbb{Z}^{n\times r}$.

Let $\lambda \in \mathbb{Z} \setminus B_1$. Then we have $\det(AV_\lambda) \neq 0$. Let $B_2 \subset \mathbb{P}$ be the set of prime divisors of $\det(AV_\lambda)$. Using Hadamard's Inequality (see Lemma A.3.3) and standard properties of matrix and vector norms, we can estimate

$$\begin{aligned}|\det(AV_\lambda)| &\leq \prod_{j=1}^{r} \|Av_j\|_2 \leq \prod_{j=1}^{r} r^{1/2}\|A\|_\infty \|v_j\|_\infty \leq \prod_{j=1}^{r} r^{1/2}\delta|\lambda|^{(n-1)(j-1)} \\ &\leq r^{r/2}\delta^r|\lambda|^{(n-1)\binom{r}{2}},\end{aligned}$$

where $v_1, \ldots, v_r \in \mathbb{Z}^n$ denote the columns of V_λ. This implies that $|B_2| \leq r^2 n \log_2(r\delta(|\lambda|+1))$.

Let $q \in \mathbb{P} \setminus B_2$. Then we have $\det(AV_\lambda) \neq 0 \pmod q$. This implies that $\det(AV_{\lambda,q}) \neq 0$, where $V_{\lambda,q} := \left(\lfloor \lambda^{(i-1)(j-1)} \rfloor_q\right)_{i,j} \in \mathbb{N}^{n\times r}$. Denoting the rows of $AV_{\lambda,q}$ by $\beta_1, \ldots, \beta_r \in \mathbb{N}^r$, we see that $\Phi_{\lambda,q}(\boldsymbol{x}^{\alpha_i}) = \boldsymbol{z}^{\beta_i}$ for all $i \in [r]$. By Lemma 4.2.10, we conclude

$$\mathrm{trdeg}_K\left(\Phi_{\lambda,q}(\boldsymbol{x}^{\alpha_1}), \ldots, \Phi_{\lambda,q}(\boldsymbol{x}^{\alpha_r})\right) = r = \mathrm{trdeg}_K(\boldsymbol{x}^{\alpha_1}, \ldots, \boldsymbol{x}^{\alpha_m}),$$

hence $\Phi_{\lambda,q}$ is faithful to $\{\boldsymbol{x}^{\alpha_1}, \ldots, \boldsymbol{x}^{\alpha_m}\}$. □

4.2.3 Sparse Polynomials

We continue with the construction of faithful homomorphisms for sets of sparse polynomials. The construction works in arbitrary characteristic, but a better complexity bound can be established in the separable case (in characteristic zero or sufficiently large characteristic).

The following lemma gives a general recipe for obtaining faithful homomorphisms in the separable case and is based on the Jacobian Criterion. The lemma demonstrates that, in order to construct a faithful homomorphism for given polynomials $f_1, \ldots, f_m \in K[\boldsymbol{x}]$ of transcendence degree r, it is sufficient to find a point $\boldsymbol{b} \in K^n$ that preserves the rank of the Jacobian matrix $J_{\boldsymbol{x}}(f_1, \ldots, f_m)$ under substitution and a matrix $A \in K^{n\times r}$ that is rank-preserving for that matrix.

Lemma 4.2.12. *Let $1 \leq r \leq n$. Let $f_1, \ldots, f_m \in K[\boldsymbol{x}]$ be polynomials of transcendence degree at most r such that $K(\boldsymbol{x})$ is a separable extension of $K(f_1, \ldots, f_m)$. Let $A = (a_{i,j}) \in K^{n\times r}$ be a matrix and let $\boldsymbol{b} \in K^n$ be a point such that*

$$\mathrm{rk}_{K(\boldsymbol{x})}(J) = \mathrm{rk}_K(J_{\boldsymbol{b}} \cdot A),$$

where $J := J_{\boldsymbol{x}}(f_1, \ldots, f_m) \in K[\boldsymbol{x}]^{m \times n}$ *and* $J_{\boldsymbol{b}} := J|_{\boldsymbol{x}=\boldsymbol{b}} \in K^{m \times n}$. *Then the* K*-algebra homomorphism*

$$\varphi \colon K[\boldsymbol{x}] \to K[\boldsymbol{z}], \quad x_i \mapsto \left(\sum_{j=1}^{r} a_{i,j} z_j \right) + b_i, \tag{4.2.4}$$

where $i \in [n]$, *is faithful to* $\{f_1, \ldots, f_m\}$.

Proof. Set $\tau := \operatorname{trdeg}_K(f_1, \ldots, f_m) \in [0, r]$. By Theorem 4.1.12, we have $\tau = \operatorname{rk}_{K(\boldsymbol{x})}(J)$. By the chain rule, we can compute

$$J_{\boldsymbol{z}}(\varphi(f_1), \ldots, \varphi(f_m)) = \varphi(J) \cdot J_{\boldsymbol{z}}(\varphi(x_1), \ldots, \varphi(x_n)) = \varphi(J) \cdot A.$$

This implies $J_{\boldsymbol{z}}(\varphi(f_1), \ldots, \varphi(f_m))|_{\boldsymbol{z}=\boldsymbol{0}} = J_{\boldsymbol{b}} \cdot A$, therefore

$$\operatorname{rk}_{K(\boldsymbol{z})} J_{\boldsymbol{z}}(\varphi(f_1), \ldots, \varphi(f_m)) \geq \operatorname{rk}_K(J_{\boldsymbol{b}} \cdot A) = \tau.$$

By Theorem 4.1.12, we conclude $\operatorname{trdeg}_K(\varphi(f_1), \ldots, \varphi(f_m)) = \tau$, thus φ is faithful to $\{f_1, \ldots, f_m\}$. □

If we want to apply this lemma to sparse polynomials, we can use sparse PIT methods from Section 3.2.2 to find $\boldsymbol{b}$ and Lemma 3.2.7 to find A (see also Remark 4.2.18).

Here we give an alternative construction that works in arbitrary characteristic. In a way, it mimics the proof of Theorem 4.2.2, but is also taylored to suit Lemma 4.2.12. We will proceed step by step. We first define three homomorphisms in (4.2.5), (4.2.10), and (4.2.12). The final homomorphism, presented in Theorem 4.2.17, will then be the composition of those maps.

Eliminating variables

We start with the simplest of the three maps. Define the K-algebra homomorphism

$$\Psi \colon K[\boldsymbol{x}] \to K[\boldsymbol{z}], \quad x_i \mapsto \begin{cases} z_i, & \text{if } i \in [r], \\ 0, & \text{if } i \in [r+1, n]. \end{cases} \tag{4.2.5}$$

It will turn out that, after *shifting* and *mixing* the $\boldsymbol{x}$-variables appropriately, this projection is faithful to a given set of polynomials of transcendence degree at most r.

Mixing the variables

Now we will define a homomorphism that imitates the renumbering of variables that took place in the first step of the proof of Theorem 4.2.2. To this end, we will construct a matrix of univariate polynomials that interpolates the permutation matrices given by the renumberings. The matrix can also be used to obtain rank-preserving matrices.

Let $I = \{i_1 < \cdots < i_r\} \in \binom{[n]}{r}$ be an index set and let $[n] \setminus I = \{i_{r+1} < \cdots < i_n\}$ be its complement. Define the permutation $\pi_I \colon [n] \to [n]$, $i_j \mapsto j$ for $j \in [n]$. This assignment yields an injection $\binom{[n]}{r} \to \mathfrak{S}_n$, $I \mapsto \pi_I$ with the property $\pi_I(I) = [r]$.

We assume that K is sufficiently large, so that we can fix an injection

$$\binom{[n]}{r} \to K, \quad I \mapsto c_I \tag{4.2.6}$$

that assigns a constant $c_I \in K$ to each r-subset $I \subseteq [n]$.

For $i, j \in [n]$, let $a_{i,j} \in K[t]$ be the unique polynomial of degree $\binom{n}{r} - 1$ satisfying

$$a_{i,j}(c_I) = \delta_{\pi_I(i),j} \quad \text{for all } I \in \binom{[n]}{r}, \tag{4.2.7}$$

where $\delta_{i,j}$ denotes the Kronecker delta. This means that $\big(a_{i,j}(c_I)\big)_{i,j} \in K^{n\times n}$ is the permutation matrix given by π_I. In particular, we have $\det(a_{i,j}(c_I)) = \operatorname{sgn}(\pi_I) \in \{-1, 1\}$. The matrix $\big(a_{i,j}\big)_{i,j} \in K[t]^{n\times n}$ can be easily constructed by Lagrange interpolation as follows. For $I \in \binom{[n]}{r}$, define

$$\ell_I := \prod_{J \neq I} \frac{t - c_J}{c_I - c_J} \in K[t],$$

where the product is over all $J \in \binom{[n]}{r} \setminus \{I\}$. Then

$$a_{i,j} = \sum_I \delta_{\pi_I(i),j} \cdot \ell_I \in K[t] \tag{4.2.8}$$

for all $i, j \in [n]$, where the sum is over all $I \in \binom{[n]}{r}$.

The polynomials $a_{i,j}$ give rise to rank-preserving matrices. Compared with Lemma 3.2.7, this construction is less efficient, because the number of bad substitutions $c \in K$ can be exponential in r, but in applications where r is constant, its complexity is acceptable.

Lemma 4.2.13. *Let $1 \leq r \leq n$ and $m \geq 1$. Let $A \in K^{m\times n}$ be a matrix with $\operatorname{rk}_K(A) \leq r$. For $c \in K$, define $P_c := \big(a_{i,j}(c)\big)_{i,j} \in K^{n\times r}$. Then there exists a set $B \subseteq K$ with $|B| \leq r\binom{n}{r} - r$ such that*

$$\operatorname{rk}_K(AP_c) = \operatorname{rk}_K(A)$$

for all $c \in K \setminus B$.

Proof. Define $P := \big(a_{i,j}\big)_{i,j} \in K[t]^{n\times r}$. After removing unnecessary rows of A, we may assume $A \in K^{r\times n}$. Since $\rho := \operatorname{rk}(A) \le r$, there exists $I \in \binom{[n]}{r}$ such that $\operatorname{rk}_K(A_{[r],I}) = \rho$. Let $c_I \in K$ be defined as in (4.2.6). By (4.2.7), we get

$$AP_{c_I} = A \cdot \big(a_{i,j}(c_I)\big)_{i,j} = A \cdot \big(\delta_{\pi_I(i),j}\big)_{i,j} = A_{[r],I}.$$

This implies $\operatorname{rk}_{K(t)}(AP) = \operatorname{rk}_K(A_{[r],I}) = \rho$, thus there exists a submatrix $M \in K[t]^{\rho\times\rho}$ of AP such that $\operatorname{rk}_{K(t)}(M) = \rho$. Therefore, the polynomial $f := \det(M) \in K[t]$ is non-zero. Let $B := \mathcal{V}_K(f) \subseteq K$ be the set of zeros of f. Then we have $|B| \le \deg(f) \le \rho\binom{n}{r} - \rho \le r\binom{n}{r} - r$. Now let $c \in K \setminus B$. Then $\det(M|_{t=c}) = f(c) \neq 0$, thus $\operatorname{rk}_K(AP_c) = \rho$. □

Remark 4.2.14. A curious feature of the matrix $\big(a_{i,j}\big)_{i,j} \in K[t]^{n\times n}$ is the property $\sum_{j=1}^{n} a_{i,j} = 1$ for all $i \in [n]$, and likewise $\sum_{i=1}^{n} a_{i,j} = 1$ for all $j \in [n]$. This follows from the fact that those sums are polynomials of degree at most $\binom{n}{r} - 1$ and evaluate to 1 for all $\binom{n}{r}$ points c_I. We say that $\big(a_{i,j}\big)_{i,j}$ is a **generalized doubly stochastic** matrix.

Define the K-algebra homomorphism

$$\Xi\colon K[\boldsymbol{x}] \to K[\boldsymbol{x}, t], \quad x_i \mapsto \sum_{j=1}^{n} a_{i,j} \cdot x_j, \tag{4.2.9}$$

where $i \in [n]$. We have $\deg(\Xi(x_i)) = \binom{n}{r}$, $\deg_{\boldsymbol{x}}(\Xi(x_i)) = 1$, and $\deg_t(\Xi(x_i)) = \binom{n}{r} - 1$ for all $i \in [n]$. For $c \in K$, define the K-algebra homomorphism

$$\Xi_c\colon K[\boldsymbol{x}] \to K[\boldsymbol{x}], \quad x_i \mapsto \sum_{j=1}^{n} a_{i,j}(c) \cdot x_j, \tag{4.2.10}$$

where $i \in [n]$. We have $\Xi_c(f) = \Xi(f)|_{t=c}$ for all $f \in K[\boldsymbol{x}]$. By definition, Ξ_{c_I} is an automorphism sending the variables $\{x_i \mid i \in I\}$ to $\{x_1, \dots, x_r\}$ and sending the variables $\{x_i \mid i \in [n] \setminus I\}$ to $\{x_{r+1}, \dots, x_n\}$ (preserving the order of indices). In general, Ξ_c is an automorphism for almost all $c \in K$.

Corollary 4.2.15. *There exists a set $B \subseteq K$ with $|B| \le n\binom{n}{r} - n$ such that Ξ_c is an automorphism of $K[\boldsymbol{x}]$ for all $c \in K \setminus B$.*

Proof. Applying Lemma 4.2.13 with $r = n$ and $A = I_n$ yields a set $B \subseteq K$ with $|B| \le n\binom{n}{r} - n$ such that the matrix $P_c \in K^{n\times n}$ is invertible for all $c \in K \setminus B$, hence Ξ_c is an automorphism of $K[\boldsymbol{x}]$ for all $c \in K \setminus B$. □

Shifting the variables

Finally, we define a homomorphism that transforms the variables of a non-zero sparse polynomial $f \in K[\boldsymbol{x}]$ in such a way that it does not vanish at the origin $\mathbf{0} = (0, \ldots, 0) \in K^n$. For this we use sparse PIT methods from Section 3.2.2.

Let $D \geq 1$ and let $q \geq 1$. Define the K-algebra homomorphisms

$$\begin{aligned} \Lambda_D \colon K[\boldsymbol{x}] &\to K[\boldsymbol{x}, t], \quad x_i \mapsto x_i + t^{D^{i-1}}, \\ \Lambda_{D,q} \colon K[\boldsymbol{x}] &\to K[\boldsymbol{x}, t], \quad x_i \mapsto x_i + t^{\lfloor D^{i-1} \rfloor_q}, \end{aligned} \tag{4.2.11}$$

where $i \in [n]$. For $c \in K$, define the K-algebra homomorphism

$$\Lambda_{D,q,c} \colon K[\boldsymbol{x}] \to K[\boldsymbol{x}], \quad x_i \mapsto x_i + c^{\lfloor D^{i-1} \rfloor_q}, \tag{4.2.12}$$

where $i \in [n]$. We have $\Lambda_{D,q,c}(f) = \Lambda_{D,q}(f)|_{t=c}$ for all $f \in K[\boldsymbol{x}]$. The map $\Lambda_{D,q,c}$ is an automorphism of $K[\boldsymbol{x}]$ and, for almost all $D \geq 1$, $q \in \mathbb{P}$, and $c \in K$, it sends a non-zero polynomial to a polynomial that does not vanish at the origin. The following lemma bounds the number of bad choices for the parameters q and c.

Lemma 4.2.16. *Let $\delta, s \geq 1$ and let $D \geq \delta + 1$. Let $f \in K[\boldsymbol{x}]$ be a non-zero polynomial of sparsity at most s and degree at most δ.*

Then there exists a set $B_1 \subset \mathbb{P}$ of primes with $|B_1| \leq (s-1)\lfloor n \log_2 D \rfloor$ satisfying the following property: For all $q \in \mathbb{P} \setminus B_1$ there exists a set $B_2 \subseteq K$ with $|B_2| < \delta q$ such that

$$\big(\Lambda_{D,q,c}(f)\big)(\mathbf{0}) \neq 0$$

for all $c \in K \setminus B_2$.

Proof. Comparing (4.2.11) with (3.2.2), we see that Lemma 3.2.10 provides a set $B_1 \subset \mathbb{P}$ of primes with $|B_1| \leq (s-1)\lfloor n \log_2 D \rfloor$ such that the polynomial $g_q := \Lambda_{D,q}(f)|_{\boldsymbol{x}=\mathbf{0}} \in K[t]$ is non-zero for all $q \in \mathbb{P} \setminus B_1$. Let $q \in \mathbb{P} \setminus B_1$, and let $B_2 := \mathcal{V}_K(g_q) \subseteq K$ be the set of zeros of g_q. Then $|B_2| \leq \deg(g_q) < \delta q$ and $\big(\Lambda_{D,q,c}(f)\big)(\mathbf{0}) = g_q(c) \neq 0$ for all $c \in K \setminus B_2$. □

The faithful homomorphism

Now we can state the main theorem of this section. Note that the homomorphism in this theorem satisfies $\Phi_{D,q,\boldsymbol{c}} = \Psi \circ \Xi_{c_1} \circ \Lambda_{D,q,c_2}$ for all $D, q \geq 1$ and $\boldsymbol{c} \in K^2$.

Theorem 4.2.17. *Let $1 \leq r \leq n$ and let $s, \delta \geq 1$. For $D, q \geq 1$ and $\boldsymbol{c} \in K^2$, define the K-algebra homomorphism*

$$\Phi_{D,q,\boldsymbol{c}} \colon K[\boldsymbol{x}] \to K[\boldsymbol{z}], \quad x_i \mapsto \left(\sum_{j=1}^{r} a_{i,j}(c_1) \cdot z_j \right) + c_2^{\lfloor D^{i-1} \rfloor_q}, \tag{4.2.13}$$

where $i \in [n]$ and $a_{i,j} \in K[t]$ are defined as in (4.2.8).

(a) Let $\operatorname{char}(K)$ be arbitrary. Set $D := \delta^r + 1$. Then there exists an effectively computable $N \in \mathbb{N}$ with $N = \operatorname{poly}\big(n^{\delta^r}, n^{r^2}, \delta^r\big)$ such that for all N-subsets $S \subseteq K$ we have the following: For all polynomials $f_1, \ldots, f_m \in K[\boldsymbol{x}]$ of degree at most δ and transcendence degree at most r, there exist $q \in [N]$ and $\boldsymbol{c} \in S^2$ such that $\Phi_{D,q,\boldsymbol{c}}$ is faithful to $\{f_1, \ldots, f_m\}$.

(b) Let $\operatorname{char}(K) = 0$ or $\operatorname{char}(K) > \delta^r$. Set $D := \delta r + 1$. Then there exists an effectively computable $N \in \mathbb{N}$ with $N = \operatorname{poly}\big((ns)^r, \delta\big)$ such that for all N-subsets $S \subseteq K$ we have the following: For all polynomials $f_1, \ldots, f_m \in K[\boldsymbol{x}]$ of sparsity at most s, degree at most δ, and transcendence degree at most r, there exist $q \in [N]$ and $\boldsymbol{c} \in S^2$ such that $\Phi_{D,q,\boldsymbol{c}}$ is faithful to $\{f_1, \ldots, f_m\}$.

Proof. Using Corollary A.1.2 (b), the claims (a) and (b) follow from Lemma 4.2.19 and Lemma 4.2.20 below, respectively. □

Remark 4.2.18. Part (b) of Theorem 4.2.17 can also be proven using the K-algebra homomorphism defined by

$$\Phi_{D,q,\boldsymbol{c}} \colon K[\boldsymbol{x}] \to K[\boldsymbol{z}], \quad x_i \mapsto \left(\sum_{j=1}^{r} c_1^{(i-1)(j-1)} \cdot z_j \right) + c_2^{\lfloor D^{i-1} \rfloor_q} \tag{4.2.14}$$

for $D, q \geq 1$ and $\boldsymbol{c} \in K^2$ (cf. [BMS11] for a similar construction). We were, however, unable to deduce (a) for that homomorphism.

The following lemma implies part (a) of Theorem 4.2.17. It is proven along the lines of the proof of Theorem 4.2.2. For bounding the degrees of annihilating polynomials, we invoke Perron's Theorem (Theorem 4.1.4).

Lemma 4.2.19. *Let $1 \leq r \leq n$ and let $\delta \geq 1$. Let $D \geq \delta^r + 1$ and, for $q \geq 1$ and $\boldsymbol{c} \in K^2$, let $\Phi_{D,q,\boldsymbol{c}}$ be defined as in* (4.2.13). *Let $f_1, \ldots, f_m \in K[\boldsymbol{x}]$ be polynomials of degree at most δ and transcendence degree at most r.*

Then there exists a set $B_{2,1} \subset \mathbb{P}$ of primes with $|B_{2,1}| < rn\binom{n+\delta^r}{\delta^r} \log_2 D$ satisfying the following property: For all $q \in \mathbb{P} \setminus B_{2,1}$ there exists a set $B_{2,2} \subseteq K$ with $|B_{2,2}| < r\delta^r q$ such that for all $c_2 \in K \setminus B_{2,2}$ there exists a set $B_1 \subseteq K$ with $|B_1| < r\delta^r \binom{n}{r}^r$ such that $\Phi_{D,q,\boldsymbol{c}}$ is faithful to $\{f_1, \ldots, f_m\}$ for all $c_1 \in K \setminus B_1$.

Proof. We may assume that $f_1, \dots, f_r$ are algebraically independent over K (if the transcendence degree is less than r, we can append algebraically independent variables). Let $I = \{i_1 < \cdots < i_r\} \in \binom{[n]}{r}$ be an index set with complement $[n] \setminus I = \{i_{r+1} < \cdots < i_n\}$ such that $f_1, \dots, f_r, x_{i_{r+1}}, \dots, x_{i_n}$ are algebraically independent over K. Consequently, for $j \in [r]$, x_{i_j} is algebraically dependent on $f_1, \dots, f_r, x_{i_{r+1}}, \dots, x_{i_n}$. Denote $w := (1, \delta, \dots, \delta, 1, \dots, 1) \in \mathbb{N}_{>0}^{n+1}$, where δ appears in r slots. By Theorem 4.1.4, there exists a non-zero polynomial $G_j \in K[y_0, \boldsymbol{y}] = K[y_0, y_1, \dots, y_n]$ such that $\deg_{y_0} > 0$, $\deg_w(G_j) \leq \delta^r$ and

$$G_j(x_{i_j}, f_1, \dots, f_r, x_{i_{r+1}}, \dots, x_{i_n}) = 0. \tag{4.2.15}$$

Denote by $g_j \in K[\boldsymbol{y}]$ the (non-zero) leading coefficient of G_j viewed as a polynomial in y_0 with coefficients in $K[\boldsymbol{y}]$. Since $f_1, \dots, f_r, x_{i_{r+1}}, \dots, x_{i_n}$ are algebraically independent, the polynomial

$$g_j' := g_j(f_1, \dots, f_r, x_{i_{r+1}}, \dots, x_{i_n}) \in K[\boldsymbol{x}]$$

is non-zero. We have $\deg(g_j') \leq \deg_w(g_j) \leq \delta^r$, and this implies the bound $\operatorname{sp}(g_j') \leq \binom{n+\delta^r}{\delta^r}$. Applying Lemma 4.2.16 to g_j' provides a set $B_{2,1,j} \subset \mathbb{P}$ of primes with $|B_{2,1,j}| < n\binom{n+\delta^r}{\delta^r} \log_2 D$. Set $B_{2,1} := B_{2,1,1} \cup \cdots \cup B_{2,1,r}$ and let $q \in \mathbb{P} \setminus B_{2,1}$. For $j \in [r]$, let $B_{2,2,j} \subseteq K$ be the set with $|B_{2,2,j}| < \delta^r q$ provided by Lemma 4.2.16 applied to g_j'. Set $B_{2,2} := B_{2,2,1} \cup \cdots \cup B_{2,2,r}$ and let $c_2 \in K \setminus B_{2,2}$. Then we have $\big(\Lambda_{D,q,c_2}(g_j')\big)(\mathbf{0}) \neq 0$ for all $j \in [r]$.

Next we want to show that $\Phi_{D,q,(c_I,c_2)} = \Psi \circ \Xi_{c_I} \circ \Lambda_{D,q,c_2}$ is faithful to $\{f_1, \dots, f_r\}$. Denote $\boldsymbol{f} = (f_1, \dots, f_r)$ and $e_j := \lfloor D^{i_j - 1} \rfloor_q$ for all $j \in [n]$. Now let $j \in [r]$. Applying $\Psi \circ \Xi_{c_I} \circ \Lambda_{D,q,c_2}$ to (4.2.15) yields

$$\begin{aligned} 0 &= \Psi\Big(G_j\big(x_j + c_2^{e_j}, (\Xi_{c_I} \circ \Lambda_{D,q,c_2})(\boldsymbol{f}), x_{r+1} + c_2^{e_{r+1}}, \dots, x_n + c_2^{e_n}\big)\Big) \\ &= G_j\big(z_j + c_2^{e_j}, (\Psi \circ \Xi_{c_I} \circ \Lambda_{D,q,c_2})(\boldsymbol{f}), c_2^{e_{r+1}}, \dots, c_2^{e_n}\big). \end{aligned} \tag{4.2.16}$$

On the other hand, we have

$$G_j\big(y_0, (\Psi \circ \Xi_{c_I} \circ \Lambda_{D,q,c_2})(\boldsymbol{f}), c_2^{e_{r+1}}, \dots, c_2^{e_n}\big) \neq 0, \tag{4.2.17}$$

because $(\Psi \circ \Xi_{c_I} \circ \Lambda_{D,q,c_2})(g_j') \neq 0$. The latter follows from $\big(\Lambda_{D,q,c_2}(g_j')\big)(\mathbf{0}) \neq 0$, because $\big((\Psi \circ \Xi_{c_I})(x_i)\big)(\mathbf{0}) = 0$ for all $i \in [n]$. Equations (4.2.16) and (4.2.17) show that z_j is algebraically dependent on

$$(\Psi \circ \Xi_{c_I} \circ \Lambda_{D,q,c_2})(f_1), \dots, (\Psi \circ \Xi_{c_I} \circ \Lambda_{D,q,c_2})(f_r)$$

for all $j \in [r]$, hence $\Psi \circ \Xi_{c_I} \circ \Lambda_{D,q,c_2}$ is faithful to $\{f_1, \dots, f_r\}$.

It remains to show that $\Phi_{D,q,(c,c_2)} = \Psi \circ \Xi_c \circ \Lambda_{D,q,c_2}$ is faithful to $\{f_1, \ldots, f_r\}$ for almost all $c \in K$. To this end, for $i \in [r]$, define

$$f_i' := \big((\Xi \circ \Lambda_{D,q,c_2})(f_i)\big)(\boldsymbol{z}, \boldsymbol{0}, t) \in K[\boldsymbol{z}, t],$$

where $\boldsymbol{0} = (0, \ldots, 0) \in K^{n-r}$. We first want to show that $f_1', \ldots, f_r', t$ are algebraically independent over K, so assume for the sake of contradiction that they are algebraically dependent. Then there exists a non-zero polynomial $H \in K[y_0, \boldsymbol{y}] = K[y_0, y_1, \ldots, y_r]$ such that $H(t, f_1', \ldots, f_r') = 0$. Since $t - c_I \neq 0$, we may assume that $y_0 - c_I$ does not divide H. Therefore, the polynomial $H' := H(c_I, \boldsymbol{y}) \in K[\boldsymbol{y}]$ is non-zero. We have

$$H'\big(f_1'(\boldsymbol{z}, c_I), \ldots, f_r'(\boldsymbol{z}, c_I)\big) = \big(H(t, f_1', \ldots, f_r')\big)(\boldsymbol{z}, c_I) = 0,$$

hence $f_1'(\boldsymbol{z}, c_I), \ldots, f_r'(\boldsymbol{z}, c_I)$ are algebraically dependent. Since $f_i'(\boldsymbol{z}, c_I) = (\Psi \circ \Xi_{c_I} \circ \Lambda_{D,q,c_2})(f_i)$ for all $i \in [r]$, this is a contradiction to the preceding paragraph. Therefore $f_1', \ldots, f_r', t_1$ are algebraically independent. Now we can proceed as above. For $j \in [r]$, z_j is algebraically dependent on $f_1', \ldots, f_r', t$. Denote $w := (1, d, \ldots, d, 1) \in \mathbb{N}_{>0}^{r+2}$, where $d := \delta\binom{n}{r}$ appears in r slots. Note that $\deg(f_i') \leq d$ for all $i \in [r]$. By Theorem 4.1.4, there exists a non-zero polynomial $H_j \in K[y_0, \boldsymbol{y}] = K[y_0, y_1, \ldots, y_{r+1}]$ such that $\deg_{y_0}(H_j) > 0$, $\deg_w(H_j) \leq d^r$ and $H_j(z_j, f_1', \ldots, f_r', t) = 0$. Denote by $h_j \in K[\boldsymbol{y}]$ the (non-zero) leading coefficient of H_j viewed as a polynomial in y_0 with coefficients in $K[\boldsymbol{y}]$. Since $f_1', \ldots, f_r', t$ are algebraically independent, the polynomial $h_j' := h_j(f_1', \ldots, f_r', t) \in K[\boldsymbol{z}, t]$ is non-zero. Let $B_{1,j} \subseteq K$ be the set of all $c \in K$ such that $h_j'(\boldsymbol{z}, c) = 0$. Then $|B_{1,j}| \leq \deg_t(h_j') \leq \deg_w(h_j) \leq d^r = \delta^r\binom{n}{r}^r$. Set $B_1 := B_{1,1} \cup \cdots \cup B_{1,r}$, and let $c_1 \in K \setminus B_1$. Then we have

$$H_j\big(z_j, (\Psi \circ \Xi_{c_1} \circ \Lambda_{D,q,c_2})(\boldsymbol{f}), c_1\big) = \big(H_j(z_j, f_1', \ldots, f_r', t)\big)(\boldsymbol{z}, c_1) = 0,$$

but $H_j\big(y_0, (\Psi \circ \Xi_{c_1} \circ \Lambda_{D,q,c_2})(\boldsymbol{f}), c_1\big) \neq 0$. This shows that, for all $j \in [r]$, z_j is algebraically dependent on $(\Phi_{D,q,\boldsymbol{c}})(f_1), \ldots, (\Phi_{D,q,\boldsymbol{c}})(f_r)$, where $\boldsymbol{c} := (c_1, c_2)$. Therefore $\Phi_{D,q,\boldsymbol{c}}$ is faithful to $\{f_1, \ldots, f_m\}$. □

The following lemma proves part (b), the separable case, of Theorem 4.2.17. It is based on Lemma 4.2.12 which in turn relies on the Jacobian Criterion.

Lemma 4.2.20. *Let $1 \leq r \leq n$ and let $\delta, s \geq 1$. Assume that $\mathrm{char}(K) = 0$ or $\mathrm{char}(K) > \delta^r$. Let $D \geq \delta r + 1$ and, for $q \geq 1$ and $\boldsymbol{c} \in K^2$, let $\Phi_{D,q,\boldsymbol{c}}$ be defined as in (4.2.13). Let $f_1, \ldots, f_m \in K[\boldsymbol{x}]$ be polynomials of sparsity at most s, degree at most δ, and transcendence degree at most r.*

Then there exists a set $B_{2,1} \subset \mathbb{P}$ of primes with $|B_{2,1}| < r!s^r n \log_2 D$ satisfying the following property: For all $q \in \mathbb{P} \setminus B_{2,1}$ there exists a set $B_{2,2} \subseteq K$ with $|B_{2,2}| < r\delta q$ such that for all $c_2 \in K \setminus B_{2,2}$ there exists a set $B_1 \subseteq K$ with $|B_1| < r\binom{n}{r}$ such that $\Phi_{D,q,\boldsymbol{c}}$ is faithful to $\{f_1, \ldots, f_m\}$ for all $c_1 \in K \setminus B_1$.

Proof. Denote $J := J_{\boldsymbol{x}}(f_1, \ldots, f_m) \in K[\boldsymbol{x}]^{m \times n}$. By Lemma A.5.2 and Theorem 4.1.12, there exists a submatrix $M \in K[\boldsymbol{x}]^{\tau \times \tau}$ of J such that $g := \det(M) \in K[\boldsymbol{x}]$ is non-zero, where $\tau := \operatorname{trdeg}_K(f_1, \ldots, f_m) \in [0, r]$. We have $\deg(g) \leq r\delta$ and $\operatorname{sp}(g) \leq r!s^r$. Applying Lemma 4.2.16 to g provides a set $B_{2,1} \subset \mathbb{P}$ of primes with $|B_{2,1}| < r!s^r n \log_2 D$. Let $q \in \mathbb{P} \setminus B_{2,1}$, and let $B_{2,2} \subseteq K$ with $|B_{2,2}| < r\delta q$ be the corresponding set provided by Lemma 4.2.16. Let $c_2 \in K \setminus B_{2,2}$. Then we have $\big(\Lambda_{D,q,c_2}(g)\big)(\boldsymbol{0}) \neq 0$. This implies $\operatorname{rk}_K(J_{\boldsymbol{b}}) = \tau$, where

$$\boldsymbol{b} := \big(c_2^{\lfloor D^0 \rfloor_q}, c_2^{\lfloor D^1 \rfloor_q}, \ldots, c_2^{\lfloor D^{n-1} \rfloor_q}\big) \in K^n$$

and $J_{\boldsymbol{b}} := J|_{\boldsymbol{x}=\boldsymbol{b}} \in K^{m \times n}$. By Lemma 4.2.13, there exists a set $B_1 \subseteq K$ with $|B_1| < r\binom{n}{r}$ such that $\operatorname{rk}_K(J_{\boldsymbol{b}} \cdot P_{c_1}) = \tau$ for all $c_1 \in K \setminus B_1$, where $P_{c_1} := \big(a_{i,j}(c_1)\big)_{i,j} \in K^{n \times r}$. With Lemma 4.2.12 we conclude that $\Phi_{D,q,\boldsymbol{c}}$ is faithful to $\{f_1, \ldots, f_m\}$ for all $c_1 \in K \setminus B_1$. □

4.2.4 Log-Sparse Polynomials in Positive Characteristic

In this section we construct faithful homomorphisms for sets of sparse polynomials in small positive characteristic. The construction is based on the Witt-Jacobian Criterion (see Section 4.1.3). Let p be a prime and let K be an algebraic extension of $\mathbb{F}_p$.

Theorem 4.2.21. *Let $1 \leq r \leq n$ and let $\delta, s \geq 1$. Set $D := \delta^r + 1$. For $I = \{i_1 < \cdots < i_r\} \in \binom{[n]}{r}$ with complement $[n] \setminus I = \{i_{r+1} < \cdots < i_n\}$, $q \geq 1$, and $c \in K$, define the K-algebra homomorphism*

$$\Phi_{I,q,c} \colon K[\boldsymbol{x}] \to K[\boldsymbol{z}], \quad x_{i_j} \mapsto \begin{cases} z_j, & \text{if } j \in [r], \\ c^{\lfloor D^{j-r-1} \rfloor_q}, & \text{if } j \in [r+1, n]. \end{cases} \tag{4.2.18}$$

There exists an effectively computable $N \in \mathbb{N}$ with

$$N = \operatorname{poly}\big(n, \delta^{r^2 s}, r^r, s^{rs}\big)$$

such that for all N-subsets $S \subseteq K$ we have the following: For all polynomials $f_1, \ldots, f_m \in K[\boldsymbol{x}]$ of sparsity at most s, degree at most δ, and transcendence degree at most r, there exist $I \in \binom{[n]}{r}$, $q \in [N]$, and $c \in S$ such that $\Phi_{I,q,\boldsymbol{c}}$ is faithful to $\{f_1, \ldots, f_m\}$.

Proof. Using Corollary A.1.2 (b), the assertion follows from Lemma 4.2.23 below. □

In the proof of the theorem, we switch to the ring $R = \mathrm{W}(K)$ of Witt vectors of K. Recall that, since K is perfect, we may use the identifications $R/\langle p\rangle_R = K$ and $R[\boldsymbol{x}]/\langle p\rangle_{R[\boldsymbol{x}]} = K[\boldsymbol{x}]$. For a subset $B \subseteq R$, we denote $B/\langle p\rangle_R := \{b + \langle p\rangle_R \mid b \in B\} \subseteq K$. The following lemma shows how to preserve non-degeneracy of sparse polynomials over R under substitution. The proof works by reduction to sparse PIT over K.

Lemma 4.2.22. *Let $\ell \geq 0$, let $\delta, s \geq 1$, and let $D \geq \delta + 1$. Let $I = \{i_1 < \cdots < i_r\} \in \binom{[n]}{r}$ be an index set with complement $[n] \setminus I = \{i_{r+1} < \cdots < i_n\}$. For $q \geq 1$ and $c \in R$, define the R-algebra homomorphism*

$$\Phi_{I,q,c}\colon R[\boldsymbol{x}] \to R[\boldsymbol{z}], \quad x_{i_j} \mapsto \begin{cases} z_j, & \text{if } j \in [r], \\ c^{\lfloor D^{j-r-1}\rfloor_q}, & \text{if } j \in [r+1, n]. \end{cases} \tag{4.2.19}$$

Let $g \in R[\boldsymbol{x}]$ be a polynomial of sparsity at most s and degree at most δ which is not $(\ell+1)$-degenerate.

Then there exists a set $B_1 \subset \mathbb{P}$ of primes with $|B_1| \leq (s-1)\lfloor (n-r)\log_2 D\rfloor$ satisfying the following property: For all $q \in \mathbb{P} \setminus B_1$ there exists a set $B_2 \subseteq R$ with $|B_2/\langle p\rangle_R| < \delta q$ such that $\Phi_{I,q,c}(g)$ is not $(\ell+1)$-degenerate for all $c \in R \setminus B_2$.

Proof. Write $g = \sum_{\beta\in\mathbb{N}^r} g_\beta \boldsymbol{x}_I^\beta$ with $g_\beta \in R[\boldsymbol{x}_{[n]\setminus I}]$. Since g is not $(\ell+1)$-degenerate, there exists $\alpha \in \mathbb{N}^n$ such that the coefficient $c_\alpha \in R$ of $\boldsymbol{x}^\alpha$ in g is not divisible by $p^{\min\{v_p(\alpha),\ell\}+1}$. Let $\alpha' \in \mathbb{N}^r$ be the components of α indexed by I, and let $\alpha'' \in \mathbb{N}^{n-r}$ be the components of α indexed by $[n] \setminus I$. The polynomial $g_{\alpha'}$ is not divisible by $p^{\min\{v_p(\alpha),\ell\}+1}$, because c_α appears as the coefficient of $\boldsymbol{x}_{[n]\setminus I}^{\alpha''}$.

If we have $q \geq 1$ and $c \in R$ such that $\Phi_{I,q,c}(g_{\alpha'})$ is not divisible by $p^{\min\{v_p(\alpha),\ell\}+1}$, then $\Phi_{I,q,c}(g_{\alpha'})$ cannot be divisible by the possibly higher power $p^{\min\{v_p(\alpha'),\ell\}+1}$. This means that $\Phi_{I,q,c}(g)$ is not $(\ell+1)$-degenerate, because $\Phi_{I,q,c}(g_{\alpha'})$ appears as the coefficient of $\boldsymbol{z}^{\alpha'}$.

Now write $g_{\alpha'} = p^e h$, where $0 \leq e \leq \min\{v_p(\alpha), \ell\}$ and $h \in R[\boldsymbol{x}_{[n]\setminus I}]$ is not divisible by p. We have $\mathrm{sp}(h) \leq s$ and $\deg(h) \leq \delta$. If we have $q \geq 1$ and $c \in R$ such that $\Phi_{I,q,c}(h) \neq 0$ in $R/\langle p\rangle_R$, then $\Phi_{I,q,c}(g_{\alpha'})$ is not divisible by $p^{\min\{v_p(\alpha),\ell\}+1}$, as desired. Since $R/\langle p\rangle_R \cong K$ is a field, the assertion follows from Lemma 4.2.16. □

The following lemma constitutes the proof of Theorem 4.2.21. By the explicit Witt-Jacobian criterion, preserving the transcendence degree of polynomials over K boils down to preserving the non-degeneracy of an associated

Witt-Jacobian polynomial over R. For the latter, we may use Lemma 4.2.22. Unfortunately, due to the extra leading factors of the Witt-Jacobian polynomial, its sparsity is exponential in the sparsity of the given polynomials.

Lemma 4.2.23. *Let $1 \leq r \leq n$, let $\delta, s \geq 1$, and let $D \geq r\delta^{r+1} + 1$. For $I \in \binom{[n]}{r}$, $q \geq 1$, and $c \in K$, let $\Phi_{I,q,c} \colon K[\boldsymbol{x}] \to K[\boldsymbol{z}]$ be defined as in* (4.2.18)*. Let $f_1, \ldots, f_m \in K[\boldsymbol{x}]$ be polynomials of sparsity at most s, degree at most δ, and transcendence degree at most r.*

Then there exist $I \in \binom{[n]}{r}$ and a set $B_1 \subset \mathbb{P}$ of primes with $|B_1| < (s+\delta^r)^{rs} r! s^r (n-r) \log_2 D$ satisfying the following property: For all $q \in \mathbb{P} \setminus B_1$ there exists a set $B_2 \subseteq K$ with $|B_2| < r\delta^{r+1} q$ such that $\Phi_{I,q,c}$ is faithful to $\{f_1, \ldots, f_m\}$ for all $c \in K \setminus B_2$.

Proof. We may assume that $f_1, \ldots, f_r$ are algebraically independent over K (if the transcendence degree is less than r, we can append algebraically independent variables). By lifting the coefficients of $f_1, \ldots, f_r$, we obtain polynomials $g_1, \ldots, g_r \in R[\boldsymbol{x}]$ of sparsity at most s such that $f_i = g_i \pmod{\langle p \rangle_{R[\boldsymbol{x}]}}$ for all $i \in [r]$. Set $\ell := \lfloor r \log_p \delta \rfloor \in \mathbb{N}$. By Lemma 4.1.17, we have

$$\ell \geq \log_p [K(\boldsymbol{x}) : K(f_1, \ldots, f_r)]_{\mathrm{insep}}.$$

By Theorem 4.1.24, there exists $I \in \binom{[n]}{r}$ such that the polynomial $g := \mathrm{WJP}_{\ell+1, \boldsymbol{x}_I}(g_1, \ldots, g_r) \in R[\boldsymbol{x}]$ is not $(\ell+1)$-degenerate. We have $\deg(g) \leq r\delta(p^\ell - 1) + r + r(\delta - 1) \leq r\delta p^\ell \leq r\delta^{r+1}$ and

$$\mathrm{sp}(g) \leq \binom{s + (p^\ell - 1) - 1}{s - 1}^r \cdot r! s^r \leq \left(s + \delta^r\right)^{rs} \cdot r! s^r.$$

Applying Lemma 4.2.22 to g provides a set $B_1 \subset \mathbb{P}$ of primes with $|B_1| < (s+\delta^r)^{rs} r! s^r (n-r) \log_2 D$. Let $q \in \mathbb{P} \setminus B_1$ and let $B_2' \subseteq R$ be the corresponding set provided by Lemma 4.2.22. Set $B_2 := B_2' / \langle p \rangle_R \subseteq K$. Then we have $|B_2| < r\delta^{r+1} q$. Now let $c \in K \setminus B_2$ and let $c' \in R \setminus B_2'$ such that $c = c' \pmod{\langle p \rangle_R}$. By Lemma 4.2.22, the polynomial $\Phi'_{I,q,c'}(g)$ is not $(\ell+1)$-degenerate, where $\Phi'_{I,q,c'} \colon R[\boldsymbol{x}] \to R[\boldsymbol{z}]$ is defined as in (4.2.19). Therefore, the Witt-Jacobian polynomial

$$\mathrm{WJP}_{\ell+1, \boldsymbol{z}}\left(\Phi'_{I,q,c'}(g_1), \ldots, \Phi'_{I,q,c'}(g_r)\right) = \Phi'_{I,q,c'}(g)$$

is not $(\ell+1)$-degenerate. Since we have

$$\ell \geq \log_p [K(\boldsymbol{z}) : K(\Phi_{I,q,c}(f_1), \ldots, \Phi_{I,q,c}(f_r))]_{\mathrm{insep}}$$

by Lemma 4.1.17 and $\Phi_{I,q,c}(f_i) = \Phi'_{I,q,c'}(g_i) \pmod{\langle p \rangle_{R[\boldsymbol{z}]}}$ for all $i \in [r]$, Theorem 4.1.24 implies that $\Phi_{I,q,c}(f_1), \ldots, \Phi_{I,q,c}(f_r)$ are algebraically independent over K. □

4.2.5 Products of Constant-Degree Polynomials

In this section we consider products of constant-degree polynomials. Our first result is the construction of faithful homomorphisms for sets of those polynomials of transcendence degree 2. The second result is a hitting set construction for ΣΠΣΠ-circuits with constant top and bottom fan-in.

Preserving coprimality

The constructions in this section are based on criteria that rely on unique factorization of polynomials. In order to fulfill those criteria, we will require homomorphisms that preserve the coprimality of a given set of polynomials.

We start with the definition of a graded version of the homomorphisms $\Lambda_{D,q,c}$ given in (4.2.12). Let $D, q \geq 1$. Define the K-algebra homomorphisms

$$\begin{aligned} \overline{\Lambda}_D &\colon K[\boldsymbol{x}] \to K[w, \boldsymbol{x}, t], \quad x_i \mapsto x_i + t^{D^{i-1}} w, \\ \overline{\Lambda}_{D,q} &\colon K[\boldsymbol{x}] \to K[w, \boldsymbol{x}, t], \quad x_i \mapsto x_i + t^{\lfloor D^{i-1} \rfloor_q} w, \end{aligned} \tag{4.2.20}$$

where $i \in [n]$ and w, t are new variables. For $c \in K$, define the K-algebra homomorphism

$$\overline{\Lambda}_{D,q,c} \colon K[\boldsymbol{x}] \to K[w, \boldsymbol{x}], \quad x_i \mapsto x_i + c^{\lfloor D^{i-1} \rfloor_q} w, \tag{4.2.21}$$

where $i \in [n]$. For $f \in K[\boldsymbol{x}]$, we have $\overline{\Lambda}_{D,q,c}(f) = \overline{\Lambda}_{D,q}(f)|_{t=c}$ and $\Lambda_{D,q,c}(f) = \overline{\Lambda}_{D,q,c}(f)|_{w=1}$.

We say that a polynomial $f \in K[w, \boldsymbol{x}]$ is **quasi-monic in** w if it is non-zero and satisfies $\deg_w(f) = \deg(f)$, i. e. the leading coefficient of f, viewed as a polynomial in w with coefficients in $K[\boldsymbol{x}]$, is an element of K. For almost all $D \geq 1$, $q \in \mathbb{P}$, and $c \in K$, the homomorphism $\overline{\Lambda}_{D,q,c}$ sends a non-zero polynomial to a polynomial that is quasi-monic in w. The following lemma bounds the number of bad choices for the parameters q and c.

Lemma 4.2.24. *Let $\delta, s \geq 1$ and let $D \geq \delta + 1$. Let $f \in K[\boldsymbol{x}]$ be a non-zero polynomial of sparsity at most s and degree at most δ.*

Then there exists a set $B_1 \subset \mathbb{P}$ of primes with $|B_1| \leq (s-1)\lfloor n \log_2 D \rfloor$ satisfying the following property: For all $q \in \mathbb{P} \setminus B_1$ there exists a set $B_2 \subseteq K$ with $|B_2| < \delta q$ such that

$$\deg_w(\overline{\Lambda}_{D,q,c}(f)|_{\boldsymbol{x}=\boldsymbol{0}}) = \deg_w(\overline{\Lambda}_{D,q,c}(f)) = \deg(\overline{\Lambda}_{D,q,c}(f)) = \deg(f)$$

for all $c \in K \setminus B_2$.

Proof. The coefficient of the term $w^{\deg(f)}$ in $\overline{\Lambda}_D(f)$, viewed as a polynomial in $w, \boldsymbol{x}$ with coefficients in $K[t]$, is

$$\Lambda_D(g)|_{\boldsymbol{x}=\boldsymbol{0}} = g\big(t, t^D, \ldots, t^{D^{n-1}}\big),$$

where $g \in K[\boldsymbol{x}] \setminus \{0\}$ is the homogeneous degree-$\deg(f)$ part of f. Now all assertions follow from Lemma 4.2.16. □

The following lemma shows how a K-algebra homomorphism $\Psi\colon K[\boldsymbol{x}] \to K[\boldsymbol{z}]$ (that sends the variables to polynomials with constant term zero) can be turned into a homomorphism that preserves the coprimality of given polynomials. If Ψ is graded of degree 1, then so is the new homomorphism. The construction is efficient if the polynomials under consideration are of constant degree. We prove this lemma via resultants which are defined in Appendix A.3.2. The main idea of the proof is that polynomials $f, g \in K[w, \boldsymbol{x}]$, which are non-constant and quasi-monic in w, are coprime if and only if their w-resultant is non-zero. Therefore, preserving coprimality boils down to preserving the non-zeroness of resultants. A useful fact in this regard is that a homomorphism $\varphi\colon K[w, \boldsymbol{x}] \to K[w, \boldsymbol{z}]$ with $w \mapsto w$ satisfies $\varphi(\operatorname{res}_w(f, g)) = \operatorname{res}_w(\varphi(f), \varphi(g))$ if f, g are quasi-monic in w. Note that homomorphisms do not commute with resultants in general.

Lemma 4.2.25. *Let $\delta \geq 1$, let $D_1 \geq 2\delta^2 + 1$, and let $D_2 \geq \delta + 1$. Let $\Psi\colon K[\boldsymbol{x}] \to K[\boldsymbol{z}]$ be a K-algebra homomorphism such that $\Psi(x_i)|_{\boldsymbol{z}=\boldsymbol{0}} = 0$ for all $i \in [n]$. For $\boldsymbol{q} \in \mathbb{N}_{>0}^2$ and $\boldsymbol{c} \in K^2$, we define the K-algebra homomorphism*

$$\overline{\Phi}_{\boldsymbol{q},\boldsymbol{c}}\colon K[\boldsymbol{x}] \to K[\boldsymbol{w}, \boldsymbol{z}], \quad x_i \mapsto \Psi(x_i) + c_1^{\lfloor D_1^{i-1} \rfloor_{q_1}} w_1 + c_2^{\lfloor D_2^{i-1} \rfloor_{q_2}} w_2, \quad (4.2.22)$$

where $\boldsymbol{w} = \{w_1, w_2\}$ and $i \in [n]$. Let $f_1, \ldots, f_m \in K[\boldsymbol{x}]$ be non-constant polynomials of degree at most δ.

Then there exists a set $B_{2,1} \subset \mathbb{P}$ of primes with $|B_{2,1}| < mn\binom{n+\delta}{\delta} \log_2 D_2$ such that for all $q_2 \in \mathbb{P} \setminus B_{2,1}$ there exists a set $B_{2,2} \subseteq K$ with $|B_{2,2}| < m\delta q_2$ such that for all $c_2 \in K \setminus B_{2,2}$ there exists a set $B_{1,1} \subset \mathbb{P}$ of primes with $|B_{1,1}| < \binom{m}{2} n \binom{n+2\delta^2}{2\delta^2} \log_2 D_1$ satisfying the following property: For all $q_1 \in \mathbb{P} \setminus B_{1,1}$ there exists a set $B_{1,2} \subseteq K$ with $|B_{1,2}| < \binom{m}{2} 2\delta^2 q_1$ such that for all $c_1 \in K \setminus B_{1,2}$ we have

(a) $\overline{\Phi}_{\boldsymbol{q},\boldsymbol{c}}(f_i)$ is non-constant and quasi-monic in w_2 for all $i \in [m]$, and

(b) $\gcd(\overline{\Phi}_{\boldsymbol{q},\boldsymbol{c}}(f_i), \overline{\Phi}_{\boldsymbol{q},\boldsymbol{c}}(f_j)) = 1$ for all $i, j \in [m]$ with $\gcd(f_i, f_j) = 1$.

Proof. We first set up some notation. We extend Ψ to the K-algebra homomorphism $\overline{\Psi}\colon K[\boldsymbol{w}, \boldsymbol{x}] \to K[\boldsymbol{w}, \boldsymbol{x}]$ by $w_i \mapsto w_i$ for $i \in [2]$ and $x_i \mapsto \Psi(x_i)$ for

$i \in [n]$. Furthermore, for $D, q \geq 1$ and $c \in K$, we define the K-algebra homomorphism $\overline{\Lambda}_{D,q,c}\colon K[w_2, \boldsymbol{x}] \to K[\boldsymbol{w}, \boldsymbol{x}]$ by $w_2 \mapsto w_2$ and $x_i \mapsto x_i + c^{\lfloor D^{i-1} \rfloor_q} \cdot w_1$ for $i \in [n]$, and we define the K-algebra homomorphism $\overline{\Gamma}_{D,q,c}\colon K[\boldsymbol{x}] \to K[w_2, \boldsymbol{x}]$ by $x_i \mapsto x_i + c^{\lfloor D^{i-1} \rfloor_q} \cdot w_2$ for $i \in [n]$. Note that the homomorphisms $\overline{\Lambda}_{D,q,c}$ and $\overline{\Gamma}_{D,q,c}$ are essentially defined as (4.2.21). We have

$$\overline{\Phi}_{\boldsymbol{q},\boldsymbol{c}} = \overline{\Psi} \circ \overline{\Lambda}_{D_1,q_1,c_1} \circ \overline{\Gamma}_{D_2,q_2,c_2}$$

for all $\boldsymbol{q} \in \mathbb{N}_{>0}^2$ and $\boldsymbol{c} \in K^2$.

Now we proceed to the proof. For $i \in [m]$, we have $\operatorname{sp}(f_i) \leq \binom{n+\delta}{\delta}$, thus applying Lemma 4.2.24 to f_i provides a set $B_{2,1,i} \subset \mathbb{P}$ of primes with $|B_{2,1,i}| < n\binom{n+\delta}{\delta} \log_2 D_2$. Set $B_{2,1} := B_{2,1,1} \cup \cdots \cup B_{2,1,m}$ and let $q_2 \in \mathbb{P} \setminus B_{2,1}$. For $i \in [m]$, let $B_{2,2,i} \subseteq K$ be the subset with $|B_{2,2,i}| < \delta q_2$ provided by Lemma 4.2.24 applied to f_i. Set $B_{2,2} := B_{2,2,1} \cup \cdots \cup B_{2,2,m}$ and let $c_2 \in K \setminus B_{2,2}$. For $i \in [m]$, denote $g_i := \overline{\Gamma}_{D_2,q_2,c_2}(f_i) \in K[w_2, \boldsymbol{x}]$. By Lemma 4.2.24, $g_1, \ldots, g_m$ are quasi-monic in w_2 and we have $\deg_{w_2}(g_i) = \deg(g_i) = \deg(f_i) > 0$ for all $i \in [m]$.

Now let $i, j \in [m]$ with $i < j$ such that $\gcd(f_i, f_j) = 1$ in $K[\boldsymbol{x}]$. Since $\overline{\Gamma}_{D_2,q_2,c_2}$ can be extended to an automorphism of $K[w_2, \boldsymbol{x}]$ by $w_2 \mapsto w_2$, we also have $\gcd(g_i, g_j) = 1$ in $K[w_2, \boldsymbol{x}]$. Since g_i, g_j are quasi-monic in w_2, Lemma A.3.4 (b) implies that the resultant $g_{i,j} := \operatorname{res}_{w_2}(g_i, g_j) \in K[\boldsymbol{x}]$ is a non-zero polynomial. We have $\deg(g_{i,j}) \leq 2\delta^2$, hence $\operatorname{sp}(g_{i,j}) \leq \binom{n+2\delta^2}{2\delta^2}$. Applying Lemma 4.2.16 to $g_{i,j}$ provides a set $B_{1,1,i,j} \subset \mathbb{P}$ of primes with $|B_{1,1,i,j}| < n\binom{n+2\delta^2}{2\delta^2} \log_2 D_1$. Set $B_{1,1} := \bigcup_{i,j} B_{1,1,i,j}$, where the union is over all $i, j \in [m]$ as above, and let $q_1 \in \mathbb{P} \setminus B_{1,1}$. For $i, j \in [m]$ as above, let $B_{1,2,i,j} \subseteq K$ be the subset with $|B_{1,2,i,j}| < 2\delta^2 q_1$ provided by Lemma 4.2.16 applied to $g_{i,j}$. Set $B_{1,2} := \bigcup_{i,j} B_{1,2,i,j}$, where the union is over all $i, j \in [m]$ as above, and let $c_1 \in K \setminus B_{1,2}$. By Lemma 4.2.16, we have $\overline{\Lambda}_{D_2,q_2,c_2}(g_{i,j})|_{w_1=1,\boldsymbol{x}=\boldsymbol{0}} \neq 0$ for all $i, j \in [m]$ as above.

To finish the proof, we have to verify that $\overline{\Phi}_{\boldsymbol{q},\boldsymbol{c}}$ satisfies (a) and (b). We have $(\overline{\Psi} \circ \overline{\Lambda}_{D_1,q_1,c_1})(w_2) = w_2$ and $(\overline{\Psi} \circ \overline{\Lambda}_{D_1,q_1,c_1})(x_i) \in K[w_1, \boldsymbol{z}]$ for all $i \in [n]$. Since g_i is quasi-monic in w_2 and non-constant for all $i \in [m]$, this implies (a). To show (b), let $i, j \in [m]$ with $i < j$ such that $\gcd(f_i, f_j) = 1$ in $K[\boldsymbol{x}]$. By the just stated property, the homomorphism $\overline{\Psi} \circ \overline{\Lambda}_{D_1,q_1,c_1}$ commutes with taking resultants of polynomials that are quasi-monic in w_2. Therefore, we have

$$\begin{aligned}
\operatorname{res}_{w_2}\big(\overline{\Phi}_{\boldsymbol{q},\boldsymbol{c}}(f_i), \overline{\Phi}_{\boldsymbol{q},\boldsymbol{c}}(f_j)\big) &= \operatorname{res}_{w_2}\big((\overline{\Psi} \circ \overline{\Lambda}_{D_1,q_1,c_1})(g_i), (\overline{\Psi} \circ \overline{\Lambda}_{D_1,q_1,c_1})(g_j)\big) \\
&= (\overline{\Psi} \circ \overline{\Lambda}_{D_1,q_1,c_1})\big(\operatorname{res}_{w_2}(g_i, g_j)\big) \\
&= (\overline{\Psi} \circ \overline{\Lambda}_{D_1,q_1,c_1})(g_{i,j}) \neq 0,
\end{aligned}$$

because $(\overline{\Psi} \circ \overline{\Lambda}_{D_1,q_1,c_1})(g_{i,j})|_{w_1=1,\boldsymbol{z}=\boldsymbol{0}} = \overline{\Lambda}_{D_1,q_1,c_1}(g_{i,j})|_{w_1=1,\boldsymbol{x}=\boldsymbol{0}} \neq 0$ by the assumption on Ψ. By Lemma A.3.4 (b), we get (b). □

The following corollary is a variant of Lemma 4.2.25 with one w variable less.

Corollary 4.2.26. *Let $\delta \geq 1$, let $D_1 \geq 2\delta^2 + 1$, and let $D_2 \geq \delta + 1$. Let $\Psi\colon K[\boldsymbol{x}] \to K[\boldsymbol{z}]$ be a K-algebra homomorphism such that $\Psi(x_i)|_{\boldsymbol{z}=\boldsymbol{0}} = 0$ for all $i \in [n]$. For $\boldsymbol{q} \in \mathbb{N}_{>0}^2$ and $\boldsymbol{c} \in K^2$, we define the K-algebra homomorphism*

$$\Phi_{\boldsymbol{q},\boldsymbol{c}}\colon K[\boldsymbol{x}] \to K[w, \boldsymbol{z}], \quad x_i \mapsto \Psi(x_i) + c_1^{\lfloor D_1^{i-1} \rfloor_{q_1}} + c_2^{\lfloor D_2^{i-1} \rfloor_{q_2}} w, \tag{4.2.23}$$

where $i \in [n]$. Let $f_1, \ldots, f_m \in K[\boldsymbol{x}]$ be non-constant polynomials of degree at most δ.

Then there exists a set $B_{2,1} \subset \mathbb{P}$ of primes with $|B_{2,1}| < mn\binom{n+\delta}{\delta} \log_2 D_2$ such that for all $q_2 \in \mathbb{P} \setminus B_{2,1}$ there exists a set $B_{2,2} \subseteq K$ with $|B_{2,2}| < m\delta q_2$ such that for all $c_2 \in K \setminus B_{2,2}$ there exists a set $B_{1,1} \subset \mathbb{P}$ of primes with $|B_{1,1}| < \binom{m}{2} n\binom{n+2\delta^2}{2\delta^2} \log_2 D_1$ satisfying the following property: For all $q_1 \in \mathbb{P} \setminus B_{1,1}$ there exists a set $B_{1,2} \subseteq K$ with $|B_{1,2}| < \binom{m}{2} 2\delta^2 q_1$ such that for all $c_1 \in K \setminus B_{1,2}$ we have

(a) $\Phi_{\boldsymbol{q},\boldsymbol{c}}(f_i)$ is non-constant and quasi-monic in w for all $i \in [m]$, and

(b) $\gcd(\Phi_{\boldsymbol{q},\boldsymbol{c}}(f_i), \Phi_{\boldsymbol{q},\boldsymbol{c}}(f_j)) = 1$ for all $i, j \in [m]$ with $\gcd(f_i, f_j) = 1$.

Proof. This can be proven, *mutatis mutandis*, like Lemma 4.2.25. □

Transcendence degree two

Now we turn our attention to homogeneous products of constant-degree polynomials. We will construct faithful homomorphisms for sets of those polynomials of transcendence degree at most 2.

Theorem 4.2.27. *Let $n \geq 2$ and let $1 \leq \delta \leq d$. Set $D_1 := 2\delta^2 + 1$ and $D_2 := \delta + 1$. For $\boldsymbol{q} \in \mathbb{N}_{>0}^2$ and $\boldsymbol{c} \in K^2$, define the K-algebra homomorphism*

$$\Phi_{\boldsymbol{q},\boldsymbol{c}}\colon K[\boldsymbol{x}] \to K[z_1, z_2], \quad x_i \mapsto c_1^{\lfloor D_1^{i-1} \rfloor_{q_1}} \cdot z_1 + c_2^{\lfloor D_2^{i-1} \rfloor_{q_2}} \cdot z_2, \tag{4.2.24}$$

where $i \in [n]$.

There exists an effectively computable $N \in \mathbb{N}$ with $N = \operatorname{poly}\bigl(n^{\delta^2}, \delta, d\bigr)$ such that for all N-subsets $S \subseteq K$ we have the following: For all homogeneous polynomials $f_1, \ldots, f_m \in K[\boldsymbol{x}]$ of degree at most d, transcendence degree at most 2, and with irreducible factors of degree at most δ, there exist $\boldsymbol{q} \in [N]^2$ and $\boldsymbol{c} \in S^2$ such that $\Phi_{\boldsymbol{q},\boldsymbol{c}}$ is faithful to $\{f_1, \ldots, f_m\}$.

Proof. Using Corollary A.1.2 (b), the assertion follows from Lemma 4.2.31 below. □

The proof is based on a criterion for the algebraic independence of two homogeneous polynomials (Corollary 4.2.30) which can be derived from a homogeneous version of Lüroth's Theorem.

Theorem 4.2.28 (Extended Lüroth's Theorem)**.** *Let $K \subseteq L \subseteq K(\boldsymbol{x})$ be field extensions such that* $\operatorname{trdeg}(L/K) = 1$.

(a) There exists $f \in K(\boldsymbol{x})$ such that $L = K(f)$.

(b) If $L \cap K[\boldsymbol{x}]$ contains a non-constant polynomial, then there exists a polynomial $f \in K[\boldsymbol{x}]$ such that $L = K(f)$.

(c) If $L \cap K[\boldsymbol{x}]$ contains a non-constant homogeneous polynomial, then there exists a homogeneous polynomial $f \in K[\boldsymbol{x}]$ such that $L = K(f)$.

Proof. Parts (a) and (b) are proven in [Sch00, Section 1.2, Theorem 3 and 4]. To show (c), let $g \in L \cap K[\boldsymbol{x}]$ be a non-constant homogeneous polynomial. By (b), $L = K(f)$ for some $f \in K[\boldsymbol{x}]$. We may assume that $f(\mathbf{0}) = 0$. By Lemma 4.2.29 below, there exists $G \in K[y]$ such that $g = G(f)$. Denote by $G_{\max}, G_{\min} \in K[y]$ the homogeneous components of G of maximal and minimal degree, respectively, and likewise denote by $f_{\max}, f_{\min} \in K[\boldsymbol{x}]$ the homogeneous components of f of maximal and minimal degree, respectively. Since $f(\mathbf{0}) = 0$, we have $f_{\min} \notin K$. Therefore, the homogeneous components of $G(f)$ of maximal and minimal degree are given by $G_{\max}(f_{\max})$ and $G_{\min}(f_{\min})$, respectively. But since $g = G(f)$ is homogeneous, this implies $f_{\max} = f_{\min}$, hence f is homogeneous. □

The following lemma was used in the proof of part (c) of the Extended Lüroth Theorem.

Lemma 4.2.29. *Let $f \in K[\boldsymbol{x}]$. Then we have $K(f) \cap K[\boldsymbol{x}] = K[f]$.*

Proof. For $f \in K$ the assertion is evident, so assume that f is non-constant. We have $K[f] \subseteq K(f) \cap K[\boldsymbol{x}]$. To show the converse inclusion, let $g \in K(f) \cap K[\boldsymbol{x}]$. Then there exist coprime polynomials $G_1, G_2 \in K[y]$ with $G_2(f) \neq 0$ such that $g = G_1(f)/G_2(f)$. Division with remainder yields polynomials $Q, R \in K[y]$ such that $G_1 = Q \cdot G_2 + R$ and either $R = 0$ or $\deg_y(R) < \deg_y(G_2)$. If $R = 0$, then the coprimality of G_1 and G_2 implies $G_2 \in K$, thus $g = G_2^{-1} \cdot G_1(f) \in K[f]$ and we are done. So let $R \neq 0$. We have $g \cdot G_2(f) = G_1(f) = Q(f) \cdot G_2(f) + R(f)$, hence $R(f) = (g - Q(f)) \cdot G_2(f)$. Since f is non-constant, we have $\deg(R(f)) = \deg_y(R) \cdot \deg(f) < \deg_y(G_2) \cdot \deg(f) = \deg(G_2(f))$. This implies $g = Q(f) \in K[f]$. □

The Extended Lüroth Theorem implies that two non-constant homogeneous polynomials of transcendence degree 1 have associated powers, providing us with an annihilating polynomial of simple shape.

Corollary 4.2.30. *Let $f_1, f_2 \in K[\boldsymbol{x}]$ be non-constant homogeneous polynomials of degree at most $D \geq 1$. Then f_1, f_2 are algebraically dependent over K if and only if $f_1^{d_1} = c \cdot f_2^{d_2}$ for some $d_1, d_2 \in [D]$ and some $c \in K^*$.*

Proof. If $f_1^{d_1} = c \cdot f_2^{d_2}$ for some $d_1, d_2 \in [D]$ and some $c \in K^*$, then f_1, f_2 are clearly algebraically dependent over K.

Conversely, assume that f_1, f_2 are algebraically dependent over K. Since f_1, f_2 are non-constant, the field $L := K(f_1, f_2)$ has transcendence degree 1 over K. By Theorem 4.2.28 (c), there exists a homogeneous polynomial $h \in K[\boldsymbol{x}]$ such that $L = K(h)$. Since f_1, f_2 are non-zero and homogeneous, $f_1 = c_1 h^{d_2}$ and $f_2 = c_2 h^{d_1}$ for some $d_1, d_2 \in [D]$ and some $c_1, c_2 \in K^*$. Setting $c := c_1^{d_1} c_2^{-d_2} \in K^*$, we obtain $f_1^{d_1} = c_1^{d_1} h^{d_1 d_2} = c \cdot c_2^{d_2} h^{d_1 d_2} = c \cdot f_2^{d_2}$. □

The following lemma constitutes the proof of Theorem 4.2.27. The main idea of the proof is that, in view of Corollary 4.2.30, two algebraically independent homogeneous polynomials can become dependent under a graded homomorphism only if the coprimality of some pair of their factors gets violated. Therefore, preserving the algebraic independence of two homogeneous polynomials reduces to preserving the coprimality of their irreducible factors. For the latter, we can invoke Lemma 4.2.25.

Lemma 4.2.31. *Let $n \geq 2$, let $1 \leq \delta \leq d$, let $D_1 \geq 2\delta^2 + 1$, and let $D_2 \geq \delta + 1$. For $\boldsymbol{q} \in \mathbb{N}_{>0}^2$ and $\boldsymbol{c} \in K^2$, let $\Phi_{\boldsymbol{q},\boldsymbol{c}}$ be defined as in (4.2.24). Let $f_1, \ldots, f_m \in K[\boldsymbol{x}]$ be homogeneous polynomials of degree at most d, transcendence degree at most 2, and with irreducible factors of degree at most δ.*

Then there exists a set $B_{2,1} \subset \mathbb{P}$ of primes with $|B_{2,1}| < 2nd\binom{n+\delta}{\delta} \log_2 D_2$ such that for all $q_2 \in \mathbb{P} \setminus B_{2,1}$ there exists a set $B_{2,2} \subseteq K$ with $|B_{2,2}| < 2\delta d q_2$ such that for all $c_2 \in K \setminus B_{2,2}$ there exists a set $B_{1,1} \subset \mathbb{P}$ of primes with $|B_{1,1}| < \binom{2d}{2} n \binom{n+2\delta^2}{2\delta^2} \log_2 D_1$ satisfying the following property: For all $q_1 \in \mathbb{P} \setminus B_{1,1}$ there exists a set $B_{1,2} \subseteq K$ with $|B_{1,2}| < \binom{2d}{2} 2\delta^2 q_1$ such that $\Phi_{\boldsymbol{q},\boldsymbol{c}}$ is faithful to $\{f_1, \ldots, f_m\}$ for all $c_1 \in K \setminus B_{1,2}$.

Proof. We may assume that f_1, f_2 are algebraically independent over K (if the transcendence degree is less than 2, we can append algebraically independent variables). Let $g_1, \ldots, g_k \in K[\boldsymbol{x}]$ be the (pairwise non-associated) irreducible factors of f_1 and f_2. We have $k \leq 2d$.

Now let $\Phi \colon K[\boldsymbol{x}] \to K[z_1, z_2]$ be a graded K-algebra homomorphism. We want to show the following claim: If $\Phi(g_i)$ is non-constant for all $i \in [k]$,

and if $\gcd(\Phi(g_i), \Phi(g_j)) = 1$ in $K[z_1, z_2]$ for all $i, j \in [k]$ with $i \neq j$, then $\Phi(f_1), \Phi(f_2)$ are algebraically independent over K. To this end, let $d_1, d_2 \geq 1$. Let $\alpha, \beta \in \mathbb{N}^k$ such that $f_1 = u_1 \cdot g_1^{\alpha_1} \cdots g_k^{\alpha_k}$ and $f_2 = u_2 \cdot g_1^{\beta_1} \cdots g_k^{\beta_k}$ for some $u_1, u_2 \in K^*$. Since f_1, f_2 are algebraically independent over K, the powers $f_1^{d_1}$ and $f_2^{d_2}$ are not associated. Hence, by unique factorization, there exists $i \in [k]$ such that $d_1\alpha_i \neq d_2\beta_i$. By the assumptions on Φ, the images $\Phi(g_1), \ldots, \Phi(g_k)$ are non-zero (not necessarily irreducible) non-units and pairwise coprime. By unique factorization, we can infer that $\Phi(f_1)^{d_1} = u_1 \cdot \Phi(g_1)^{\alpha_1 d_1} \cdots \Phi(g_k)^{\alpha_k d_1}$ and $\Phi(f_2)^{d_2} = u_2 \cdot \Phi(g_1)^{\beta_1 d_2} \cdots \Phi(g_k)^{\beta_k d_2}$ are not associated. Since Φ is graded, $\Phi(f_1)$ and $\Phi(f_2)$ are homogeneous, hence Corollary 4.2.30 implies that $\Phi(f_1), \Phi(f_2)$ are algebraically independent over K and the claim is proven.

Now the assertion follows from Lemma 4.2.25 applied to the homomorphism $\Psi\colon K[\boldsymbol{x}] \to K$ defined by $x_i \mapsto 0$ for all $i \in [n]$, and to the polynomials $g_1, \ldots, g_k$. Note that in this case, for $\boldsymbol{q} \in \mathbb{N}^2_{>0}$ and $\boldsymbol{c} \in K^2$, the definition of $\overline{\Phi}_{\boldsymbol{q},\boldsymbol{c}}\colon K[\boldsymbol{x}] \to K[w_1, w_2]$ in (4.2.22) agrees with the definition of $\Phi_{\boldsymbol{q},\boldsymbol{c}}\colon K[\boldsymbol{x}] \to K[z_1, z_2]$ in (4.2.24) when w_1, w_2 are replaced by z_1, z_2. □

A rank-based approach to identity testing of ΣΠΣΠ-circuits with constant top and bottom fan-in

We continue with a hitting set construction for ΣΠΣΠ-circuits, which are sums of products of sparse polynomials. Our method is a generalization of the rank-based approach for ΣΠΣ-circuits by Dvir, Karnin & Shpilka [DS07, KS11a].

Definition 4.2.32. Let $n, k, d, \delta \geq 1$ and consider the arithmetic circuit

$$C = \sum_{i=1}^{k} \prod_{j=1}^{d} f_{i,j}, \tag{4.2.25}$$

where $f_{i,j} \in K[\boldsymbol{x}] \setminus \{0\}$ are polynomials (in sparse ΣΠ-representation) of degree at most δ. The set of all circuits as in (4.2.25) is denoted by $\Sigma_k\Pi_d\Sigma\Pi_\delta$.

(a) The parameters k and δ are called **top** and **bottom fan-in** of C, respectively. For $i \in [k]$, the product $T_i := \prod_{j=1}^{d} f_{i,j}$ is called a **multiplication term** of C. We call $\mathcal{S}(C) := \{f_{i,j} \mid i \in [k] \text{ and } j \in [d]\} \subseteq K[\boldsymbol{x}]$ the set of **sparse polynomials** of C.

(b) The **content** of C is defined as $\operatorname{cont}(C) := \gcd(T_1, \ldots, T_k) \in K[\boldsymbol{x}] \setminus \{0\}$. If $\operatorname{cont}(C) = 1$, then C is called **simple**. The **simple part** of C is defined as the arithmetic circuit $\operatorname{sim}(C) := C/\operatorname{cont}(C)$.

(c) For $I \subseteq [k]$, we define the arithmetic circuit $C_I := \sum_{i \in I} T_i$. If $C_I \neq 0$ for all non-empty proper subsets $I \subset [k]$, then C is called **minimal**.

(d) The **rank** of C is defined as $\mathrm{rk}(C) := \mathrm{trdeg}_K(\mathcal{S}(C))$.

(e) Let $R_\delta(k,d)$ be the smallest $r \in \mathbb{N}_{>0}$ with the following property: Every simple and minimal $\Sigma_k\Pi_d\Sigma\Pi_\delta$-circuit C computing the zero polynomial satisfies $\mathrm{rk}(C) < r$.

For $\delta = 1$ and $f_{i,j}$ homogeneous for all $i \in [k]$ and $j \in [d]$, those definitions agree with the respective notions for $\Sigma\Pi\Sigma$-circuits.

Simple and minimal $\Sigma_k\Pi_d\Sigma\Pi_\delta$-circuits computing the zero polynomial are in a sense the smallest polynomial identities in this class.

We will assume that the top fan-in k and the bottom fan-in δ are constants. Note that for k unbounded, there are no efficient PIT algorithms known even for $\Sigma\Pi\Sigma$-circuits. On the other hand, if $k = 2$ and δ is unbounded, we obtain an instance of the as yet unsolved sparse factorization problem [vzGK85, SSS11]. One of the difficulties that arise when δ is unbounded is that factors of sparse polynomials are not sparse in general.

Except for the top fan-in 2 case (and the previously known bottom fan-in 1 case), our hitting set construction is conditional in the sense that its efficiency depends on a good upper bound for $R_\delta(k,d)$. We will discuss this question below. The following theorem shows how to reduce the number of variables of a $\Sigma_k\Pi_d\Sigma\Pi_\delta$-circuit from n to $R_\delta(k,d)+1$ while preserving non-zeroness.

Theorem 4.2.33. *Let $n, \delta, d, k \geq 1$ and let $r := R_\delta(k,d)$. For $\boldsymbol{D} = (D_2, D_3) \in \mathbb{N}_{>0}^2$, $\boldsymbol{q} = (q_2, q_3) \in \mathbb{N}_{>0}^2$ and $\boldsymbol{c} = (c_1, c_2, c_3) \in K^3$, define the K-algebra homomorphism*

$$\Phi_{\boldsymbol{D},\boldsymbol{q},\boldsymbol{c}} \colon K[\boldsymbol{x}] \to K[w, \boldsymbol{z}],$$
$$x_i \mapsto \left(\sum_{j=1}^{r} a_{i,j}(c_1) \cdot z_j\right) + c_2^{\lfloor D_2^{i-1} \rfloor_{q_2}} + c_3^{\lfloor D_3^{i-1} \rfloor_{q_3}} w, \quad (4.2.26)$$

where $i \in [n]$ and $a_{i,j} \in K[t]$ are defined as in (4.2.8).

(a) Let $\mathrm{char}(K)$ be arbitrary. Set $D_2 := 2\delta^{r+1}+1$ and $D_3 := \delta+1$. Then there exists an effectively computable $N \in \mathbb{N}$ with $N = \mathrm{poly}\big(n^{kr^2\delta^{r+1}}, \delta^r, dk\big)$ such that for all N-subsets $S \subseteq K$ we have the following: For all non-zero $C \in \Sigma_k\Pi_d\Sigma\Pi_\delta$ there exist $\boldsymbol{q} \in [N]^2$ and $\boldsymbol{c} \in S^3$ such that $\Phi_{\boldsymbol{D},\boldsymbol{q},\boldsymbol{c}}(C) \neq 0$.

(b) Let $\mathrm{char}(K) = 0$ or $\mathrm{char}(K) > \delta^r$. Set $D_2 := 2\delta^2 r + 1$ and $D_3 := \delta + 1$. Then there exists an effectively computable $N \in \mathbb{N}$ with $N =$

$\operatorname{poly}\big(n^{rk\delta^2}, r^r, \delta dk\big)$ *such that for all* N*-subsets* $S \subseteq K$ *we have the following: For all non-zero* $C \in \Sigma_k\Pi_d\Sigma\Pi_\delta$ *there exist* $\boldsymbol{q} \in [N]^2$ *and* $\boldsymbol{c} \in S^3$ *such that* $\Phi_{\boldsymbol{D},\boldsymbol{q},\boldsymbol{c}}(C) \neq 0$.

The proof of this theorem, given below, is based on the following lemma. It is a generalization of [KS11a, Theorem 3.4] to $\Sigma\Pi\Sigma\Pi$-circuits. According to this lemma, a homomorphism preserves the non-zeroness of a given $\Sigma_k\Pi_d\Sigma\Pi_\delta$-circuit C if it preserves the simple part of C_I and rank at least $R_\delta(k,d)$ of the simple part of C_I for all non-trivial subcircuits C_I of C.

Lemma 4.2.34. *Let* $n, r, k, d, \delta \geq 1$. *Let* C *be a* $\Sigma_k\Pi_d\Sigma\Pi_\delta$*-circuit and let* $\varphi\colon K[\boldsymbol{x}] \to K[\boldsymbol{z}]$ *be a* K*-algebra homomorphism of degree* 1 *that satisfies*

(a) $\varphi(\operatorname{sim}(C_I)) = \operatorname{sim}(\varphi(C_I))$ *and*

(b) $\operatorname{rk}(\varphi(\operatorname{sim}(C_I))) \geq \min\{\operatorname{rk}(\operatorname{sim}(C_I)), R_\delta(k,d)\}$

for all non-empty $I \subseteq [k]$. *Then we have* $C = 0$ *if and only if* $\varphi(C) = 0$.

Proof. If $C = 0$, then clearly $\varphi(C) = 0$. Conversely, assume that $\varphi(C) = 0$. Since $\varphi(C) = \varphi(C_{I_1}) + \cdots + \varphi(C_{I_m})$ for some non-empty $I_1, \ldots, I_m \subseteq [k]$ with $\varphi(C_{I_i})$ zero and minimal for all $i \in [m]$, we may assume that $\varphi(C)$ is simple. By assumption (a), we have $\varphi(\operatorname{sim}(C)) = \operatorname{sim}(\varphi(C))$, thus $\varphi(\operatorname{sim}(C))$ is a minimal and simple circuit computing the zero polynomial. Since φ is of degree 1, we have $\varphi(\operatorname{sim}(C)) \in \Sigma_k\Pi_d\Sigma\Pi_\delta$, hence $\operatorname{rk}(\varphi(\operatorname{sim}(C))) < R_\delta(k,d)$. By assumption (b), this implies $\operatorname{rk}(\varphi(\operatorname{sim}(C))) = \operatorname{rk}(\operatorname{sim}(C))$, thus φ is faithful to $\mathcal{S}(\operatorname{sim}(C))$. Lemma 4.2.7 yields $\operatorname{sim}(C) = 0$, hence $C = 0$. □

The following lemma demonstrates that the simple part of a $\Sigma\Pi\Sigma\Pi$-circuit C can be preserved by preserving the coprimality of the constant-degree polynomials in $\mathcal{S}(C)$. The latter can be accomplished by Corollary 4.2.26.

Lemma 4.2.35. *Let* C *be a* $\Sigma_k\Pi_d\Sigma\Pi_\delta$*-circuit and let* $f_1, \ldots, f_m \in K[\boldsymbol{x}]$ *be the (pairwise non-associated) irreducible factors of the polynomials in* $\mathcal{S}(C)$. *Let* $\varphi\colon K[\boldsymbol{x}] \to K[\boldsymbol{z}]$ *be a* K*-algebra homomorphism such that*

(a) $\varphi(f_i) \neq 0$ *for all* $i \in [m]$, *and*

(b) $\gcd(\varphi(f_i), \varphi(f_j)) = 1$ *for all* $i, j \in [m]$ *with* $i < j$.

Then we have $\varphi(\operatorname{sim}(C)) = \operatorname{sim}(\varphi(C))$.

Proof. Replacing C by its simple part, we may assume that C is simple. Then we have to verify that $\varphi(C)$ is again simple. To this end, write $C = \sum_{i=1}^{k} T_i$, where $T_1, \ldots, T_k \in K[\boldsymbol{x}]$ are multiplication terms with $\gcd(T_1, \ldots, T_k) = 1$. Now assume for the sake of contradiction that $\operatorname{cont}(\varphi(C)) \neq 1$. Then $k \geq 2$

and there exists an irreducible polynomial $g \in K[\boldsymbol{x}]$ dividing $\varphi(T_i)$ for all $i \in [k]$. Therefore, there exist $j_1, \ldots, j_k \in [m]$ such that f_{j_i} divides T_i and g divides $\varphi(f_{j_i})$ for all $i \in [k]$. Since $\gcd(T_1, \ldots, T_k) = 1$, there exist $i_1, i_2 \in [k]$ such that $j_{i_1} < j_{i_2}$. This implies that g divides $\gcd(\varphi(f_{j_{i_1}}), \varphi(f_{j_{i_2}})) = 1$, a contradiction. □

Proof of Theorem 4.2.33. We start with some easy estimates. Let C be a $\Sigma_k\Pi_d\Sigma\Pi_\delta$-circuit. Then $\mathrm{sp}(f) \leq \binom{n+\delta}{\delta}$ for all $f \in \mathcal{S}(C)$. If $f_1, \ldots, f_m \in K[\boldsymbol{x}]$ are the (pairwise non-associate) irreducible factors of the polynomials in $\mathcal{S}(C)$, then we have $m \leq kd\delta$.

Now we show (a). By Lemma 4.2.19, Corollary 4.2.26, and Corollary A.1.2 (b), there exists an effectively computable $N \in \mathbb{N}$ with

$$N = \mathrm{poly}\big(n^{kr^2\delta^{r+1}}, \delta^r, dk\big)$$

such that for all N-subsets $S \subseteq K$ and all $C \in \Sigma_k\Pi_d\Sigma\Pi_\delta$ there exist $\boldsymbol{q} \in [N]^2$ and $\boldsymbol{c} \in S^3$ such that

(a) $\Phi_{\boldsymbol{D},\boldsymbol{q},\boldsymbol{c}}(f_i) \neq 0$ for all $i \in [m]$ and $\gcd(\Phi_{\boldsymbol{D},\boldsymbol{q},\boldsymbol{c}}(f_i), \Phi_{\boldsymbol{D},\boldsymbol{q},\boldsymbol{c}}(f_j)) = 1$ for all $i, j \in [m]$ with $i < j$, where $f_1, \ldots, f_m \in K[\boldsymbol{x}]$ are the (pairwise non-associate) irreducible factors of the polynomials in $\mathcal{S}(C)$, and

(b) $\Phi_{\boldsymbol{D},\boldsymbol{q},\boldsymbol{c}}$ is faithful to some subset $\{f_1, \ldots, f_m\} \subseteq \mathcal{S}(\mathrm{sim}(C_I))$ of transcendence degree $\min\{\mathrm{rk}(\mathrm{sim}(C_I)), R_\delta(k,d)\}$ for all non-empty $I \subseteq [k]$.

By Lemmas 4.2.34 and 4.2.35, we obtain assertion (a).

Part (b) can be shown similarly, with the difference that we can use Lemma 4.2.20 instead of Lemma 4.2.19 in zero or large characteristic. □

Rank bounds

First we state some trivial upper bounds for $R_\delta(k,d)$. We have $R_\delta(k,d) \leq kd$, because $|\mathcal{S}(C)| \leq kd$ for all $C \in \Sigma_k\Pi_d\Sigma\Pi_\delta$ and $\mathcal{S}(C)$ is algebraically dependent over K if $C = 0$. In the top fan-in 2 case, we have $R_\delta(2,d) = 1$, because a simple, minimal, and zero $\Sigma_2\Pi_d\Sigma\Pi_\delta$-circuit is of the form $c - c$ for some $c \in K$.

Rank bounds for $\Sigma_k\Pi\Sigma_d$-circuits were studied in [DS07, SS11a, KS09, SS10]. Since linear forms are algebraically independent if and only if they are linearly independent, those rank bounds also apply to $R_1(k,d)$. By [SS10], we have $R_1(k,d) = O(k^2 \log d)$ for arbitrary fields K, and $R_1(k,d) = O(k^2)$ for ordered fields K.

On the other hand, examples in [KS07, SS11a] demonstrate $R_1(k,d) = \Omega(k)$ if $\mathrm{char}(K) = 0$, and $R_1(k,d) = \Omega(k \log_p d)$ if $\mathrm{char}(K) = p > 0$.

Finding a good upper bound for $R_\delta(k,d)$ in the general case remains an open question. The experience with $\Sigma\Pi\Sigma$-circuits leads us to the following natural conjecture.

Conjecture 4.2.36. *We have*

$$R_\delta(k,d) = \begin{cases} \operatorname{poly}(\delta k), & \text{if } \operatorname{char}(K) = 0, \\ \operatorname{poly}(\delta k \log_p d), & \text{if } \operatorname{char}(K) = p > 0. \end{cases}$$

4.2.6 Summary

We summarize the results of Sections 4.2.1 to 4.2.5. We constructed hitting sets for the circuit classes listed in the following table.

#	Circuit class	$\operatorname{char}(K)$	Hitting set size	Comment
(a)	$\operatorname{Alg}_{\tau,D}\Sigma$	any	$\operatorname{poly}\big(n, D^\tau\big)$	
(b)	$\operatorname{Alg}_{\tau,D}\Pi_\delta$	any	$\operatorname{poly}\big((n\delta D)^\tau\big)$	
(c)	$\operatorname{Alg}_{\tau,D}\Sigma_s\Pi_\delta$	any	$\operatorname{poly}\big(n^{\delta^\tau}, n^{\tau^2}, (\delta D)^\tau\big)$	
(d)		0 or $> \delta^\tau$	$\operatorname{poly}\big((ns\delta D)^\tau\big)$	
(e)		$p > 0$	$\operatorname{poly}\big(\delta^{\tau^2 s}, (n\tau D)^\tau, s^{\tau s}\big)$	$K \subseteq \overline{\mathbb{F}}_p$
(f)	$\operatorname{Alg}_{2,D}\Pi_d\Sigma\Pi_\delta$	any	$\operatorname{poly}\big(n^{\delta^2}, \delta d D\big)$	
(g)	$\Sigma_k\Pi_d\Sigma\Pi_\delta$	any	$\operatorname{poly}\big(n^{kr^2\delta^{r+1}}, (\delta d)^r, k\big)$	$r = R_\delta(k,d)$
(h)		0 or $> \delta^r$	$\operatorname{poly}\big(n^{rk\delta^2}, (\delta d r)^r, k\big)$	$r = R_\delta(k,d)$

The hitting sets of (a)–(f) are based on Theorem 4.2.4 in conjunction with the construction of faithful homomorphisms in Theorems 4.2.8, 4.2.9, 4.2.17 (a), 4.2.17 (b), 4.2.21, and 4.2.27, respectively. Items (g) and (h) use Theorem 3.2.4 together with Theorem 4.2.33. Note that the latter theorem also uses the concept of faithfulness.

Remark 4.2.37. In [ASSS12], faithful homomorphisms were constructed for sets of products of linear forms using the Jacobian Criterion. Thereby, for $\operatorname{char}(K) = 0$ or $\operatorname{char}(K) > \delta^\tau$, they obtained hitting sets for $\operatorname{Alg}_{\tau,D}\Pi_\delta\Sigma$ of size $\operatorname{poly}\big(n, (\delta D)^\tau\big)$, where $\Pi_\delta\Sigma$ denotes the set of products of linear forms of degree δ.

4.3 Algebraic Independence Testing

In this section we study the complexity of testing algebraic independence of arithmetic circuits.

Problem 4.3.1. Let K be a computable field and let $\mathcal{C}$ be a circuit class over K. Then the **algebraic independence testing** problem $\mathsf{AlgIndep}_K(\mathcal{C})$ is defined as follows: Given circuits $C_1, \ldots, C_m \in \mathcal{C}$, decide whether the polynomials $C_1, \ldots, C_m$ are algebraically independent over K. We set $\mathsf{AlgIndep}_K := \mathsf{AlgIndep}_K(\mathcal{C}_{\text{all}})$.

Algebraic independence testing of a constant number of arithmetic circuits

We start with the special case where the number of arithmetic circuits is fixed. Here the degree bound for annihilating polynomials yields an efficient randomized algorithm for polynomial-degree circuits.

Let K be a computable field and let $\mathcal{C}$ be a circuit class over K. For fixed $m \geq 1$, we denote by $\mathsf{AlgIndep}_K(\mathcal{C})_m$ the following problem: Given circuits $C_1, \ldots, C_m \in \mathcal{C}$, decide whether the polynomials $C_1, \ldots, C_m$ are algebraically independent over K.

Theorem 4.3.2. *Let $m \geq 1$, and let $K = \mathbb{Q}$ or $K = \mathbb{F}_q$ for some prime power q. Then we have $\mathsf{AlgIndep}_K(\mathcal{C}_{\text{poly-deg}})_m \in \mathbf{RP}$.*

Proof. Using Lemma 4.3.3 below, we can reduce to the linear independence testing problem (see Corollary 3.3.3). □

Lemma 4.3.3. *Let $f_1, \ldots, f_m \in K[\boldsymbol{x}]$ be polynomials of degree at most $\delta \geq 1$. Then $f_1, \ldots, f_m$ are algebraically independent over K if and only if*

$$\left\{ f_1^{i_1} \cdots f_m^{i_m} \mid \boldsymbol{i} \in \mathbb{N}^m \text{ such that } |\boldsymbol{i}| \leq \delta^m \right\}$$

is K-linearly independent.

Proof. The lemma is a direct consequence of Theorem 4.1.5. □

Algebraic independence testing over $\mathbb{Q}$

In characteristic zero, testing algebraic independence reduces to (the complement of) PIT by the Jacobian Criterion (cf. [DGW09, Kay09]).

Theorem 4.3.4. *Let K be a computable field with $\mathrm{char}(K) = 0$. Then the problems $\mathsf{AlgIndep}_K$ and $\overline{\mathsf{PIT}}_K$ are polynomial-time equivalent.*

Proof. Let C be an arithmetic circuit over $K[\boldsymbol{x}]$. Then $C \neq 0$ if and only if $C \cdot x_1$ is algebraically independent over K. Therefore, $\overline{\mathsf{PIT}}_K$ reduces to $\mathsf{AlgIndep}_K$.

Conversely, let $C_1, \ldots, C_m$ be arithmetic circuits over $K[\boldsymbol{x}]$. We may assume $m \leq n$ (instances with $m > n$ are algebraically dependent over K and can be mapped to the zero circuit). Consider the polynomial

$$\det \begin{pmatrix} & J & \\ & & \\ t_{m+1,1} & \cdots & t_{m+1,n} \\ \vdots & & \vdots \\ t_{n,1} & \cdots & t_{n,n} \end{pmatrix} \in K[\boldsymbol{t}, \boldsymbol{x}],$$

where $J := J_{\boldsymbol{x}}(C_1, \ldots, C_m) \in K[\boldsymbol{x}]^{m \times n}$ is the Jacobian matrix of $C_1, \ldots, C_m$ and $\boldsymbol{t} = \{t_{i,j} \mid i \in [m+1, n] \text{ and } j \in [n]\}$ are new variables. An arithmetic circuit C for this polynomial can be computed in polynomial time, using [BS83] for the partial derivatives and the Berkowitz algorithm (see Lemma A.3.1) for the determinant. By the Jacobian criterion, $C_1, \ldots, C_m$ are algebraically independent over K if and only if $\mathrm{rk}_{K(\boldsymbol{x})}(J) = m$ if and only if J can be completed to a non-singular matrix of $K(\boldsymbol{x})^{n \times n}$ if and only if $C \neq 0$. Therefore, $\mathsf{AlgIndep}_K$ reduces to $\overline{\mathsf{PIT}}_K$. □

As a consequence of Theorem 4.3.4, we obtain an efficient randomized algorithm for the algebraic independence testing problem over $\mathbb{Q}$.

Corollary 4.3.5. *We have* $\mathsf{AlgIndep}_{\mathbb{Q}} \in \mathbf{RP}$.

Proof. This follows from Theorems 4.3.4 and 2.5.7. □

Algebraic independence testing over finite fields

In [DGW09, Kay09] the question was posed whether there are efficient randomized algorithms for testing algebraic independence over finite fields. The previously best known complexity bound was $\mathsf{AlgIndep}_{\mathbb{F}_q} \in \mathbf{PSPACE}$. This result can be obtained from the degree bound for annihilating polynomials and linear algebra. Using the Witt-Jacobian Criterion (see Section 4.1.3), we show that algebraic independence over finite fields can be tested by a non-deterministic polynomial-time Turing machine with a #**P**-oracle. Since we have the inclusion $\mathbf{NP}^{\#\mathbf{P}} \subseteq \mathbf{PSPACE}$, this is an improvement over the previously known complexity bound.

Theorem 4.3.6. *We have* $\mathsf{AlgIndep}_{\mathbb{F}_q} \in \mathbf{NP}^{\#\mathbf{P}}$ *for all prime powers* q.

For the proof and algorithm, given below, we will require an explicit realization of the truncated Witt ring $\mathrm{W}_{\ell+1}(\mathbb{F}_{p^t})$ of a finite field $\mathbb{F}_{p^t}$. We will make use of the fact that this Witt ring is isomorphic to the Galois ring $G_{\ell+1,t}$ (see Appendix A.6.1), which can be represented as follows.

Lemma 4.3.7. *Let p be a prime, let $\ell \geq 0$, and let $t \geq 1$. There exists a monic polynomial $h \in \mathbb{Z}/\langle p^{\ell+1}\rangle[x]$ of degree t, dividing $x^{p^t}-1$ in $\mathbb{Z}/\langle p^{\ell+1}\rangle[x]$, such that $\overline{h} := h \pmod{\langle p\rangle}$ is irreducible in $\mathbb{F}_p[x]$ and $\overline{\xi} := x + \langle \overline{h}\rangle$ is a primitive (p^t-1)-th root of unity in $\mathbb{F}_p[x]/\langle \overline{h}\rangle$. Then we have isomorphisms*

$$G_{\ell+1,t} \cong \mathbb{Z}/\langle p^{\ell+1}\rangle[x]/\langle h\rangle \qquad \text{and} \qquad \mathbb{F}_{p^t} \cong \mathbb{F}_p[x]/\langle \overline{h}\rangle,$$

and $\xi := x + \langle h\rangle$ is a primitive (p^t-1)-th root of unity in $G_{\ell+1,t}$.

Proof. This follows from the proof of [Wan03, Theorem 14.8]. □

The idea of the algorithm is that, by the explicit Witt-Jacobian Criterion, given circuits $C_1, \ldots, C_m$ over $\mathbb{F}_q[\boldsymbol{x}]$ are algebraically independent over $\mathbb{F}_q$ if and only if the associated $(\ell+1)$-th Witt-Jacobian polynomial with respect to some $\boldsymbol{x}_I$, where $I \in \binom{[n]}{m}$, has a term $\boldsymbol{x}^\alpha$ whose coefficient is not divisible by $p^{\min\{v_p(\alpha),\ell\}+1}$. A non-deterministic Turing machine can guess I and α. The computationally hardest part consists of computing the coefficient of $\boldsymbol{x}^\alpha$. For this step, we use the interpolation formula in the following lemma which is motivated by [KS11b, Theorem IV.1]. The formula comprises an exponential number of summands, but can be computed with the help of a #**P**-oracle.

Lemma 4.3.8. *In the situation of Lemma 4.3.7, let $f \in G_{\ell+1,t}[z]$ be a polynomial of degree at most p^t-2. Then the coefficient of z^d in f is given by*

$$(p^t-1)^{-1} \cdot \sum_{i=0}^{p^t-2} \xi^{-id} \cdot f(\xi^i) \in G_{\ell+1,t}$$

for all $d \in [0, p^t-2]$.

Proof. Set $u := p^t - 1 \in \mathbb{N}_{>0}$. Note that u is a unit in $G_{\ell+1,t}$, because $u \notin \langle p\rangle$. It suffices to show that $\sum_{i=0}^{u-1} \xi^{-id}\xi^{ij} = u \cdot \delta_{d,j}$ for all $d, j \in [0, u-1]$. This is clear for $d = j$, so let $d \neq j$. Then $\sum_{i=0}^{u-1} \xi^{-id}\xi^{ij} = \sum_{i=0}^{u-1} \xi^{i(j-d)} = 0$, because ξ^{j-d} is a u-th root of unity $\neq 1$ and $\xi^{j-d}-1$ is a non-zerodivisor in $G_{\ell+1,t}$. □

Now we can state the algorithm, whose steps are explained in more detail in the proof beneath. Note that the algorithm makes just a single call to the #**P**-oracle.

Algorithm 4.3.9 (Algebraic independence testing over finite fields)**.**
Input: Arithmetic circuits $C_1, \ldots, C_m$ over $K[x_1, \ldots, x_n]$, where and K is a finite field.
Acceptance: If $C_1, \ldots, C_m$ are algebraically independent over K, then there exists an accepting computation path, otherwise all computation paths reject.

(1) Set $s \leftarrow \max_{1\le i\le m}|C_i|$, $\delta \leftarrow s^s$, $\ell \leftarrow \lfloor m \log_p \delta \rfloor$, and $D \leftarrow m\delta^{m+1}+1$. Let $t \ge 1$ be the least multiple of $\log_p|K|$ such that $p^t > D^n$.

(2) Using non-determinism, guess a monic polynomial $h \in \mathbb{Z}/\langle p^{\ell+1}\rangle[x]$ of degree t. Let $\overline{h} \in \mathbb{F}_p[x]$ such that $\overline{h} = h \pmod{\langle p\rangle}$, and set $\xi \leftarrow x + \langle h\rangle$ and $\overline{\xi} \leftarrow x + \langle \overline{h}\rangle$. Check that h divides $x^{p^t-1}-1$ in $\mathbb{Z}/\langle p^{\ell+1}\rangle[x]$, $\overline{h}$ is irreducible in $\mathbb{F}_p[x]$, and $\overline{\xi}$ has order p^t-1 in $\mathbb{F}_p[x]/\langle\overline{h}\rangle$ (for the last test, also guess a prime factorization of p^t-1), otherwise reject. Finally, set $G_{\ell+1,t} \leftarrow \mathbb{Z}/\langle p^{\ell+1}\rangle[x]/\langle h\rangle$ and $\mathbb{F}_{p^t} \leftarrow \mathbb{F}_p[x]/\langle\overline{h}\rangle$, and compute an embedding $K \subseteq \mathbb{F}_{p^t}$.

(3) Using non-determinism, guess $I \in \binom{[n]}{m}$ and $\alpha \in [0, D-1]^n$.

(4) Compute arithmetic circuits $C'_1, \ldots, C'_m$ over $G_{\ell+1,t}[\boldsymbol{x}]$ such that $C_i = C'_i \pmod{\langle p\rangle_{G_{\ell+1,t}[\boldsymbol{x}]}}$ for all $i \in [m]$.

(5) Compute an arithmetic circuit C over $G_{\ell+1,t}[\boldsymbol{x}]$ for the Witt-Jacobian polynomial $\mathrm{WJP}_{\ell+1,\boldsymbol{x}_I}(C'_1, \ldots, C'_m)$.

(6) Compute an arithmetic circuit C' over $G_{\ell+1,t}[z]$ for the Kronecker substitution $C\big(z, z^D, \ldots, z^{D^{n-1}}\big)$ and set $d \leftarrow \sum_{i=1}^n \alpha_i D^{i-1} \in \mathbb{N}$.

(7) Using a #**P**-oracle, compute

$$c \leftarrow \sum_{i=0}^{p^t-2} \xi^{-id} \cdot C'(\xi^i) \in G_{\ell+1,t}. \tag{4.3.1}$$

(8) If c is divisible by $p^{\min\{v_p(\alpha),\ell\}+1}$ in $G_{\ell+1,t}$, then reject, otherwise accept.

Proof of Theorem 4.3.6. We show that Algorithm 4.3.9 works correctly and can be implemented to run in polynomial time on a non-deterministic Turing machine with a #**P**-oracle. For this, we use the notation of the algorithm and, in addition, set $u := p^t - 1 \in \mathbb{N}_{>0}$.

In step (1), various constants are computed satisfying the following estimates. By Lemma 2.2.4, we have $\deg(C_i) \le \delta$ for all $i \in [m]$. Consequently, we obtain $\deg(C) \le m\delta(p^\ell-1) + m + m(\delta-1) \le m\delta^{m+1} < D$ and $\deg_z(C') \le D^n - 1 \le u - 1$.

In step (2), representations of the Galois ring $G_{\ell+1,t}$ and the field $\mathbb{F}_{p^t}$ are computed according to Lemma 4.3.7. The irreducibility of $\overline{h}$ can be tested efficiently by checking whether $\gcd(\overline{h}, x^{p^i} - x) = 1$ in $\mathbb{F}_p[x]$ for all $i \in \{1, \ldots, \lfloor t/2\rfloor\}$ (see Lemma A.3.5). For the order test, verify $\overline{\xi}^i \ne 1$ for all maximal divisors i of u (using its prime factorization). An embedding $K \subseteq \mathbb{F}_{p^t}$ can be computed efficiently as described in [Len91, §2] and is used to convert the constants of the input circuits into the new representation.

In step (3), an index set I and an exponent vector α are chosen non-deterministically to determine a monomial of a Witt-Jacobian polynomial whose degeneracy condition is checked in the subsequent steps of the algorithm.

The arithmetic circuits $C'_1, \ldots, C'_m$ in step (4) can be computed by lifting all constants $\overline{a} \in \mathbb{F}_{p^t}$ of $C_1, \ldots, C_m$ to some $a \in G_{\ell+1,t}$ with $\overline{a} = a \pmod{\langle p \rangle}$. Since $G_{\ell+1,t}$ is a free $\mathbb{Z}/\langle p^{\ell+1} \rangle$-module with basis $1, \xi, \ldots, \xi^{t-1}$, this lifting can be done coordinate-wise in our representation.

To compute the arithmetic circuit C in step (5) in polynomial time, we use [BS83] for the partial derivatives, the Berkowitz algorithm (see Lemma A.3.1) for the determinant, and repeated squaring for the high power.

The Kronecker substitution in step (6) can be computed again by repeated squaring. Since $\deg(C) < D$, Lemma 2.6.2 implies that the coefficient of $\boldsymbol{x}^\alpha$ in C equals the coefficient of z^d in C'. Since $\deg_z(C') \leq u - 1$, this coefficient is $u^{-1}c$ by Lemma 4.3.8. Since u is a unit in $G_{\ell+1,t}$, Theorem 4.1.24 implies that the test in step (8) correctly decides the algebraic independence of $C_1, \ldots, C_m$.

It remains to show that the computation of c in step (7) can be performed in polynomial time with the help of a $\#\mathbf{P}$-oracle. For $i \in [0, u-1]$, the summand $c_i := \xi^{-id} \cdot C'(\xi^i) \in G_{\ell+1,t}$ of (4.3.1) can be written as $c_i = \sum_{j=0}^{t-1} c_{i,j} \xi^j$ with $c_{i,j} \in \mathbb{Z}/\langle p^{\ell+1} \rangle$. Therefore, each c_i can be represented by a tuple $\boldsymbol{c}_i \in [0, p^{\ell+1} - 1]^t$ of integers, and a desired representation of c is given by the component-wise integer sum $\boldsymbol{c} := \sum_{i=0}^{u-1} \boldsymbol{c}_i \in [0, N-1]^t$, where $N := u \cdot p^{\ell+1} \in \mathbb{N}$. Those tuples can be encoded into single integers via the bijection

$$\iota \colon [0, N-1]^t \to [0, N^t - 1], \quad (n_0, \ldots, n_{t-1}) \mapsto \sum_{j=0}^{t-1} n_j N^j$$

from Lemma 2.6.2. This bijection and its inverse are efficiently computable, and we have $\iota(\boldsymbol{c}) = \sum_{i=0}^{u-1} \iota(\boldsymbol{c}_i)$. Hence it suffices to show that $\iota(\boldsymbol{c})$ can be computed in $\#\mathbf{P}$. To this end, we design a non-deterministic polynomial-time Turing machine that, given $G_{\ell+1,t}$, ξ and C' as input, has exactly $\iota(\boldsymbol{c})$ accepting computation paths for the corresponding $\boldsymbol{c}$. First we branch non-deterministically over all integers $i \in [0, u-1]$. In each branch i, we compute c_i. This can be done in polynomial time, because C' can be efficiently evaluated and the powers of ξ can be obtained by repeated squaring. If $\iota(\boldsymbol{c}_i) = 0$, we reject, otherwise we branch again non-deterministically into exactly $\iota(\boldsymbol{c}_i)$ computation paths that all accept. This implies that the machine has altogether $\sum_{i=0}^{u-1} \iota(\boldsymbol{c}_i) = \iota(\boldsymbol{c})$ accepting computation paths. □

4.4 Computation of Algebraic Relations

In the final section of this chapter we investigate the complexity of computing the algebraic relations of arithmetic circuits.

Exponential-space computation of algebraic relations

Let K be a field and let $K[\boldsymbol{x}] = K[x_1, \ldots, x_n]$ be a polynomial ring over K. The algebraic relations $\mathrm{AlgRel}_{K[\boldsymbol{y}]}(f_1, \ldots, f_m)$ of polynomials $f_1, \ldots, f_m \in K[\boldsymbol{x}]$ can be expressed as an elimination ideal in $K[\boldsymbol{x}, \boldsymbol{y}]$.

Lemma 4.4.1 ([KR00, Corollary 3.6.3])**.** *Let $f_1, \ldots, f_m \in K[\boldsymbol{x}]$ be polynomials. Then we have*

$$\mathrm{AlgRel}_{K[\boldsymbol{y}]}(f_1, \ldots, f_m) = \langle y_1 - f_1, \ldots, y_m - f_m \rangle_{K[\boldsymbol{x},\boldsymbol{y}]} \cap K[\boldsymbol{y}], \qquad (4.4.1)$$

where $\boldsymbol{y} = \{y_1, \ldots, y_m\}$ are new variables.

This elimination ideal can be computed via Gröbner basis methods (for an introduction to Gröbner bases, we refer to [KR00]). Since Gröbner bases can be computed in exponential space [KM96], we obtain the following theorem.

Theorem 4.4.2. *Let $K = \mathbb{Q}$ or $K = \mathbb{F}_q$ for some prime power q. Then there exists an exponential-space bounded Turing machine that, given arithmetic circuits $C_1, \ldots, C_m$ over $K[\boldsymbol{x}]$, computes a generating system of the ideal $\mathrm{AlgRel}_{K[\boldsymbol{y}]}(C_1, \ldots, C_m)$.*

Proof sketch. Let $C_1, \ldots, C_m$ be arithmetic circuits over $K[\boldsymbol{x}]$ and denote $J := \langle y_1 - C_1, \ldots, y_m - C_m \rangle_{K[\boldsymbol{x},\boldsymbol{y}]}$. By Lemma 4.4.1, we have

$$\mathrm{AlgRel}_{K[\boldsymbol{y}]}(C_1, \ldots, C_m) = J \cap K[\boldsymbol{y}].$$

Let σ be a term ordering on $\mathbb{T}(\boldsymbol{x}, \boldsymbol{y})$ which is an elimination ordering for $\boldsymbol{x}$. Let $G \subset K[\boldsymbol{x}, \boldsymbol{y}]$ be a σ-Gröbner basis of J. Then, by [KR00, Theorem 3.4.5 (b)], $G \cap K[\boldsymbol{y}]$ is a σ'-Gröbner basis of $J \cap K[\boldsymbol{y}]$, where σ' is the restriction of σ to $\mathbb{T}(\boldsymbol{y})$.

Let $s := \sum_{i=1}^{m} \mathrm{size}(C_i)$ and let $\delta := s^s$. By Lemma 2.2.4, we have $\deg(y_i - C_i) \leq \delta$ for all $i \in [m]$.

First let $K = \mathbb{Q}$. The bit-size of the coefficients of $y_1 - C_1, \ldots, y_m - C_m$ is bounded by $B := s^{s+1}$. By [KM96], a σ-Gröbner basis $G \subset K[\boldsymbol{x}, \boldsymbol{y}]$ of J can be computed in space $\mathrm{poly}\big(2^n, \log m, \log \delta, B\big) = \mathrm{poly}\big(2^n, s^s\big)$ (in [KM96] the input polynomials are given in sparse representation, but we can compute the coefficients of $y_1 - C_1, \ldots, y_m - C_m$ in space $\mathrm{poly}(s^s)$). This algorithm can be modified to output just the polynomials in G that contain no $\boldsymbol{x}$-variables.

If $K = \mathbb{F}_q$ for some prime power q, then the algorithm in [KM96] works *mutatis mutandis*. Most notably, the underlying degree bound for Gröbner bases in [Dub90] holds over any field. □

Remark 4.4.3. The exponential-space upper bound for computing Gröbner bases is best possible [MM82]. However, it is conceivable that the computation of elimination ideals of the shape (4.4.1) is easier.

Hardness of computing minimal polynomials

Kayal obtained hardness results connected with the computation of annihilating polynomials [Kay09]. We prove one of his results in a slightly generalized setting.

Let K be a field and let $K[\boldsymbol{x}] = K[x_1, \ldots, x_n]$ be a polynomial ring over K. We consider a situation where we have a more reasonable bound on the size of a generating system of the algebraic relations than in the general case. Let $f_1, \ldots, f_m \in K[\boldsymbol{x}]$ be polynomials such that $\operatorname{trdeg}_K(f_1, \ldots, f_m) = m - 1$. Then, by Lemma 4.1.6, the ideal $\operatorname{AlgRel}_{K[\boldsymbol{y}]}(f_1, \ldots, f_m)$ is generated by a minimal polynomial $F \in K[\boldsymbol{y}]$ of $f_1, \ldots, f_m$ (recall Definition 4.1.7). If $K = \mathbb{Q}$ or $K = \mathbb{F}_q$ for some prime power q, then the degree bound for annihilating polynomials implies that a minimal polynomial of arithmetic circuits $C_1, \ldots, C_m$ of transcendence degree $m - 1$ can be computed in polynomial space.

The following theorem gives evidence that the computation of minimal polynomials is hard [Kay09, Section V]. It shows that, if ϕ is a boolean circuit over $\boldsymbol{x}$ with arithmetization $\operatorname{arith}_\phi$, then a minimal polynomial of $\operatorname{arith}_\phi$, $x_1^2 - x_1, \ldots, x_n^2 - x_n$ encodes information about the number of satisfying assignments of ϕ. Recall that computing this number is a $\#\mathbf{P}$-hard problem [AB09, Theorem 17.10].

Theorem 4.4.4. *Let ϕ be a boolean circuit over $\boldsymbol{x}$ and let $N \in [0, 2^n]$ be the number of satisfying assignments of ϕ. Let $C := \operatorname{arith}_\phi \in K[\boldsymbol{x}]$ be the arithmetization of ϕ and let $f_i := x_i^2 - x_i \in K[\boldsymbol{x}]$ for $i \in [n]$. Let $F \in K[y, y_1, \ldots, y_n]$ be a minimal polynomial of $C, f_1, \ldots, f_n$. Then we have*

$$F(y, 0, \ldots, 0)^k = c \cdot (y - 1)^N \cdot y^{2^n - N}$$

for some $k \geq 1$ and $c \in K^*$.

Before we give the proof of this theorem, we draw some consequences. Let $K = \mathbb{Q}$ or $K = \mathbb{F}_q$ for some prime power q. Suppose we were able to efficiently compute an arithmetic circuit G for the polynomial $F(y, 0, \ldots, 0) \in K[y]$ of encoding size $\operatorname{poly}(|\phi|, n)$. Then, by checking whether $G(1) = 0$, we could

decide the satisfiability of ϕ, an **NP**-hard problem. Note that, in contrast to [Kay09], we do not require G to be monic. Therefore, in the case $K = \mathbb{Q}$, the only efficient test for the zeroness of $G(1)$ we know of is a randomized check.

Now let $K = \mathbb{Q}$. We have

$$\frac{G(-1)G(2)}{G(1/2)^2} = 2^{3\cdot 2^n/k} \quad \text{and} \quad \frac{G(-1)^4}{G(1/2)^2 G(2)^2} = 2^{6N/k}.$$

Using random modular evaluations of G, it is possible to efficiently extract the exponents $3 \cdot 2^n/k$ and $6N/k$ (cf. the proof of [Kay09, Claim 15.2]) from which we obtain N. This implies that computing an arithmetic circuit for G (more precisely, a suitably defined function problem) is even #**P**-hard under randomized reductions (cf. [Kay09, Theorem 15]; note that we do neither require G to be monic nor to be over $\mathbb{Z}$).

For the proof of Theorem 4.4.4 we set up some notation. Let σ be a term ordering on $\mathbb{T}(\boldsymbol{x})$, let $\delta_1, \ldots, \delta_n \geq 1$, and let $f_1, \ldots, f_n \in K[\boldsymbol{x}]$ be polynomials such that $\mathrm{lt}_\sigma(f_i) = x_i^{\delta_i}$ for all $i \in [n]$. Moreover, let $\boldsymbol{b} = (b_1, \ldots, b_s) \in \overline{K}^n$. By Lemma 4.1.3, $f_1 - b_1, \ldots, f_n - b_n$ are algebraically independent over K. Define the ideal

$$I^{\boldsymbol{b}} := \langle f_1 - b_1, \ldots, f_n - b_n \rangle_{\overline{K}[\boldsymbol{x}]}.$$

By [KR00, Corollary 2.5.10], $\{f_1 - b_1, \ldots, f_n - b_n\}$ is a σ-Gröbner basis of $I^{\boldsymbol{b}}$, and by [KR00, Proposition 3.7.1], $I^{\boldsymbol{b}}$ is a zero-dimensional ideal, hence $A^{\boldsymbol{b}} := \overline{K}[\boldsymbol{x}]/I^{\boldsymbol{b}}$ is finite-dimensional as a $\overline{K}$-vector space. More precisely, $B^{\boldsymbol{b}} := B + I^{\boldsymbol{b}}$ is a $\overline{K}$-basis of $A^{\boldsymbol{b}}$, where

$$B := \left\{ \boldsymbol{x}^\alpha \mid \alpha \in [0, \delta_1 - 1] \times \cdots \times [0, \delta_n - 1] \right\} \subset \mathbb{T}(\boldsymbol{x}),$$

in particular, we have $\dim_{\overline{K}}(A^{\boldsymbol{b}}) = \delta_1 \cdots \delta_n =: d$.

Now let $f \in K[\boldsymbol{x}]$ be another polynomial. Multiplication by f in $A^{\boldsymbol{b}}$ yields a $\overline{K}$-linear map

$$m_f^{\boldsymbol{b}} \colon A^{\boldsymbol{b}} \to A^{\boldsymbol{b}}, \quad g + I^{\boldsymbol{b}} \mapsto fg + I^{\boldsymbol{b}}.$$

Let $M_f^{\boldsymbol{b}} \in \overline{K}^{d \times d}$ be the matrix of $m_f^{\boldsymbol{b}}$ with respect to $B^{\boldsymbol{b}}$ and let $\chi_{M_f^{\boldsymbol{b}}} \in \overline{K}[y]$ be the characteristic polynomial of $M_f^{\boldsymbol{b}}$.

Let $\boldsymbol{a} \in \mathcal{V}_{\overline{K}^n}(I^{\boldsymbol{b}})$ and let $A_{\boldsymbol{a}}^{\boldsymbol{b}} := U_{\boldsymbol{a}}^{-1} A^{\boldsymbol{b}}$ be the localization of $A^{\boldsymbol{b}}$ with respect to the multiplicatively closed set

$$U_{\boldsymbol{a}} := \left\{ f + I^{\boldsymbol{b}} \mid f \in \overline{K}[\boldsymbol{x}] \text{ such that } f(\boldsymbol{a}) \neq 0 \right\} \subset A^{\boldsymbol{b}}.$$

The number $\mu(\boldsymbol{a}) := \dim_{\overline{K}}(A_{\boldsymbol{a}}^{\boldsymbol{b}}) \in \mathbb{N}_{>0}$ is called the **multiplicity** of $\boldsymbol{a}$.

Theorem 4.4.5 (Stickelberger's Theorem)**.** *Let* $\mathcal{V}_{\overline{K}^n}(I^{\boldsymbol{b}}) = \{\boldsymbol{a}_1, \ldots, \boldsymbol{a}_m\}$. *Then we have* $A^{\boldsymbol{b}} \cong \prod_{i=1}^m A^{\boldsymbol{b}}_{\boldsymbol{a}_i}$ *and* $\chi_{M_f^{\boldsymbol{b}}} = \prod_{i=1}^m (y - f(\boldsymbol{a}_i))^{\mu(\boldsymbol{a}_i)}$.

Proof. For $\operatorname{char}(K) = 0$, this is [BPR06, Theorem 4.94 and Theorem 4.98]. The assumption on the characteristic is only used in [BPR06, Lemma 4.90], however, the fact that $\overline{K}$ is infinite is sufficient. □

The following lemma sheds light on the connection between minimal polynomials of $f, f_1, \ldots, f_n$ and the characteristic polynomial of $M_f^{\boldsymbol{b}}$.

Lemma 4.4.6. *Let* $\boldsymbol{b} \in \overline{K}^n$ *and let* $F \in K[y, y_1, \ldots, y_n]$ *be a minimal polynomial of* $f, f_1, \ldots, f_n$. *Then* $F(y, \boldsymbol{b})^k = c \cdot \chi_{M_f^{\boldsymbol{b}}}$ *for some* $k \geq 1$ *and* $c \in K^*$.

Proof. Let $\boldsymbol{y} := \{y_1, \ldots, y_n\}$ and define

$$I^{\boldsymbol{y}} := \big\langle f_1 - y_1, \ldots, f_n - y_n \big\rangle_{\overline{K(\boldsymbol{y})}[\boldsymbol{x}]}.$$

Then $A^{\boldsymbol{y}} := \overline{K(\boldsymbol{y})}[\boldsymbol{x}]/I^{\boldsymbol{y}}$ is finite-dimensional as a $\overline{K(\boldsymbol{y})}$-vector space. More precisely, $B^{\boldsymbol{y}} := B + I^{\boldsymbol{y}}$ is a $\overline{K(\boldsymbol{y})}$-basis of $A^{\boldsymbol{y}}$, hence $\dim_{\overline{K(\boldsymbol{y})}}(A^{\boldsymbol{y}}) = d$. Let

$$m_f^{\boldsymbol{y}} \colon A^{\boldsymbol{y}} \to A^{\boldsymbol{y}}, \quad g + I^{\boldsymbol{y}} \mapsto fg + I^{\boldsymbol{y}}$$

and let $M_f^{\boldsymbol{y}} \in \overline{K(\boldsymbol{y})}^{d \times d}$ be the matrix of $m_f^{\boldsymbol{y}}$ with respect to $B^{\boldsymbol{y}}$. Let $\boldsymbol{x}^\alpha \in B$. By [KR00, Corollary 2.5.10], $\{f_1 - y_1, \ldots, f_n - y_n\} \subset K[\boldsymbol{y}][\boldsymbol{x}]$ is a σ-Gröbner basis of $I^{\boldsymbol{y}}$ with monic leading terms. By the Division Algorithm [KR00, Theorem 1.6.4], there exist polynomials $q_1, \ldots, q_n, r \in K[\boldsymbol{y}][\boldsymbol{x}]$ such that $f \cdot \boldsymbol{x}^\alpha = q_1(f_1 - y_1) + \cdots + q_n(f_n - y_n) + r$ and $\operatorname{Supp}(r) \subseteq B$. This shows that, in fact, we have $M_f^{\boldsymbol{y}} \in K[\boldsymbol{y}]^{d \times d}$ and $M_f^{\boldsymbol{b}} = M_f^{\boldsymbol{y}}(\boldsymbol{b})$ for all $\boldsymbol{b} \in \overline{K}^n$. In particular, we have $\chi_{M_f^{\boldsymbol{y}}} \in K[y, \boldsymbol{y}]$ and $\chi_{M_f^{\boldsymbol{b}}} = \chi_{M_f^{\boldsymbol{y}}}(y, \boldsymbol{b})$.

Now we want to show that F vanishes on $\mathcal{V}_{\overline{K}^{n+1}}(\chi_{M_f^{\boldsymbol{y}}})$. To this end, let $(c_0, \boldsymbol{c}) = (c_0, c_1, \ldots, c_n) \in \mathcal{V}_{\overline{K}^{n+1}}(\chi_{M_f^{\boldsymbol{y}}})$. Then $\chi_{M_f^{\boldsymbol{c}}}(c_0) = \chi_{M_f^{\boldsymbol{y}}}(c_0, \boldsymbol{c}) = 0$. Thus, c_0 is an eigenvalue of $M_f^{\boldsymbol{c}}$. By Theorem 4.4.5, there exists $\boldsymbol{a} \in \mathcal{V}_{\overline{K}^n}(I^{\boldsymbol{c}})$ such that $f(\boldsymbol{a}) = c_0$. Therefore, we have $F(c_0, \boldsymbol{c}) = \big(F(f, f_1, \ldots, f_n)\big)(\boldsymbol{a}) = 0$.

By Hilbert's Nullstellensatz (see Theorem A.4.1), F is in the radical of $\langle \chi_{M_f^{\boldsymbol{y}}} \rangle_{K[y, \boldsymbol{y}]}$, and since F is irreducible, there exist $k \geq 1$ and $c \in K^*$ such that $F^k = c \cdot \chi_{M_f^{\boldsymbol{y}}}$. We conclude $F(y, \boldsymbol{b})^k = c \cdot \chi_{M_f^{\boldsymbol{y}}}(y, \boldsymbol{b}) = c \cdot \chi_{M_f^{\boldsymbol{b}}}$. □

Proof of Theorem 4.4.4. We have $\mathcal{V}_{\overline{K}^n}(f_1, \ldots, f_n) = \{0, 1\}^n$, thus $m = 2^n = d$ (with the notation above). By Theorem 4.4.5, we have $\mu(\boldsymbol{a}) = 1$ for all $\boldsymbol{a} \in \{0, 1\}^n$ and, together with Lemma 2.3.6 (a), we obtain

$$\chi_{M_C^{\mathfrak{o}}} = \prod_{\boldsymbol{a} \in \{0,1\}^n} (y - C(\boldsymbol{a})) = (y - 1)^N \cdot y^{2^n - N}.$$

Therefore, the assertion follows from Lemma 4.4.6. □

Chapter 5

Conclusion

In this thesis we used the concept of faithful homomorphisms to construct hitting sets for various classes of arithmetic circuits. By those techniques, we also obtained a promising blackbox algorithm candidate for $\Sigma_k\Pi_d\Sigma\Pi_\delta$-circuits, when k and δ are constants. To be useful, a good upper bound for $R_\delta(k,d)$ has to be found (see Conjecture 4.2.36). Even bounds for the special cases $k = 3$ and $\delta = 2$ would be interesting. Another direction for research on small-depth PIT is to consider $\Sigma_k\Pi_\delta\Sigma$-circuits with unbounded top fan-in k.

Another question that has not yet been answered in a satisfactory way is the complexity status of algebraic independence testing over a finite field $\mathbb{F}_q$. Using the Witt-Jacobian Criterion, we could make some progress by showing $\mathsf{AlgIndep}_{\mathbb{F}_q} \in \mathbf{NP}^{\#\mathbf{P}}$. We conjecture, however, that $\mathsf{AlgIndep}_{\mathbb{F}_q} \in \mathbf{BPP}$. This could be shown by devising an efficient randomized test for non-degeneracy of Witt-Jacobian polynomials. It was shown by Stefan Mengel that testing 2-degeneracy of general arithmetic circuits is hard [MSS12]. It is conceivable that degeneracy testing of Witt-Jacobian polynomials is easier due to their special shape.

Appendix A

Preliminaries

A.1 Notation

We fix some notation.

Sets

By $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ we denote the sets of non-negative integers, integers, rational numbers, real numbers, and complex numbers, respectively.

The power set of a set S will be denoted by 2^S, and, for $k \geq 0$, the set of k-subsets of S will be denoted by $\binom{S}{k}$. If S is a subset of T, we write $S \subseteq T$, and if S is a strict subset of T, we write $S \subset T$.

For $m, n \in \mathbb{Z}$, we define $[m, n] := \{m, m+1, \ldots, n\}$ (with the convention $[m, n] = \varnothing$ if $m > n$) and $[n] := [1, n]$. The group of permutations $[n] \to [n]$ will be denoted by $\mathfrak{S}_n$ for $n \geq 1$.

Asymptotic notation

Let $f, g \colon \mathbb{N}^k \to \mathbb{R}_{\geq 0}$ be functions. We write $g = O(f)$ if there exist $c > 0$ and $N \geq 0$ such that $g(n_1, \ldots, n_k) \leq c \cdot f(n_1, \ldots, n_k)$ for all $n_1, \ldots, n_k \geq N$. If $f = O(g)$, then we write $g = \Omega(f)$. Finally, if $g = O(f)$ and $f = O(g)$, then we write $g = \Theta(f)$.

Let $f_1, \ldots, f_m \colon \mathbb{N}^k \to \mathbb{R}_{\geq 0}$ be functions and let $g \colon \mathbb{N}^{mk} \to \mathbb{R}_{\geq 0}$ be another function. We write $g = \mathrm{poly}(f_1, \ldots, f_m)$ if there exists a fixed polynomial $F \in \mathbb{N}[x_1, \ldots, x_m]$ such that $g = O\big(F(f_1, \ldots, f_m)\big)$.

Prime numbers

We denote the set of **prime numbers** by $\mathbb{P}$. The following theorem gives a lower bound on the number of primes in an interval.

Theorem A.1.1 ([RS62, Corollary 1, (3.5)])**.** *Let $k \geq 17$. Then we have*

$$|[k] \cap \mathbb{P}| > k/\log k.$$

Corollary A.1.2. *Let $k \geq 2$. Then we have*

(a) $|[2^k] \cap \mathbb{P}| \geq 2^k/k$, *and*

(b) $|[k^2] \cap \mathbb{P}| \geq k$.

Proof. Since $[16] \cap \mathbb{P} = \{2, 3, 5, 7, 11, 13\}$, (a) and (b) hold for $k = 2, 3, 4$. For $k \geq 5$, (a) and (b) follow from Theorem A.1.1. □

A.2 Complexity Theory

The model of computation for the complexity considerations in this thesis is that of Turing machines. For the definition of **deterministic**, **nondeterministic**, and **probabilistic Turing machines**, we refer to the standard references [Pap94, AB09]. Furthermore, we assume familiarity with the complexity classes in the tower

$$\mathbf{L} \subseteq \mathbf{NL} \subseteq \mathbf{P} \subseteq \mathbf{NP} \subseteq \mathbf{PH} \subseteq \mathbf{PSPACE} \subseteq \mathbf{EXP} \subseteq \mathbf{EXPSPACE}.$$

We say that problems in **P** can be decided **efficiently**.

Randomized computation

The complexity class **RP** consists of problems for which there exists a randomized polynomial-time Turing machine that accepts yes-instances with probability $\geq 1/2$ and always rejects no-instances. Similarly, the class **coRP** consists of problems for which there exists a randomized polynomial-time Turing machine that always accepts yes-instances and rejects no-instances with probability $\geq 1/2$. The classes **RP** and **coRP** represent the problems that can be solved by **efficient randomized** algorithms with one-sided error. We have $\mathbf{P} \subseteq \mathbf{RP} \subseteq \mathbf{NP}$ and $\mathbf{P} \subseteq \mathbf{coRP} \subseteq \mathbf{coNP}$. Finally, problems in $\mathbf{ZPP} := \mathbf{RP} \cap \mathbf{coRP}$ can be solved by algorithms that never err, but run in expected polynomial time.

The complexity class **BPP** consists of problems for which there exists a randomized polynomial-time Turing machine that accepts yes-instances with probability $\geq 2/3$ and accepts no-instances with probability $\leq 1/3$. It represents the class of problems that can be solved by efficient randomized algorithms with two-sided error. We have $\mathbf{RP} \subseteq \mathbf{BPP}$ and $\mathbf{coRP} \subseteq \mathbf{BPP}$. It is known that **BPP** is in the second level of the polynomial hierarchy, but it is conjectured that $\mathbf{BPP} = \mathbf{P}$.

Parallel computation

We say that a problem can be decided **efficiently in parallel**, if it can be decided in polylogarithmic time on a parallel random-access machine (PRAM) with a polynomial number of processors. The class of those problems is denoted by **NC**. We have $\mathbf{NL} \subseteq \mathbf{NC} \subseteq \mathbf{P}$. The complexity classes **RNC** and **coRNC** are randomized versions of **NC** with one-sided error and are defined analogously to **RP** and **coRP**. It is conjectured that $\mathbf{RNC} = \mathbf{NC}$.

Complexity of counting

The complexity class $\#\mathbf{P}$ was defined in [Val79] and is the set of functions $f\colon \{0,1\}^* \to \mathbb{N}$ for which there exists a non-deterministic polynomial-time Turing machine that on input $x \in \{0,1\}^*$ has exactly $f(x)$ accepting computation paths. In Section 4.3 we consider the complexity class $\mathbf{NP}^{\#\mathbf{P}}$ of problems whose yes-instances are accepted by a non-deterministic polynomial-time Turing machine with an **oracle** for a $\#\mathbf{P}$-function. We have the inclusions

$$\mathbf{PH} \subseteq \mathbf{P}^{\#\mathbf{P}} \subseteq \mathbf{NP}^{\#\mathbf{P}} \subseteq \mathbf{PSPACE}.$$

A.3 Rings, Modules, and Algebras

In this thesis, "ring" means commutative ring with unity, unless stated otherwise. We denote the group of units of a ring R by R^*.

Let R be a ring, let M be an R-module, and let $S \subseteq M$ be a subset. Then we write $\langle S \rangle_R$ for the submodule of M generated by S. If $M = R$ is a ring, this means that $\langle S \rangle_R$ is the ideal generated by S. If $R = K$ is a field, then M is a K-vector space and $\langle S \rangle_K$ denotes the K-subspace of M spanned by S.

Let R be a ring. An **R-algebra** is a ring A together with a structural homomorphism $R \to A$. Given a subset $S \subseteq A$, we write $R[S]$ for the R-subalgebra of A generated by S. Now let $R = K$ be a field. Then a K-algebra $\neq \{0\}$ is a ring containing K as a subring. A finitely generated K-algebra is called **affine K-algebra**, and an affine K-algebra which is an integral domain is called **affine K-domain**.

A.3.1 Matrices and Determinants

In this section we introduce some notation for matrices and collect a few lemmas concerning determinants.

Let R be a ring and let $A = \big(a_{i,j}\big)_{i,j} \in R^{m\times n}$ be a matrix. For non-empty index sets $I \subseteq [m]$ and $J \subseteq [n]$, we call $A_{I,J} := \big(a_{i,j}\big)_{i\in I, j\in J} \in R^{|I|\times|J|}$ the **submatrix** of A indexed by I and J.

Now let $B \in R^{r\times s}$ be another matrix. Then the **Kronecker product** of A and B is defined as the block matrix

$$A \otimes B := \begin{pmatrix} a_{1,1}B & \cdots & a_{1,n}B \\ \vdots & & \vdots \\ a_{m,1}B & \cdots & a_{m,n}B \end{pmatrix} \in K^{mr\times ns}.$$

The following result is due to Berkowitz [Ber84]. It gives rise to an efficient, parallelizable, and division-free algorithm for the computation of determinants.

Lemma A.3.1 (Berkowitz's Algorithm, [Sol02, §2])**.** *Let R be a ring and let $A = \big(a_{i,j}\big) \in R^{n\times n}$. For $k \in [n]$, define the matrix $B^{(k)} = \big(b^{(k)}_{i,j}\big) \in R^{(n+2-k)\times(n+1-k)}$ by*

$$b^{(k)}_{i,j} := \begin{cases} 0, & \text{if } i \le j-1, \\ 1, & \text{if } i = j, \\ -a_{k,k}, & \text{if } i = j+1, \\ -A_{\{k\},[k+1,n]} \cdot A^{i-j-2}_{[k+1,n],[k+1,n]} \cdot A_{[k+1,n],\{k\}}, & \text{if } i \ge j+2, \end{cases}$$

for $i \in [n+2-k]$ and $j \in [n+1-k]$. Denote $(c_n, \ldots, c_0)^\top := B^{(1)} \cdots B^{(n)} \in R^{n+1}$. Then the characteristic polynomial of A is given by

$$\det(yI_n - A) = \sum_{i=0}^{n} c_i y^i \in R[y].$$

In particular, we have $\det(A) = (-1)^n c_0$.

The Cauchy–Binet Formula is a generalization of the product rule for determinants of square matrices.

Lemma A.3.2 (Cauchy–Binet Formula, [Zen93])**.** *Let R be a ring, and let $A \in R^{n\times m}$ and $B \in R^{m\times n}$ be matrices over R. Then*

$$\det(AB) = \sum_{I} \det(A_{[n],I}) \cdot \det(B_{I,[n]}),$$

where the sum is over all $I \in \binom{[m]}{n}$.

Finally, Hadamard's Inequality provides an upper bound for the absolute value of the determinant of a complex matrix.

Lemma A.3.3 (Hadamard's Inequality, [Coh93, Proposition 2.2.4]). *Let $A \in \mathbb{C}^{n\times n}$ be a matrix with columns $a_1, \ldots, a_n \in \mathbb{C}^n$. Then*

$$|\det(A)| \leq \prod_{j=1}^{n} \|a_j\|_2.$$

A.3.2 Polynomial Rings

In this section we fix some notation related to polynomial rings. For more about polynomials we refer to [KR00]. Let $n \geq 1$, let K be a field, and let $K[\boldsymbol{x}] = K[x_1, \ldots, x_n]$ be a polynomial ring over K.

A polynomial of the form $\boldsymbol{x}^\alpha := x_1^{\alpha_1} \cdots x_n^{\alpha_n}$, where $\alpha \in \mathbb{N}^n$ is some **exponent vector**, is called a **term**. The set of all terms is denoted by $\mathbb{T}(\boldsymbol{x})$. A polynomial of the form $c\boldsymbol{x}^\alpha$ for some $c \in K$ and $\alpha \in \mathbb{N}$ is called a **monomial**. Note that some authors define monomial and term conversely.

A polynomial $f \in K[\boldsymbol{x}]$ can be written uniquely as $f = \sum_{\alpha\in\mathbb{N}^n} c_\alpha \boldsymbol{x}^\alpha$, with $c_\alpha \in K$ for all $\alpha \in \mathbb{N}^n$ such that the **support** of f, defined by $\operatorname{Supp}(f) := \{\boldsymbol{x}^\alpha \mid c_\alpha \neq 0\} \subset \mathbb{T}(\boldsymbol{x})$, is finite. We define the **logarithmic support** of f as $\operatorname{LSupp}(f) := \{\alpha \in \mathbb{N}^n \mid c_\alpha \neq 0\}$. The number $\operatorname{sp}(f) := \#\operatorname{Supp}(f) \in \mathbb{N}$ is called the **sparsity** of f. If $\boldsymbol{x}^\alpha \in \operatorname{Supp}(f)$, then $\boldsymbol{x}^\alpha$ is called a term of f and $c_\alpha \boldsymbol{x}^\alpha$ is called a monomial of f.

A **term ordering** σ on $\mathbb{T}(\boldsymbol{x})$ is a well-ordered binary relation $<_\sigma$ on the terms that respects multiplication. We denote the **leading term**, **leading coefficient**, and **leading monomial** of a non-zero polynomial $f \in K[\boldsymbol{x}]$ with respect to σ by $\operatorname{lt}_\sigma(f)$, $\operatorname{lc}_\sigma(f)$, and $\operatorname{lm}_\sigma(f)$, respectively.

Let $f \in K[\boldsymbol{x}]$ be a non-zero polynomial. We denote by $\deg(f)$ the (total) degree of f. For $i \in [n]$, we denote by $\deg_{x_i}(f)$ the degree of f viewed as a polynomial in x_i with coefficients in $K[\boldsymbol{x} \setminus \{x_i\}]$. We do not define the degree of the zero polynomial, though, at some places we will implicitly assume $\deg(0) = -\infty$. Now let $\alpha \in \mathbb{R}^n_{\geq 0}$. For a **weight vector** $w \in \mathbb{N}^n$, we set $|\alpha|_w := \sum_{i=1}^n w_i\alpha_i \in \mathbb{R}_{\geq 0}$. For the weight vector $\mathbf{1} := (1, \ldots, 1) \in \mathbb{N}^n$, we set $|\alpha| := |\alpha|_{\mathbf{1}}$. We define the **$w$-weighted degree** of f as $\deg_w(f) := \max\{|\alpha|_w \mid \alpha \in \operatorname{LSupp}(f)\} \in \mathbb{N}$. In particular, $\deg_{\mathbf{1}}(f)$ is the total degree of f.

Let $d \geq 0$. We denote by $\mathbb{T}(\boldsymbol{x})_d \subset \mathbb{T}(\boldsymbol{x})$ the set of terms of degree d and by $\mathbb{T}(\boldsymbol{x})_{\leq d} \subset \mathbb{T}(\boldsymbol{x})$ the set of terms of degree $\leq d$. Furthermore, we define the K-vector spaces $K[\boldsymbol{x}]_d := \langle \mathbb{T}(\boldsymbol{x})_d \rangle_K$ and $K[\boldsymbol{x}]_{\leq d} := \langle \mathbb{T}(\boldsymbol{x})_{\leq d} \rangle_K$. The polynomial ring is graded by $K[\boldsymbol{x}] = \bigoplus_{i\geq 0} K[\boldsymbol{x}]_i$. The elements of $K[\boldsymbol{x}]_d$

are called **homogeneous polynomials** or **forms** of degree d. In particular, elements of $K[\boldsymbol{x}]_1$ are called **linear forms**. Note that the zero polynomial is homogeneous of every degree. We have $\dim_K K[\boldsymbol{x}]_d = |\mathbb{T}(\boldsymbol{x})_d| = \binom{n+d-1}{d}$ and $\dim_K K[\boldsymbol{x}]_{\leq d} = |\mathbb{T}(\boldsymbol{x})_{\leq d}| = \binom{n+d}{d} \leq (n+1)^d$.

Let $K[\boldsymbol{z}] = K[z_1, \dots, z_r]$ be another polynomial ring over K, and let $\varphi\colon K[\boldsymbol{x}] \to K[\boldsymbol{z}]$ be a K-algebra homomorphism given by $x_i \mapsto f_i$ for $i \in [n]$, where $f_1, \dots, f_n \in K[\boldsymbol{z}]$. We define the **degree** of φ by

$$\deg(\varphi) := \max\bigl\{\deg(f_1), \dots, \deg(f_n), 0\bigr\} \in \mathbb{N}.$$

If $f_1, \dots, f_n$ are homogeneous, then φ is called **graded**. The image of a homogeneous polynomial of degree d under a graded homomorphism φ is homogeneous of degree $d \cdot \deg(\varphi)$. Finally, if $f_1, \dots, f_n$ are monomials, then φ is called **toric**. Toric homomorphisms are **sparsity-preserving**, i. e. they satisfy $\mathrm{sp}(\varphi(f)) \leq \mathrm{sp}(f)$ for all $f \in K[\boldsymbol{x}]$.

Resultants

Below we state a lemma about resultants that will be used in Section 4.2.5. Let $f, g \in K[w, \boldsymbol{x}]$ be polynomials such that $d := \deg_w(f) > 0$ and $e := \deg_w(g) > 0$. Write $f = \sum_{i=0}^{d} f_i \cdot w^i$ and $g = \sum_{j=0}^{e} g_j \cdot w^j$ with $f_i, g_j \in K[\boldsymbol{x}]$ for $i \in [d]$ and $j \in [e]$. Then the **Sylvester matrix** of f and g with respect to w is defined as

$$\mathrm{syl}_w(f,g) := \underbrace{\begin{pmatrix} f_0 & & & & g_0 & & & \\ f_1 & f_0 & & & g_1 & g_0 & & \\ & f_1 & \ddots & & & g_1 & \ddots & \\ \vdots & & \ddots & f_0 & \vdots & & \ddots & g_0 \\ & \vdots & & f_1 & & \vdots & & g_1 \\ f_d & & & & g_e & & & \\ & f_d & & \vdots & & g_e & & \vdots \\ & & \ddots & & & & \ddots & \\ & & & f_d & & & & g_e \end{pmatrix}}_{e \text{ columns} \quad\quad d \text{ columns}} \in K[\boldsymbol{x}]^{(d+e)\times(d+e)}.$$

The w**-resultant** of f and g is defined as $\mathrm{res}_w(f,g) := \det \mathrm{syl}_w(f,g) \in K[\boldsymbol{x}]$.

Lemma A.3.4 ([CLO97, Chapter 3, §6, Proposition 1])**.** *Let* $f, g \in K[w, \boldsymbol{x}]$ *be polynomials such that* $\deg_w(f) > 0$ *and* $\deg_w(g) > 0$*.*

(a) We have $\mathrm{res}_w(f,g) \in \langle f, g \rangle_{K[w,\boldsymbol{x}]}$*.*

(b) We have $\operatorname{res}_w(f,g) = 0$ *if and only if* f *and* g *have a common factor* $h \in K[w, \boldsymbol{x}]$ *with* $\deg_w(h) > 0$.

A.3.3 Field Theory

We review some concepts from field theory. For more about fields, we refer to [Lan02, Mor96]. Let L/K be a field extension, i. e. K is a subfield of L. For a subset $B \subseteq L$, we denote by $K(B)$ the field extension of K generated by B. The field L is a K-vector space and $[L : K] := \dim_K(L) \in \mathbb{N} \cup \{\infty\}$ is called the **degree** of L/K. If $[L : K] < \infty$, then L/K is called finite. A field extension is finite if and only if it is algebraic and finitely generated. For the **algebraic closure** of K we write $\overline{K}$.

A subset $B \subset L$ is called a **transcendence basis** of L/K if B is algebraically independent over K and $L/K(B)$ is algebraic. Transcendence bases exist for every field extension. All transcendence bases of L/K have the same cardinality, which is called the **transcendence degree** of L/K and is denoted by $\operatorname{trdeg}(L/K) \in \mathbb{N} \cup \{\infty\}$.

Finite fields

Let p be a prime, let $d \geq 1$, and let $q = p^d$. We denote by $\mathbb{F}_q$ the (up to isomorphism) unique finite field with q elements. There exists an irreducible polynomial $f \in \mathbb{F}_p[x]$ such that $\mathbb{F}_q \cong \mathbb{F}_p[x]/\langle f \rangle$. The following lemma characterizes irreducible polynomials over finite fields.

Lemma A.3.5 (Ben-Or irreducibility test, [Ben81, Lemma 1])**.** *Let* $d \geq 1$*, let* q *be a prime power and let* $f \in \mathbb{F}_q[x]$ *be a polynomial of degree* d*. Then* f *is irreducible in* $\mathbb{F}_q[x]$ *if and only if*

$$\gcd\bigl(f, x^{q^k} - x\bigr) = 1$$

for all $k \in \{1, \ldots, \lfloor d/2 \rfloor\}$.

Separability

Let K be a field. A univariate polynomial $f \in K[x]$ is called **separable** if it has no multiple roots in $\overline{K}$. Now assume that f is irreducible. Then f is separable if and only if its formal derivative $\partial_x f$ is non-zero. Consequently, if $\operatorname{char}(K) = 0$, then f is always separable, and if $\operatorname{char}(K) = p > 0$, then f is separable if and only if $f \notin K[x^p]$.

Let L/K be a field extension. If an element $a \in L$ is algebraic over K, then it is called **separable** over K if its minimal polynomial in $K[x]$

is separable. Those separable elements form a field $K \subseteq K_{\text{sep}} \subseteq L$ which is called the **separable closure** of K in L. Now assume that L/K is an algebraic extension. Then $[L : K]_{\text{sep}} := [K_{\text{sep}} : K] \in \mathbb{N}_{>0}$ and $[L : K]_{\text{insep}} := [L : K_{\text{sep}}] \in \mathbb{N}_{>0}$ are called the **separable** and **inseparable degree** of L/K, respectively. If $L = K_{\text{sep}}$, then L/K is called **separable**. The extension L/K_{sep} is **purely inseparable**, i. e., for all $a \in L$ we have $a^{p^e} \in K_{\text{sep}}$ for some $e \geq 0$.

A finitely generated field extension L/K is called **separable** if it has a transcendence basis $B \subset L$ such that the finite extension $L/K(B)$ is separable. In this case, B is called a **separating transcendence basis** of L/K. If L/K is separable, then every generating system of L over K contains a separating transcendence basis. If K is a perfect field, then every finitely generated field extension of K is separable.

A.4 Algebraic Geometry

We state some preliminaries from algebraic geometry required mainly in Section 2.7. For more detailed information on this topic, see [Eis95] and [Kem11].

Let L/K be a field extension and let $K[\boldsymbol{x}] = K[x_1, \ldots, x_n]$ be a polynomial ring over K. For a subset $S \subseteq K[\boldsymbol{x}]$, we define the **affine L-variety**

$$\mathcal{V}_{L^n}(S) := \big\{\boldsymbol{a} \in L^n \mid f(\boldsymbol{a}) = 0 \text{ for all } f \in S\big\}.$$

The affine L-varieties satisfy the axioms of closed sets in a topology. We call this topology the **Zariski topology on L^n with coefficients in K**. On a subset $X \subseteq L^n$, we define the Zariski topology as the induced subspace topology. The closure of a subset $X \subseteq L^n$ in the Zariski topology is called the **Zariski closure** of X and is denoted by $\overline{X}$. We have $\overline{X} = \mathcal{V}_{L^n}(\mathcal{I}_{K[\boldsymbol{x}]}(X))$, where

$$\mathcal{I}_{K[\boldsymbol{x}]}(X) := \big\{f \in K[\boldsymbol{x}] \mid f(\boldsymbol{a}) = 0 \text{ for all } \boldsymbol{a} \in X\big\}$$

is the **vanishing ideal** of X in $K[\boldsymbol{x}]$. In the setting $L = \overline{K}$, Hilbert's famous Nullstellensatz holds.

Theorem A.4.1 (Hilbert's Nullstellensatz, [Kem11, Theorem 1.17 and Exercise 1.9])**.** *Let $I \subseteq K[\boldsymbol{x}]$ be an ideal. Then we have*

$$\mathcal{I}_{K[\boldsymbol{x}]}\big(\mathcal{V}_{\overline{K}^n}(I)\big) = \sqrt{I},$$

where $\sqrt{I}$ denotes the radical ideal of I.

Affine varieties are Noetherian topological spaces. Recall that a topological space X is called **Noetherian** if there exists no infinite strictly descending chain of closed subsets in X. A topological space X is called **irreducible** if $X \neq \varnothing$ and X cannot be written as the union of two proper closed subsets. A Noetherian space X can be uniquely written (up to order) as $X = C_1 \cup \cdots \cup C_m$, where $m \geq 0$ and $C_1, \ldots, C_m \subseteq X$ are irreducible closed subsets with $C_i \nsubseteq C_j$ for $i \neq j$. The sets $C_1, \ldots, C_m$ are called the **irreducible components** of X.

The **Krull dimension** of a topological space X, denoted by $\dim(X)$, is defined as the supremum over all $m \geq 0$ for which there exists a chain $X_0 \subset \cdots \subset X_m$ of distinct irreducible closed subsets of X. If no irreducible closed subset exists, we set $\dim(X) = -1$.

Let $X \subseteq L^m$ and $Y \subseteq L^n$ be affine varieties, and let $f_1, \ldots, f_n \in K[x_1, \ldots, x_m]$ be polynomials. Then the map

$$\varphi\colon X \to Y, \quad \boldsymbol{a} \mapsto (f_1(\boldsymbol{a}), \ldots, f_n(\boldsymbol{a}))$$

is called a **morphism**. We say that φ is **dominant** if its image is dense in Y, i. e. $\overline{\varphi(X)} = Y$. We define the **degree** of φ by

$$\deg(\varphi) := \max\bigl\{\deg(f_1), \ldots, \deg(f_n), 0\bigr\} \in \mathbb{N}.$$

Note that this definition depends on the choice of $f_1, \ldots, f_n$.

From now on, we switch to the setting $K = L = \overline{K}$. The following lemma provides a bound on the dimension of fibers of morphisms.

Lemma A.4.2 ([Kem11, Corollary 10.6])**.** *Let $X \subseteq \overline{K}^m$ be an irreducible affine variety, let $Y \subseteq \overline{K}^n$ be an affine variety, and let $\varphi\colon X \to Y$ be a morphism. Then we have*

$$\dim(\varphi^{-1}(\boldsymbol{b})) \geq \dim(X) - \dim(Y)$$

for all $\boldsymbol{b} \in \varphi(X)$.

Let X be a topological space. A subset $Y \subseteq X$ is called locally closed if Y is the intersection of an open and a closed subset of X. A subset $C \subseteq X$ is called **constructible** if C is the union of finitely many locally closed subsets.

Lemma A.4.3 ([Kem11, Exercise 10.7])**.** *Let $X \subseteq \overline{K}^n$ be a constructible set. Then there exists a subset $U \subseteq X$ which is open and dense in $\overline{X}$.*

The following theorem shows that the image of a constructible set under a morphism is again constructible.

Theorem A.4.4 (Chevalley's Theorem, [Kem11, Corollary 10.8 and Exercise 10.9])**.** *Let $X \subseteq \overline{K}^m$ and $Y \subseteq \overline{K}^n$ be affine varieties, let $\varphi\colon X \to Y$ be a morphism, and let $C \subseteq X$ be a constructible set. Then $\varphi(C)$ is again constructible.*

The degree of a variety

Now we will define the degree of a variety according to [Hei83]. Recall that an **affine linear subspace** is a variety defined by polynomials of degree at most 1.

Definition A.4.5. Let $X \subseteq \overline{K}^n$ be an irreducible affine variety and let $r = \dim(X)$. Then the **degree** of X is defined as

$$\deg_{\overline{K}^n}(X) := \max\left\{ |X \cap E| \;\middle|\; \begin{array}{l} E \subseteq \overline{K}^n \text{ affine linear subspace s. t.} \\ \dim(E) = n - r \text{ and } |X \cap E| < \infty \end{array} \right\} \in \mathbb{N}_{>0}.$$

For a constructible set $X \subseteq \overline{K}^n$, we define

$$\deg_{\overline{K}^n}(X) := \sum_{i=1}^{m} \deg_{\overline{K}^n}(C_i) \in \mathbb{N},$$

where $C_1, \ldots, C_m \subseteq \overline{K}^n$ are the irreducible components of $\overline{X}$.

We have $\deg_{\overline{K}^n}(\overline{K}^n) = 1$. For non-constant polynomials $f \in K[\boldsymbol{x}]$, the affine variety $X := \mathcal{V}_{\overline{K}^n}(f)$ is called **affine hypersurface** and we have $\dim(X) = n - 1$ and $\deg_{\overline{K}^n}(X) \leq \deg(f)$. If $\deg(f) = 1$, X is called **affine hyperplane**.

Lemma A.4.6 ([Hei83, Remark 2.1])**.** *Let $X \subseteq \overline{K}^n$ be an irreducible affine variety and let $U \subseteq X$ be a non-empty open subset. Then there exists an affine linear subspace $E \subseteq \overline{K}^n$ with $\dim(E) = n - \dim(X)$ such that $\deg_{\overline{K}^n}(X) = |U \cap E|$.*

The following theorem is an affine version of the classical Bézout's Theorem (without multiplicities).

Theorem A.4.7 (Bézout's Inequality, [Hei83, Theorem 1])**.** *Let $X, Y \subseteq \overline{K}^n$ be constructible sets. Then we have*

$$\deg_{\overline{K}^n}(X \cap Y) \leq \deg_{\overline{K}^n}(X) \cdot \deg_{\overline{K}^n}(Y).$$

Corollary A.4.8 ([HS80a, Proposition 2.3])**.** *Let $X_1, \ldots, X_m \subseteq \overline{K}^n$ be affine varieties. Then we have*

$$\deg_{\overline{K}^n}\left(\bigcap_{i=1}^{m} X_i\right) \leq \deg_{\overline{K}^n}(X_1) \cdot \left(\max\{\deg_{\overline{K}^n}(X_i) \mid i \in [2, m]\}\right)^{\dim(X_1)}.$$

A.5 Differentials and the de Rham Complex

In this section we introduce Kähler differentials and the de Rham Complex. For more on differential modules, we refer to [Eis95, Mor96].

Definition A.5.1. Let R be a ring, let A be an R-algebra, and let M be an A-module.

(a) An R-linear map $D\colon A \to M$ is called an **R-derivation** of A into M, if it satisfies the **Leibniz rule**

$$D(ab) = a\,D(b) + D(a)\,b$$

for all $a, b \in A$. The set $\mathrm{Der}_R(A, M)$ of all such derivations forms an A-module in a natural way.

(b) The **module of Kähler differentials** of A over R, denoted by $\Omega^1_{A/R}$, is the A-module generated by the set of symbols $\{\mathrm{d}a \mid a \in A\}$ subject to the relations

$$\begin{aligned} \mathrm{d}(ra + sb) &= r\ \mathrm{d}a + s\ \mathrm{d}b, && (R\text{-linearity}) \\ \mathrm{d}(ab) &= a\ \mathrm{d}b + b\ \mathrm{d}a && (\text{Leibniz rule}) \end{aligned}$$

for all $r, s \in R$ and $a, b \in A$. The map $\mathrm{d}\colon A \to \Omega^1_{A/R}$ defined by $a \mapsto \mathrm{d}a$ is an R-derivation called the **universal R-derivation** of A.

For $m \geq 0$, let $\Omega^m_{A/R} := \bigwedge^m \Omega^1_{A/R}$ be the m-th exterior power over A. The universal derivation $\mathrm{d}\colon \Omega^0_{A/R} \to \Omega^1_{A/R}$ extends to the **exterior derivative** $\mathrm{d}^m\colon \Omega^m_{A/R} \to \Omega^{m+1}_{A/R}$ given by

$$\mathrm{d}^m(a\ \mathrm{d}a_1 \wedge \cdots \wedge \mathrm{d}a_m) = \mathrm{d}a \wedge \mathrm{d}a_1 \wedge \cdots \wedge \mathrm{d}a_m$$

for $a, a_1, \ldots, a_m \in A$. It satisfies $\mathrm{d}^{m+1} \circ \mathrm{d}^m = 0$, so we obtain a complex of R-modules

$$\Omega^\bullet_{A/R}\colon \quad 0 \to A \xrightarrow{d} \Omega^1_{A/R} \xrightarrow{d^1} \cdots \to \Omega^m_{A/R} \xrightarrow{d^m} \Omega^{m+1}_{A/R} \to \cdots$$

called the **de Rham complex** of A over R. The direct sum $\Omega_{A/R} := \bigoplus_{m\geq 0} \Omega^m_{A/R}$ is a differential graded R-algebra. Recall that a **differential graded R-algebra** is a graded R-algebra $M = \bigoplus_{i\geq 0} M^i$ which is graded skew-commutative, i. e. we have $\omega\eta = (-1)^{ij}\eta\omega$ for $\omega \in M^i$ and $\eta \in M^j$, together with an R-derivation $\mathrm{d}\colon M^i \to M^{i+1}$ satisfying $\mathrm{d} \circ \mathrm{d} = 0$ and the graded Leibnitz rule $\mathrm{d}(\omega\eta) = \eta\ \mathrm{d}\omega + (-1)^i\omega\ \mathrm{d}\eta$ for $\omega \in M^i$ and $\eta \in M$.

The de Rham complex of $K[\boldsymbol{x}]$

Let K be a field and let $K[\boldsymbol{x}] = K[x_1, \dots, x_n]$ be a polynomial ring over K. Then $\Omega^1_{K[\boldsymbol{x}]/K}$ is a free $K[\boldsymbol{x}]$-module of rank n with basis $\{\mathrm{d}x_1, \dots, \mathrm{d}x_n\}$. The universal derivation $\mathrm{d}\colon K[\boldsymbol{x}] \to \Omega^1_{K[\boldsymbol{x}]/K}$ is given by $f \mapsto \sum_{i=1}^n (\partial_{x_i} f)\,\mathrm{d}x_i$, where $\partial_{x_i} f \in K[\boldsymbol{x}]$ denotes the i-th **formal partial derivative** of f for $i \in [n]$.

Let $f_1, \dots, f_m \in K[\boldsymbol{x}]$ be polynomials and let $\boldsymbol{u} \subseteq \boldsymbol{x}$ be a subset of the variables. Write $\boldsymbol{u} = \{x_{j_1}, \dots, x_{j_r}\}$ with $1 \le j_1 < \cdots < j_r \le n$. The **Jacobian matrix of $f_1, \dots, f_m$ with respect to $\boldsymbol{u}$** is defined as

$$J_{\boldsymbol{u}}(f_1, \dots, f_m) := \begin{pmatrix} \partial_{x_{j_1}} f_1 & \cdots & \partial_{x_{j_r}} f_1 \\ \vdots & & \vdots \\ \partial_{x_{j_1}} f_m & \cdots & \partial_{x_{j_r}} f_m \end{pmatrix} \in K[\boldsymbol{x}]^{m \times r}. \tag{A.5.1}$$

Now let $m \le n$ and let $I = \{j_1 < \ldots < j_m\} \in \binom{[n]}{m}$ be an index set. We use the notations $\boldsymbol{x}_I = \{x_{j_1}, \dots, x_{j_m}\}$ and $\bigwedge_{j\in I} \mathrm{d}x_j := \mathrm{d}x_{j_1} \wedge \cdots \wedge \mathrm{d}x_{j_m}$. The $K[\boldsymbol{x}]$-module $\Omega^m_{K[\boldsymbol{x}]/K}$ is free of rank $\binom{n}{m}$ with basis $\big\{\bigwedge_{j\in I} \mathrm{d}x_j \mid I \in \binom{[n]}{m}\big\}$. An element $\mathrm{d}f_1 \wedge \cdots \wedge \mathrm{d}f_m \in \Omega^m_{K[\boldsymbol{x}]/K}$ can be represented in this basis as

$$\mathrm{d}f_1 \wedge \cdots \wedge \mathrm{d}f_m = \sum_I \det J_{\boldsymbol{x}_I}(f_1, \dots, f_m) \cdot \textstyle\bigwedge_{j\in I} \mathrm{d}x_j, \tag{A.5.2}$$

where the sum is over all $I \in \binom{[n]}{m}$. If $m > n$, then we have $\Omega^m_{K[\boldsymbol{x}]/K} = \{0\}$.

Lemma A.5.2. *Let $f_1, \dots, f_m \in K[\boldsymbol{x}]$ be polynomials. Then*

$$\mathrm{d}f_1 \wedge \cdots \wedge \mathrm{d}f_m \neq 0 \quad \textit{in } \Omega^m_{K[\boldsymbol{x}]/K}$$

if and only if $\operatorname{rk}_{K(\boldsymbol{x})} J_{\boldsymbol{x}}(f_1, \dots, f_m) = m$.

Proof. By (A.5.2), the differential $\mathrm{d}f_1 \wedge \cdots \wedge \mathrm{d}f_m$ is non-zero if and only if the Jacobian matrix $J_{\boldsymbol{x}}(f_1, \dots, f_m)$ has a non-zero $m \times m$-minor. □

Let $K[\boldsymbol{z}] = K[z_1, \dots, z_r]$ be another polynomial ring over K. Let $f \in K[\boldsymbol{x}]$ and and let $g_1, \dots, g_n \in K[\boldsymbol{z}]$. By the **chain rule**, we have

$$\partial_{z_i}\big(f(g_1, \dots, g_n)\big) = \sum_{j=1}^n (\partial_{x_j} f)(g_1, \dots, g_n) \cdot \partial_{z_i}(f_j)$$

for all $i \in [r]$. Now let $\varphi\colon K[\boldsymbol{x}] \to K[\boldsymbol{z}]$ be the K-algebra homomorphism given by $x_i \mapsto g_i$ for $i \in [n]$ and let $f_1, \dots, f_m \in K[\boldsymbol{x}]$. Then the chain rule implies the matrix equation

$$J_{\boldsymbol{z}}(\varphi(f_1), \dots, \varphi(f_m)) = \varphi\big(J_{\boldsymbol{x}}(f_1, \dots, f_m)\big) \cdot J_{\boldsymbol{z}}(g_1, \dots, g_n).$$

Transfer lemmas

Lemma A.5.3 (Base change)**.** *Let R be a ring, let A and R' be R-algebras. Then $A' := R' \otimes_R A$ is an R'-algebra and, for all $m \geq 0$, there is an A'-module isomorphism*

$$R' \otimes_A \Omega^m_{A/R} \to \Omega^m_{A'/R'}$$

given by $b \otimes (\mathrm{d}a_1 \wedge \cdots \wedge \mathrm{d}a_m) \mapsto b\ \mathrm{d}(1 \otimes a_1) \wedge \cdots \wedge \mathrm{d}(1 \otimes a_m)$ for $a_1, \ldots, a_m \in A$ and $b \in R'$.

Proof. The case $m = 0$ is evident, the case $m = 1$ is [Eis95, Proposition 16.4] and for $m \geq 2$ the statement follows from [Eis95, Proposition A2.2 b]. □

Lemma A.5.4 (Localization)**.** *Let R be a ring, let A be an R-algebra and let $B = S^{-1}A$ for some multiplicatively closed set $S \subseteq A$. Then, for all $m \geq 0$, there is a B-module isomorphism*

$$B \otimes_A \Omega^m_{A/R} \to \Omega^m_{B/R}$$

given by $b \otimes (\mathrm{d}a_1 \wedge \cdots \wedge \mathrm{d}a_m) \mapsto b\ \mathrm{d}a_1 \wedge \cdots \wedge \mathrm{d}a_m$ for $a_1, \ldots, a_m \in A$ and $b \in B$. The universal R-derivation $\mathrm{d}\colon B \to \Omega^1_{B/R}$ satisfies $\mathrm{d}(s^{-1}) = -s^{-2}\ \mathrm{d}s$ for $s \in S$.

Proof. The case $m = 0$ is evident, the case $m = 1$ and the second statement is [Eis95, Proposition 16.9] and for $m \geq 2$ the statement follows from [Eis95, Proposition A2.2 b]. □

Lemma A.5.5 (Separable extension)**.** *Let L/K be an algebraic and separable field extension and let R be a subring of K. Then, for all $m \geq 0$, there is an L-vector space isomorphism*

$$L \otimes_K \Omega^m_{K/R} \to \Omega^m_{L/R}$$

given by $b \otimes (\mathrm{d}a_1 \wedge \cdots \wedge \mathrm{d}a_m) \mapsto b\ \mathrm{d}a_1 \wedge \cdots \wedge \mathrm{d}a_m$ for $a_1, \ldots, a_m \in K$ and $b \in L$.

Proof. The case $m = 0$ is evident, the case $m = 1$ is [Eis95, Lemma 16.15] and for $m \geq 2$ the statement follows from [Eis95, Proposition A2.2 b]. □

Separability

The separability of a finitely generated field extension is characterized by the vector space dimension of its Kähler differentials.

Lemma A.5.6 ([Eis95, Corollary 16.17 a])**.** *Let L/K be a finitely generated field extension. Then*

$$\dim_L \Omega^1_{L/K} \geq \operatorname{trdeg}(L/K),$$

with equality if and only if L/K is separable.

A.6 The Ring of Witt Vectors and the de Rham-Witt Complex

In this section we introduce Witt rings [Wit37] and the de Rham-Witt complex constructed by Illusie [Ill79].

A.6.1 The Ring of Witt Vectors

Let p be a fixed prime. For $n \geq 0$, the **n-th Witt polynomial** is defined as

$$w_n := \sum_{i=0}^{n} p^i \, x_i^{p^{n-i}} \in \mathbb{Z}[x_0, \dots, x_n].$$

For all $n \geq 0$, there exist unique polynomials $S_n, P_n \in \mathbb{Z}[x_0, \dots, x_n, y_0, \dots y_n]$ such that

$$\begin{aligned} w_n(S_0, \dots, S_n) &= w_n(x_0, \dots, x_n) + w_n(y_0, \dots, y_n) \quad \text{and} \\ w_n(P_0, \dots, P_n) &= w_n(x_0, \dots, x_n) \cdot w_n(y_0, \dots, y_n) \end{aligned}$$

(see [Haz09, Theorem 5.2]). The polynomials S_n, P_n can be determined recursively by the formulas

$$\begin{aligned} S_n &= p^{-n} \left(w_n(x_0, \dots, x_n) + w_n(y_0, \dots, y_n) - \sum_{i=0}^{n-1} p^i \, S_i^{p^{n-i}} \right) \quad \text{and} \\ P_n &= p^{-n} \left(w_n(x_0, \dots, x_n) \cdot w_n(y_0, \dots, y_n) - \sum_{i=0}^{n-1} p^i \, P_i^{p^{n-i}} \right), \end{aligned}$$

in particular, we have

$$\begin{aligned} S_0 &= x_0 + y_0, & S_1 &= x_1 + y_1 - \sum_{i=1}^{p-1} p^{-1} \binom{p}{i} x_0^i y_0^{p-i}, \\ P_0 &= x_0 y_0, & P_1 &= x_0^p y_1 + x_1 y_0^p + p \, x_1 y_1. \end{aligned}$$

Definition A.6.1. Let p be a fixed prime and let A be a ring. The ring of **(p-typical) Witt vectors** of A, denoted by $\mathrm{W}(A)$, is the set $A^{\mathbb{N}}$ with addition and multiplication defined by

$$\begin{aligned} a + b &:= (S_0(a_0, b_0), S_1(a_0, a_1, b_0, b_1), \dots) \quad \text{and} \\ a \cdot b &:= (P_0(a_0, b_0), P_1(a_0, a_1, b_0, b_1), \dots), \end{aligned}$$

for all $a = (a_0, a_1, \dots), b = (b_0, b_1, \dots) \in \mathrm{W}(A)$. The additive and multiplicative identity elements of $\mathrm{W}(A)$ are $(0, 0, 0, \dots)$ and $(1, 0, 0, \dots)$, respectively.

By [Haz09, Theorem 5.14], $\mathrm{W}(A)$ is indeed a ring and we have a ring homomorphism

$$w\colon \mathrm{W}(A) \to A^{\mathbb{N}}, \quad a \mapsto (w_0(a), w_1(a), \dots),$$

where $A^{\mathbb{N}}$ is the usual product ring.

Let $\ell \geq 1$. The projection $\mathrm{W}_\ell(A)$ of $\mathrm{W}(A)$ to the first ℓ coordinates is again a ring which is called the ring of **truncated Witt vectors** of A of **length** ℓ. We have $\mathrm{W}_1(A) = A$.

The **Teichmüller lift** of a ring element $a \in A$ is defined as $[a] := (a, 0, 0, \dots) \in \mathrm{W}(A)$. The image of $[a]$ in $\mathrm{W}_\ell(A)$ is denoted by $[a]_{\leq \ell}$. The map $A \to \mathrm{W}(A)$, $a \mapsto [a]$ is multiplicative, i. e. we have $[ab] = [a][b]$ for all $a, b \in A$.

Restriction, Verschiebung, and Frobenius maps

For $\ell \geq 1$, we have ring epimorphisms

$$\mathrm{R}\colon \mathrm{W}_{\ell+1}(A) \to \mathrm{W}_\ell(A), \quad (a_0, \dots, a_\ell) \mapsto (a_0, \dots, a_{\ell-1}),$$

called **restriction maps**. We obtain a projective system of rings $\mathrm{W}_\bullet(A) = ((\mathrm{W}_\ell(A))_{\ell \geq 1}, \mathrm{R}\colon \mathrm{W}_{\ell+1}(A) \to \mathrm{W}_\ell(A))$ with limit $\mathrm{W}(A)$.

The additive group homomorphism

$$\mathrm{V}\colon \mathrm{W}(A) \to \mathrm{W}(A), \quad (a_0, a_1, \dots) \mapsto (0, a_0, a_1, \cdots)$$

is called **Verschiebung** (shift). It induces additive maps $\mathrm{V}\colon \mathrm{W}_\ell(A) \to \mathrm{W}_{\ell+1}(A)$, and we have exact sequences

$$0 \to \mathrm{W}(A) \xrightarrow{\mathrm{V}^\ell} \mathrm{W}(A) \to \mathrm{W}_\ell(A) \to 0,$$
$$0 \to \mathrm{W}_r(A) \xrightarrow{\mathrm{V}^\ell} \mathrm{W}_{\ell+r}(A) \xrightarrow{\mathrm{R}^r} \mathrm{W}_\ell(A) \to 0$$

for all $\ell, r \geq 1$.

Now let A be an $\mathbb{F}_p$-algebra. Then the Frobenius endomorphism $\mathrm{F}\colon A \to A$, $a \mapsto a^p$ induces a ring endomorphism

$$\mathrm{F}\colon \mathrm{W}(A) \to \mathrm{W}(A), \quad (a_0, a_1, \dots) \mapsto (a_0^p, a_1^p, \dots) \tag{A.6.1}$$

which we call **Frobenius endomorphism**, too. We have $\mathrm{V}\,\mathrm{F} = \mathrm{F}\,\mathrm{V} = p$ and $a\ \mathrm{V}\,b = \mathrm{V}(\mathrm{F}\,a \cdot b)$ for all $a, b \in W(A)$, in particular, $\mathrm{V}[1] = p$. For $\ell \geq 1$, the Frobenius also induces endomorphisms $\mathrm{F}\colon \mathrm{W}_\ell(A) \to \mathrm{W}_\ell(A)$. If A is perfect, i. e. F is an automorphism of A, then the induced endomorphisms are automorphisms as well.

Witt vectors of finite fields

The Witt vectors of finite fields form (the unramified extensions of) the p-adic integers [Kob84, Rob00]. First we consider the prime field $\mathbb{F}_p$. Then $\mathrm{W}(\mathbb{F}_p)$ is the ring of **p-adic integers**, denoted by $\mathbb{Z}_p$. Its quotient field $\mathbb{Q}_p = \mathrm{Quot}(\mathbb{Z}_p)$ is called the field of **p-adic numbers**.

Now let $q = p^t$ for some $t \geq 1$. There exists a unique unramified extension of $\mathbb{Q}_p$ (in its algebraic closure $\overline{\mathbb{Q}}_p$) of degree t, which we denote by $\mathbb{Q}_q$. The integral closure of $\mathbb{Z}_p$ in $\mathbb{Q}_q$ is denoted by $\mathbb{Z}_q$. We have $\mathbb{Z}_q = \mathrm{W}(\mathbb{F}_q)$.

The truncated Witt rings of $\mathbb{F}_q$ are Galois rings [Wan03]. A finite ring R is called **Galois ring** if the set of its zerodivisors together with zero is the ideal $\langle p \rangle_R$. Then R is a local ring of characteristic p^ℓ for some $\ell \geq 1$ with residue field $\mathbb{F}_{p^t} = R/\langle p \rangle$ for some $t \geq 1$, and we have $|R| = p^{\ell t}$. A Galois ring of characteristic p^ℓ with $p^{\ell t}$ elements exists for all $\ell, t \geq 1$, is unique up to isomorphism, and will be denoted by $G_{\ell,t}$. For the construction of $G_{\ell,t}$, see Lemma 4.3.7. By [Rag69, (3.5)]), we have $\mathrm{W}_\ell(\mathbb{F}_{p^t}) = G_{\ell,t}$, in particular $\mathrm{W}_\ell(\mathbb{F}_p) = \mathbb{Z}/\langle p^\ell \rangle$.

Some lemmas

Lemma A.6.2. *Let A be an $\mathbb{F}_p$-algebra and let $a, b \in \mathrm{W}(A)$ such that $a - b \in \mathrm{V}\,\mathrm{W}(A)$. Then*

$$a^{p^\ell} - b^{p^\ell} \in \mathrm{V}^{\ell+1}\,\mathrm{W}(A)$$

for all $\ell \geq 0$.

Proof. We use induction on ℓ. The case $\ell = 0$ holds by assumption, so let $\ell \geq 1$. By induction, there exists $c \in \mathrm{V}^\ell\,\mathrm{W}(A)$ such that $a^{p^{\ell-1}} = b^{p^{\ell-1}} + c$. Using $\mathrm{V}\,\mathrm{F} = p$ and $p^{-1}\binom{p}{i} \in \mathbb{N}$ for $i \in [p-1]$, we conclude

$$\begin{aligned} a^{p^\ell} - b^{p^\ell} &= \big(b^{p^{\ell-1}} + c\big)^p - b^{p^\ell} \\ &= c^p + \sum_{i=1}^{p-1} \binom{p}{i} \mathrm{V}\,\mathrm{F}\big(b^{p^{\ell-1}(p-i)} c^i\big) \in \mathrm{V}^{\ell+1}\,\mathrm{W}(A), \end{aligned}$$

finishing the proof. □

Definition A.6.3. The **p-adic valuation** $v_p \colon \mathbb{Q} \to \mathbb{Z} \cup \{\infty\}$ of $\mathbb{Q}$ is defined as follows. If $a \in \mathbb{Q}$ is non-zero, then $v_p(a)$ is the unique integer $v \in \mathbb{Z}$ such that $a = p^v \frac{r}{s}$, where $r, s \in \mathbb{Z} \setminus p\mathbb{Z}$. For $a = 0$, we set $v_p(a) := \infty$. For vectors $\alpha \in \mathbb{Q}^s$, we extend this notion by setting $v_p(\alpha) := \min\{v_p(\alpha_1), \ldots, v_p(\alpha_s)\} \in \mathbb{Z} \cup \{\infty\}$.

Lemma A.6.4. *Let $\alpha, \beta \in \mathbb{Q}^s$. Then $v_p(\alpha+\beta) \geq \min\{v_p(\alpha), v_p(\beta)\}$, with equality if $v_p(\alpha) \neq v_p(\beta)$.*

Proof. Let $i \in [s]$ such that $v_p(\alpha+\beta) = v_p(\alpha_i+\beta_i)$. Then $v_p(\alpha+\beta) = v_p(\alpha_i+\beta_i) \geq \min\{v_p(\alpha_i), v_p(\beta_i)\} \geq \min\{v_p(\alpha), v_p(\beta)\}$.

Now assume $v_p(\alpha) \neq v_p(\beta)$, say $v_p(\alpha) < v_p(\beta)$. Let $i \in [s]$ such that $v_p(\alpha) = v_p(\alpha_i)$. Then $v_p(\alpha_i) < v_p(\beta_i)$, therefore $v_p(\alpha+\beta) \leq v_p(\alpha_i+\beta_i) = \min\{v_p(\alpha_i), v_p(\beta_i)\} = v_p(\alpha_i) = v_p(\alpha) = \min\{v_p(\alpha), v_p(\beta)\}$. □

Lemma A.6.5 ([Sin80, Theorem 32])**.** *Let $\ell \geq 0$ and let $\boldsymbol{i} \in \mathbb{N}^s$ such that $|\boldsymbol{i}| = p^\ell$. Then $p^{\ell - v_p(\boldsymbol{i})}$ divides $\binom{p^\ell}{\boldsymbol{i}}$.*

Lemma A.6.6. *Let $A = R[\boldsymbol{a}] = R[a_1, \ldots, a_m]$ be a finitely generated R-algebra, where R is an $\mathbb{F}_p$-algebra and $a_1, \ldots, a_m \in A$. Let $\ell \geq 0$ and let $f = \sum_{i=1}^s c_i \boldsymbol{a}^{\alpha_i}$ be an element of A, where $c_i \in R$ and $\alpha_i \in \mathbb{N}^m$ for $i \in [s]$. Then, in $\mathrm{W}_{\ell+1}(A)$, we have*

$$[f] = \sum_{|\boldsymbol{i}|=p^\ell} p^{-\ell+v_p(\boldsymbol{i})} \binom{p^\ell}{\boldsymbol{i}} \mathrm{V}^{\ell-v_p(\boldsymbol{i})} \mathrm{F}^{-v_p(\boldsymbol{i})}\big([c_1\boldsymbol{a}^{\alpha_1}]^{i_1} \cdots [c_s\boldsymbol{a}^{\alpha_s}]^{i_s}\big), \qquad \text{(A.6.2)}$$

where the sum is over all $\boldsymbol{i} = (i_1, \ldots, i_s) \in \mathbb{N}^s$.

Remark A.6.7. Note that the RHS of (A.6.2) is a well-defined element of $\mathrm{W}(A)$, because $p^{-\ell+v_p(\boldsymbol{i})} \cdot \binom{p^\ell}{\boldsymbol{i}} \in \mathbb{N}$ by Lemma A.6.5, $v_p(\boldsymbol{i}) \leq \ell$, and $p^{-v_p(\boldsymbol{i})} \cdot \boldsymbol{i} \in \mathbb{N}^s$ for all $\boldsymbol{i} \in \mathbb{N}^s$ with $|\boldsymbol{i}| = p^\ell$.

Proof of Lemma A.6.6. We have $[f] = \sum_{i=1}^s [c_i\boldsymbol{a}^{\alpha_i}]$ in $\mathrm{W}_1(A)$, so Lemma A.6.2 implies

$$\mathrm{F}^\ell[f] = [f]^{p^\ell} = \left(\sum_{i=1}^s [c_i\boldsymbol{a}^{\alpha_i}]\right)^{p^\ell} = \sum_{|\boldsymbol{i}|=p^\ell} \binom{p^\ell}{\boldsymbol{i}} [c_1\boldsymbol{a}^{\alpha_1}]^{i_1} \cdots [c_s\boldsymbol{a}^{\alpha_s}]^{i_s}$$

in $\mathrm{W}_{\ell+1}(A)$. Since $\mathrm{V}\,\mathrm{F} = \mathrm{F}\,\mathrm{V} = p$, we see that this is equal to $\mathrm{F}^\ell\, w$, where w denotes the RHS of (A.6.2). The injectivity of F implies $[f] = w$ in $\mathrm{W}_{\ell+1}(A)$. □

A.6.2 The de Rham-Witt Complex

Let p be a fixed prime.

Definition A.6.8. A **de Rham V-pro-complex** is a projective system $M_\bullet = ((M)_{\ell\geq 1}, \mathrm{R}\colon M_{\ell+1} \to M_\ell)$ of differential graded $\mathbb{Z}$-algebras together with additive homomorpisms $(\mathrm{V}\colon M_\ell^m \to M_{\ell+1}^m)_{m\geq 0, \ell\geq 1}$ such that $\mathrm{R}\,\mathrm{V} = \mathrm{V}\,\mathrm{R}$ and the following properties are satisfied:

(a) M_1^0 is an $\mathbb{F}_p$-algebra and $M_\ell^0 = \mathrm{W}_\ell(M_1^0)$, where $\mathrm{R}\colon M_{\ell+1}^0 \to M_\ell^0$ and $\mathrm{V}\colon M_\ell^0 \to M_{\ell+1}^0$ are the restriction and Verschiebung maps of Witt rings,

(b) $\mathrm{V}(\omega\,\mathrm{d}\eta) = (\mathrm{V}\,\omega)\,\mathrm{dV}\,\eta$ for all $\omega \in M_\ell^m$ and $\eta \in M_\ell^n$, and

(c) $(\mathrm{V}\,w)\,\mathrm{d}[a] = \mathrm{V}([a]^{p-1}w)\,\mathrm{dV}[a]$ for all $a \in M_1^0$ and $w \in M_\ell^0$.

Theorem A.6.9 ([Ill79, Théorème I.1.3])**.** *Let A be an $\mathbb{F}_p$-algebra. Then there exists a functorial de Rham V-pro-complex $\mathrm{W}_\bullet\,\Omega_A^\bullet$ with $\mathrm{W}_\ell\,\Omega_A^0 = \mathrm{W}_\ell(A)$ for all $\ell \geq 1$. We have an epimomorphism of differential graded $\mathbb{Z}$-algebras $\pi_\ell\colon \Omega^\bullet_{\mathrm{W}_\ell(A)/\,\mathrm{W}_\ell(\mathbb{F}_p)} \twoheadrightarrow \mathrm{W}_\ell\,\Omega_A^\bullet$ for all $\ell \geq 1$ such that π_ℓ^0 is the identity and π_1 is an isomorphism.*

Definition A.6.10. Let A be an $\mathbb{F}_p$-algebra. The de Rham V-pro-complex $\mathrm{W}_\bullet\,\Omega_A^\bullet$ from Theorem A.6.9 is called the **de Rham-Witt pro-complex of** A.

The Frobenius map

Theorem A.6.11 ([Ill79, Théorème I.2.17])**.** *Let A be an $\mathbb{F}_p$-algebra. The morphism of projective systems of rings $\mathrm{R}\,\mathrm{F} = \mathrm{F}\,\mathrm{R}\colon \mathrm{W}_\bullet(A) \to \mathrm{W}_{\bullet-1}(A)$ extends uniquely to a morphism of projective systems of graded algebras $\mathrm{F}\colon \mathrm{W}_\bullet\,\Omega_A^\bullet \to \mathrm{W}_{\bullet-1}\,\Omega_A^\bullet$ such that*

(a) $\mathrm{F}\,\mathrm{d}[a]_{\leq \ell+1} = [a]_{\leq \ell}^{p-1}\,\mathrm{d}[a]_{\leq \ell}$ *for all $a \in A$ and $\ell \geq 1$, and*

(b) $\mathrm{F}\,\mathrm{dV} = \mathrm{d}$ *in $\mathrm{W}_\ell\,\Omega_A^1$ for all $\ell \geq 1$.*

Let A be an $\mathbb{F}_p$-algebra. Define the **canonical filtration**

$$\mathrm{Fil}^\ell\,\mathrm{W}_{\ell+i}\,\Omega_A^\bullet := \ker\bigl(\mathrm{R}^i\colon\ \mathrm{W}_{\ell+i}\,\Omega_A^\bullet \to \mathrm{W}_\ell\,\Omega_A^\bullet\bigr)$$

for all $\ell \geq 1$ and $i \geq 0$.

Lemma A.6.12. *Let K be a perfect field. Then we have*

$$\ker\bigl(\mathrm{F}^i\colon\ \mathrm{W}_{\ell+i}\,\Omega^m_{K(\boldsymbol{x})} \to \mathrm{W}_\ell\,\Omega^m_{K(\boldsymbol{x})}\bigr) \subseteq \mathrm{Fil}^\ell\,\mathrm{W}_{\ell+i}\,\Omega^m_{K(\boldsymbol{x})}$$

for all $i, m \geq 0$ and $\ell \geq 1$.

Proof. Let $i, m \geq 0$, let $\ell \geq 1$, and let $\omega \in \mathrm{W}_{\ell+i}\,\Omega^m_{K(\boldsymbol{x})}$ such that $\mathrm{F}^i\,\omega = 0$. Applying $\mathrm{V}^i\colon\ \mathrm{W}_\ell\,\Omega^m_{K(\boldsymbol{x})} \to \mathrm{W}_{\ell+i}\,\Omega^m_{K(\boldsymbol{x})}$ and using $\mathrm{V}^i\,\mathrm{F}^i = p^i$, we obtain $p^i\omega = 0$. By [Ill79, Proposition I.3.4], we conclude $\omega \in \mathrm{Fil}^\ell\,\mathrm{W}_{\ell+i}\,\Omega^m_{K(\boldsymbol{x})}$. □

Transfer lemmas

Lemma A.6.13 (Base change, [Ill79, Proposition I.1.9.2]). *Let K'/K be an extension of perfect fields of characteristic p. Let A be a K-algebra and set $A' := K' \otimes_K A$. Then there is a natural $\mathrm{W}_\ell(K')$-module isomorphism*

$$\mathrm{W}_\ell(K') \otimes_{\mathrm{W}_\ell(K)} \mathrm{W}_\ell \Omega^m_A \to \mathrm{W}_\ell \Omega^m_{A'}$$

for all $\ell \geq 1$ and $m \geq 0$.

Lemma A.6.14 (Localization, [Ill79, Proposition I.1.11]). *Let A be an $\mathbb{F}_p$-algebra and let $B = S^{-1}A$ for some multiplicatively closed set $S \subseteq A$. Then there is a natural $\mathrm{W}_\ell(B)$-module isomorphism*

$$\mathrm{W}_\ell(B) \otimes_{\mathrm{W}_\ell(A)} \mathrm{W}_\ell \Omega^m_A \to \mathrm{W}_\ell \Omega^m_B$$

for all $\ell \geq 1$ and $m \geq 0$.

Lemma A.6.15 (Finite separable extension). *Let L/K be a finite separable field extension of characteristic p. Then there is a natural $\mathrm{W}_\ell(L)$-module isomorphism*

$$\mathrm{W}_\ell(L) \otimes_{\mathrm{W}_\ell(K)} \mathrm{W}_\ell \Omega^m_K \to \mathrm{W}_\ell \Omega^m_L$$

for all $\ell \geq 1$ and $m \geq 0$.

Proof. Since L/K is finite and separable, the induced morphism $K \to L$ is étale. Now the assertion follows from [Ill79, Proposition I.1.14]. □

A.6.3 The de Rham-Witt Complex of $K[\boldsymbol{x}]$

Let p be a fixed prime, let $K/\mathbb{F}_p$ be an algebraic extension, and let $K[\boldsymbol{x}] = K[x_1, \ldots, x_n]$ be a polynomial ring over K. In [Ill79, §I.2], an explicit description of $\mathrm{W}_\bullet \Omega^\bullet_{K[\boldsymbol{x}]}$ is given for the case $K = \mathbb{F}_p$. By virtue of Lemma A.6.13, this construction can be generalized to our setting (note that K is perfect).

Let $R := \mathrm{W}(K)$ be the Witt ring of K and let $Q := \mathrm{Quot}(R)$ be its quotient field. Furthermore, define the ring $Q[\boldsymbol{x}^{p^{-\infty}}] := \bigcup_{i \geq 0} Q[\boldsymbol{x}^{p^{-i}}]$. For $m \geq 0$, we use the abbreviations

$$\Omega^m_{R[\boldsymbol{x}]} := \Omega^m_{R[\boldsymbol{x}]/R} \qquad \text{and} \qquad \Omega^m_{Q[\boldsymbol{x}^{p^{-\infty}}]} := \Omega^m_{Q[\boldsymbol{x}^{p^{-\infty}}]/Q}\,.$$

Since the universal derivation $\mathrm{d}\colon Q[\boldsymbol{x}^{p^{-\infty}}] \to \Omega^1_{Q[\boldsymbol{x}^{p^{-\infty}}]}$ satisfies

$$\mathrm{d}\big(x_j^{p^{-i}}\big) = p^{-i} x_j^{p^{-i}}\, \mathrm{d}x_j / x_j$$

for all $i \geq 0$ and $j \in [n]$, every differential form $\omega \in \Omega^m_{Q[\boldsymbol{x}^{p^{-\infty}}]}$ can be written uniquely as

$$\omega = \sum_I c_I \cdot \bigwedge_{j \in I} \mathrm{d} \log x_j, \tag{A.6.3}$$

where the sum is over all $I \in \binom{[n]}{m}$, the $c_I \in Q[\boldsymbol{x}^{p^{-\infty}}]$ are divisible by $(\prod_{j \in I} x_j)^{p^{-i}}$ for some $i \geq 0$, and $\mathrm{d} \log x_j := \mathrm{d}x_j / x_j$. The c_I are called **coordinates** of ω. The form ω is called **integral** if all its coordinates have coefficients in R. For $m \geq 0$, we define

$$\mathrm{E}^m := \mathrm{E}^m_{K[\boldsymbol{x}]} := \big\{ \omega \in \Omega^m_{Q[\boldsymbol{x}^{p^{-\infty}}]} \mid \text{both } \omega \text{ and } \mathrm{d}\omega \text{ are integral} \big\}.$$

Then $\mathrm{E} := \bigoplus_{m \geq 0} \mathrm{E}^m$ is a differential graded subalgebra of $\Omega^m_{Q[\boldsymbol{x}^{p^{-\infty}}]}$ containing $\Omega^m_{R[\boldsymbol{x}]}$.

Let $\mathrm{F} \colon Q[\boldsymbol{x}^{p^{-\infty}}] \to Q[\boldsymbol{x}^{p^{-\infty}}]$ be the unique $\mathbb{Q}_p$-algebra automorphism extending the Frobenius automorphism of R and sending

$$\mathrm{F}\big(x_j^{p^{-i}}\big) = x_j^{p^{-i+1}}$$

for all $i \geq 0$ and $j \in [n]$. The map F extends to an automorphism

$$\mathrm{F} \colon \Omega^m_{Q[\boldsymbol{x}^{p^{-\infty}}]} \to \Omega^m_{Q[\boldsymbol{x}^{p^{-\infty}}]}$$

of differential graded algebras by acting on the coordinates of the differential forms. We also define

$$\mathrm{V} := p\,\mathrm{F}^{-1} \colon \Omega^m_{Q[\boldsymbol{x}^{p^{-\infty}}]} \to \Omega^m_{Q[\boldsymbol{x}^{p^{-\infty}}]}.$$

Then we have $\mathrm{d}\,\mathrm{F} = p\,\mathrm{F}\,\mathrm{d}$ and $\mathrm{V}\,\mathrm{d} = p\,\mathrm{d}\,\mathrm{V}$, in particular, E is closed under F and V. Setting

$$\mathrm{Fil}^\ell \mathrm{E}^m := \mathrm{V}^\ell \mathrm{E}^m + \mathrm{d}\,\mathrm{V}^\ell \mathrm{E}^{m-1}$$

for all $\ell, m \geq 0$, we obtain a filtration $\mathrm{E} = \mathrm{Fil}^0 \mathrm{E} \supseteq \mathrm{Fil}^1 \mathrm{E} \supseteq \cdots$ of differential graded ideals of E. This yields a projective system $\mathrm{E}_\bullet = ((\mathrm{E}_\ell)_{\ell \geq 1}, \mathrm{R} \colon \mathrm{E}_{\ell+1} \to \mathrm{E}_\ell)$ of differential graded algebras, where $\mathrm{E}_\ell := \mathrm{E} \,/\, \mathrm{Fil}^\ell \mathrm{E}$ and $\mathrm{R} \colon \mathrm{E}_{\ell+1} \twoheadrightarrow \mathrm{E}_\ell$ for all $\ell \geq 0$.

Theorem A.6.16. *Let $\mathrm{E}_\bullet = ((\mathrm{E}_\ell)_{\ell \geq 1}, \mathrm{R} \colon \mathrm{E}_{\ell+1} \to \mathrm{E}_\ell)$ be the projective system defined above.*

(a) The projective system $\mathrm{E}_\bullet$ together with V is a de Rham V-pro-complex, where E^0_ℓ is identified with $\mathrm{W}_\ell(K[\boldsymbol{x}])$ for all $\ell \geq 1$ via a $\mathrm{W}(K)$-algebra isomorphism

$$\tau \colon \mathrm{W}_\ell(K[\boldsymbol{x}]) \to \mathrm{E}^0_\ell$$

satisfying $\tau\,\mathrm{V} = \mathrm{V}\,\tau$ and $\tau([x_i]) = x_i$ for all $i \in [n]$.

(b) We have an isomorphism $\mathrm{W}_\bullet \Omega^\bullet_{K[\boldsymbol{x}]} \cong \mathrm{E}_\bullet$ *of de Rham* V*-pro-complexes.*

Proof. The case $K = \mathbb{F}_p$ follows from [Ill79, Théorème I.2.5]. Now let $K/\mathbb{F}_p$ be an algebraic extension. Then K is perfect, thus Lemma A.6.13 yields an isomorphism

$$\mathrm{W}_\bullet \Omega^\bullet_{K[\boldsymbol{x}]} \cong \mathrm{W}_\bullet(K) \otimes_{\mathrm{W}(\mathbb{F}_p)} \mathrm{W}_\bullet \Omega^\bullet_{\mathbb{F}_p[\boldsymbol{x}]}$$

of de Rham V-pro-complexes. □

Lemma A.6.17 ([Ill79, Corollaire I.2.13])**.** *For all* $\ell \geq 0$*, we have an injective map* $p\colon \mathrm{E}_\ell \to \mathrm{E}_{\ell+1}$*, induced by multiplication with* p *in* E.

Bibliography

[AB03] Manindra Agrawal and Somenath Biswas. Primality and Identity Testing via Chinese Remaindering. *Journal of the ACM*, 50:429–443, 2003. 2, 30

[AB09] Sanjeev Arora and Boaz Barak. *Computational Complexity: A Modern Approach*. Cambridge University Press, Cambridge, 2009. 123, 130

[ABKM06] Eric Allender, Peter Bürgisser, Johan Kjeldgaard-Pedersen, and Peter Bro Miltersen. On the Complexity of Numerical Analysis. In *Proceedings of the 21st Annual IEEE Conference on Computational Complexity (CCC)*, pages 331–339, 2006. 32

[Agr03] Manindra Agrawal. On Derandomizing Tests for Certain Polynomial Identities. In *Proceedings of the 18th IEEE Annual Conference on Computational Complexity (CCC)*, pages 355–359, 2003. 2, 33

[Agr05] Manindra Agrawal. Proving Lower Bounds Via Pseudo-random Generators. In *Proceedings of the 25th International Conference on Foundations of Software Technology and Theoretical Computer Science (FSTTCS)*, volume 3821 of *Lecture Notes in Computer Science*, pages 92–105, 2005. 2, 33, 39, 48

[AHT07] Manindra Agrawal, Thanh Minh Hoang, and Thomas Thierauf. The Polynomially Bounded Perfect Matching Problem Is in $\mathbf{NC}^2$. In *Proceedings of the 24th Annual Symposium on Theoretical Aspects of Computer Science(STACS)*, volume 4393 of *Lecture Notes in Computer Science*, pages 489–499, 2007. 2, 48

[AKS04] Manindra Agrawal, Neeraj Kayal, and Nitin Saxena. PRIMES is in P. *Annals of Mathematics*, 160(2):781–793, 2004. 2, 33

[ALM+98] Sanjeev Arora, Carsten Lund, Rajeev Motwani, Madhu Sudan, and Mario Szegedy. Proof Verification and the Hardness of Approximation Problems. *Journal of the ACM*, 45(3):501–555, 1998. 2

[Alo99] Noga Alon. Combinatorial Nullstellensatz. *Combinatorics, Probability and Computing*, 8:7–29, 1999. 28

[AM69] Michael F. Atiyah and Ian G. Macdonald. *Introduction to Commutative Algebra*. Addison-Wesley, Reading, Massachusetts, 1969. 73

[AM08] V. Arvind and Partha Mukhopadhyay. Derandomizing the Isolation Lemma and Lower Bounds for Circuit Size. In *Proceedings of the 11th International Workshop, APPROX 2008, and 12th International Workshop, RANDOM 2008, on Approximation, Randomization and Combinatorial Optimization: Algorithms and Techniques*, volume 5171 of *Lecture Notes in Computer Science*, pages 276–289, 2008. 33, 34

[AM10] V. Arvind and Partha Mukhopadhyay. The Ideal Membership Problem and polynomial identity testing. *Information and Computation*, 208(4):351–363, 2010. 2, 27, 57

[AS98] Sanjeev Arora and Shmuel Safra. Probabilistic Checking of Proofs: A New Characterization of NP. *Journal of the ACM*, 45(1):70–122, 1998. 2

[AS09] Manindra Agrawal and Ramprasad Saptharishi. Classifying Polynomials and Identity Testing. In N. Mukunda, editor, *Current Trends in Science – Platinum Jubilee Special*, pages 149–162. Indian Academy of Sciences, 2009. 9

[ASS12] Manindra Agrawal, Chandan Saha, and Nitin Saxena. Quasi-polynomial Hitting-set for Set-depth-Delta Formulas. Manuscript, available at `http://arxiv.org/pdf/1209.2333v1.pdf`, September 2012. 66

[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 Annual ACM Symposium on Theory of Computing (STOC)*, pages 599–614, 2012. 4, 116

[AV08] Manindra Agrawal and V. Vinay. Arithmetic Circuits: A Chasm at Depth Four. In *Proceedings of the 49th Annual IEEE Symposium on Foundations of Computer Science (FOCS)*, pages 67–75, 2008. 2

[BCGR92] Samuel R. Buss, Stephen A. Cook, Arvind Gupta, and Vijaya Ramachandran. An Optimal Parallel Algorithm for Formula Evaluation. *SIAM J. on Computing*, 21(4):755–780, 1992. 25

[BCW80] Manuel Blum, Ashok K. Chandra, and Mark N. Wegman. Equivalence of free boolean graphs can be decided probabilistically in polynomial time. *Information Processing Letters*, 10(2):80–82, 1980. 2

[BE11] Markus Bläser and Christian Engels. Randomness Efficient Testing of Sparse Black Box Identities of Unbounded Degree over the Reals. In *Proceedings of the 28th International Symposium on Theoretical Aspects of Computer Science (STACS)*, pages 555–566, 2011. 30, 48

[Ben81] Michael Ben-Or. Probabilistic algorithms in finite fields. In *Proceedings of the 22nd Annual IEEE Symposium on Foundations of Computer Science (FOCS)*, pages 394–398, 1981. 135

[Ber84] Stuart J. Berkowitz. On computing the determinant in small parallel time using a small number of processors. *Information Processing Letters*, 18(3):147–150, 1984. 3, 132

[BFL91] László Babai, Lance Fortnow, and Carsten Lund. Non-deterministic exponential time has two-prover interactive protocols. *Computational Complexity*, 1(1):3–40, 1991. 2

[BFLS91] László Babai, Lance Fortnow, Leonid A. Levin, and Mario Szegedy. Checking Computations in Polylogarithmic Time. In *Proceedings of the 23rd Annual ACM Symposium on Theory of Computing (STOC)*, pages 21–31, 1991. 2

[BHLV09] Markus Bläser, Moritz Hardt, Richard J. Lipton, and Nisheeth K. Vishnoi. Deterministically testing sparse polynomial identities of unbounded degree. *Information Processing Letters*, 109(3):187–192, 2009. 2, 33, 48, 49

[BHS08] Markus Bläser, Moritz Hardt, and David Steurer. Asymptotically Optimal Hitting Sets Against Polynomials. In *Proceedings of the*

35th International Colloquium on Automata, Languages and Programming (ICALP), volume 5125 of *Lecture Notes in Computer Science*, pages 345–356, 2008. 30

[BK95] Manuel Blum and Sampath Kannan. Designing Programs that Check Their Work. *Journal of the ACM*, 42(1):269–291, 1995. 2

[BMS11] Malte Beecken, Johannes Mittmann, and Nitin Saxena. Algebraic Independence and Blackbox Identity Testing. In *Proceedings of the 38th International Colloquium on Automata, Languages and Programming (ICALP)*, volume 6756 of *Lecture Notes in Computer Science*, pages 137–148, 2011. 4, 5, 71, 100

[BMS13] Malte Beecken, Johannes Mittmann, and Nitin Saxena. Algebraic independence and blackbox identity testing. *Information and Computation*, 222:2–19, 2013. 4, 5, 71, 79

[BPR06] Saugata Basu, Richard Pollack, and Marie-Françoise Roy. *Algorithms in Real Algebraic Geometry*. Springer-Verlag, Berlin, second edition, 2006. 38, 125

[Bro87] W. Dale Brownawell. Bounds for the degrees in the Nullstellensatz. *Annals of Mathematics*, 126:277–591, 1987. 78

[BS83] Walter Baur and Volker Strassen. The complexity of partial derivatives. *Theoretical Computer Science*, 22(3):317–330, 1983. 4, 118, 121

[BT88] Michael Ben-Or and Prasoon Tiwari. A Deterministic Algorithm for Sparse Multivariate Polynomial Interpolation. In *Proceedings of the 20th Annual ACM Symposium on Theory of Computing (STOC)*, pages 301–309, 1988. 48

[BvzGH82] Allan Borodin, Joachim von zur Gathen, and John Hopcroft. Fast parallel matrix and GCD computations. *Information and Control*, 52(3):241–256, 1982. 21

[CDGK91] Michael Clausen, Andreas Dress, Johannes Grabmeier, and Marek Karpinski. On zero-testing and interpolation of k-sparse multivariate polynomials over finite fields. *Theoretical Computer Science*, 84(2):151–164, 1991. 48

[CK00] Zhi-Zhong Chen and Ming-Yang Kao. Reducing Randomness via Irrational Numbers. *SIAM J. on Computing*, 29(4):1247–1256, 2000. 2, 30

[CKW11] Xi Chen, Neeraj Kayal, and Avi Wigderson. Partial Derivatives in Arithmetic Complexity and Beyond. *Foundations and Trends in Theoretical Computer Science*, 6(1–2):1–138, 2011. 3, 64, 65, 67

[CLO97] David A. Cox, John B. Little, and Donal O'Shea. *Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra*. Springer-Verlag, New York, second edition, 1997. 134

[Coh93] Henri Cohen. *A Course in Computational Algebraic Number Theory*. Springer-Verlag, Berlin, 1993. 133

[CRS95] Suresh Chari, Pankaj Rohatgi, and Aravind Srinivasan. Randomness-Optimal Unique Element Isolation with Applications to Perfect Matching and Related Problems. *SIAM J. on Computing*, 24(5):1036–1050, 1995. 33

[DGW09] Zeev Dvir, Ariel Gabizon, and Avi Wigderson. Extractors and rank extractors for polynomial sources. *Computational Complexity*, 18(1):1–58, 2009. 4, 79, 80, 117, 118

[DL78] Richard A. DeMillo and Richard J. Lipton. A probabilistic remark on algebraic program testing. *Information Processing Letters*, 7(4):193–195, 1978. 1, 27

[DS07] Zeev Dvir and Amir Shpilka. Locally Decodable Codes with Two Queries and Polynomial Identity Testing for Depth 3 Circuits. *SIAM J. on Computing*, 36(5):1404–1434, 2007. 5, 57, 71, 112, 115

[DSY09] Zeev Dvir, Amir Shpilka, and Amir Yehudayoff. Hardness-Randomness Tradeoffs for Bounded Depth Arithmetic Circuits. *SIAM J. on Computing*, 39(4):1279–1293, 2009. 2

[Dub90] Thomas W. Dubé. The Structure of Polynomial Ideals and Gröbner Bases. *SIAM J. on Computing*, 19(4):750–773, 1990. 123

[Dvi09] Zeev Dvir. Extractors for Varieties. In *Proceedings of the 24th Annual IEEE Conference on Computational Complexity (CCC)*, pages 102–113, 2009. 4

[Edw00] Harold M. Edwards. *Fermat's Last Theorem: A Genetic Introduction to Algebraic Number Theory*. Springer-Verlag, New York, 2000. 10, 11

[Eis95] David Eisenbud. *Commutative Algebra with a View Toward Algebraic Geometry*. Springer-Verlag, New York, 1995. 136, 139, 141

[ER93] Richard Ehrenborg and Gian-Carlo Rota. Apolarity and Canonical Forms for Homogeneous Polynomials. *Europ. J. Combinatorics*, 14(3):157–181, 1993. 79

[FGL+96] Uriel Feige, Shafi Goldwasser, László Lovász, Shmuel Safra, and Mario Szegedy. Interactive Proofs and the Hardness of Approximating Cliques. *Journal of the ACM*, 43(2):268–292, 1996. 2

[Fra91] Gudmund S. Frandsen. Parallel Construction of Irreducible Polynomials. Technical Report DAIMI-PB-358, Department of Computer Science, University of Aarhus, 1991. 20

[FS12a] Michael A. Forbes and Amir Shpilka. On Identity Testing of Tensors, Low-rank Recovery and Compressed Sensing. In *Proceedings of the 44th Annual ACM Symposium on Theory of Computing (STOC)*, pages 163–172, 2012. Full version available at `http://arxiv.org/pdf/1111.0663v1.pdf`. 47, 66

[FS12b] Michael A. Forbes and Amir Shpilka. Quasipolynomial-time Identity Testing of Non-Commutative and Read-Once Oblivious Algebraic Branching Programs. Manuscript, available at `http://arxiv.org/pdf/1209.2408v1.pdf`, September 2012. 44, 51, 66, 67

[GK87] Dima Yu. Grigoriev and Marek Karpinski. The matching problem for bipartite graphs with polynomially bounded permanents is in NC. In *Proceedings of the 28th Annual IEEE Symposium on Foundations of Computer Science (FOCS)*, pages 166–172, 1987. 2, 48

[GKS90] Dima Yu. Grigoriev, Marek Karpinski, and Michael F. Singer. Fast Parallel Algorithms for Sparse Multivariate Polynomial Interpolation over Finite Fields. *SIAM J. on Computing*, 19(6):1059–1063, 1990. 20, 48

[GR08] Ariel Gabizon and Ran Raz. Deterministic extractors for affine sources over large fields. *Combinatorica*, 28(4):415–440, 2008. 3, 46, 47

[Grö49] Wolfgang Gröbner. *Moderne Algebraische Geometrie*. Springer-Verlag, Wien, 1949. 79

[Grü03] Branko Grünbaum. *Convex Polytopes*. Springer-Verlag, New York, second edition, 2003. 53

[Haz09] Michiel Hazewinkel. Witt vectors. Part 1. In Michiel Hazewinkel, editor, *Handbook of Algebra*, volume 6, pages 319–472. North-Holland, 2009. 142, 143

[Hei83] Joos Heintz. Definability and fast quantifier elimination in algebraically closed fields. *Theoretical Computer Science*, 24(3):239–277, 1983. 138

[HM97] Holly P. Hirst and Wade T. Macey. Bounding the Roots of Polynomials. *The College Mathematics Journal*, 28(4):292–295, 1997. 32

[HS80a] Joos Heintz and Claus P. Schnorr. Testing polynomials which are easy to compute (Extended Abstract). In *Proceedings of the 12th Annual ACM Symposium on Theory of Computing (STOC)*, pages 262–272, 1980. 2, 35, 39, 138

[HS80b] Joos Heintz and Malte Sieveking. Lower bounds for polynomials with algebraic coefficients. *Theoretical Computer Science*, 11(3):321–330, 1980. 35, 37

[Ier89] Doug Ierardi. Quantifier Elimination in the Theory of an Algebraically-closed Field. In *Proceedings of the 21st Annual ACM Symposium on Theory of Computing (STOC)*, pages 138–147, 1989. 39

[Ill79] Luc Illusie. Complexe de de Rham-Witt et cohomologie cristalline. *Ann. scient. Éc. Norm. Sup.*, 12(4):501–661, 1979. 6, 80, 87, 142, 146, 147, 149

[IM83] Oscar H. Ibarra and Shlomo Moran. Probabilistic Algorithms for Deciding Equivalence of Straight-Line Programs. *Journal of the ACM*, 30(1):217–228, 1983. 2, 13, 22, 23, 30

[Jac41] Carl G. J. Jacobi. De determinantibus functionalibus. *J. Reine Angew. Math.*, 22(4):319–359, 1841. 4, 78

[Kal85] K. A. Kalorkoti. A Lower Bound for the Formula Size of Rational Functions. *SIAM J. on Computing*, 14(3):678–687, 1985. 4

[Kay09] Neeraj Kayal. The Complexity of the Annihilating Polynomial. In *Proceedings of the 24th Annual IEEE Conference on Computational Complexity (CCC)*, pages 184–193, 2009. 4, 74, 117, 118, 123, 124

[Kay10] Neeraj Kayal. Algorithms for Arithmetic Circuits. Technical Report TR10-073, Electronic Colloquium on Computational Complexity (ECCC), 2010. 3, 42, 65

[Kem96] Gregor Kemper. A Constructive Approach to Noether's Problem. *Manuscripta Math.*, 90:343–363, 1996. 76

[Kem11] Gregor Kemper. *A Course in Commutative Algebra*. Springer-Verlag, Berlin, 2011. 73, 91, 136, 137

[KI04] Valentine Kabanets and Russell Impagliazzo. Derandomizing Polynomial Identity Tests Means Proving Circuit Lower Bounds. *Computational Complexity*, 13:1–46, 2004. 2, 30

[KM96] Klaus Kühnle and Ernst W. Mayr. Exponential Space Computation of Gröbner Bases. In *Proceedings of the 1996 International Symposium on Symbolic and Algebraic Computation (ISSAC)*, pages 63–71, 1996. 122, 123

[KMO+12] Stefan Kiefer, Andrzej S. Murawski, Joël Ouaknine, Björn Wachter, and James Worrell. On the Complexity of the Equivalence Problem for Probabilistic Automata. In *Proceedings of the 15th International Conference on Foundations of Software Science and Computation Structures (FoSSaCS)*, volume 7213 of *Lecture Notes in Computer Science*, pages 467–481, 2012. 2

[Kob84] Neal Koblitz. *p-adic Numbers, p-adic Analysis, and Zeta-Functions*. Springer-Verlag, New York, second edition, 1984. 144

[Koi96] Pascal Koiran. Hilbert's Nullstellensatz Is in the Polynomial Hierarchy. *Journal of Complexity*, 12(4):273–286, 1996. 25

[KR00] Martin Kreuzer and Lorenzo Robbiano. *Computational Commutative Algebra 1*. Springer-Verlag, Berlin, 2000. 78, 122, 124, 125, 133

[KR05] Martin Kreuzer and Lorenzo Robbiano. *Computational Commutative Algebra 2*. Springer-Verlag, Berlin, 2005. 73

[Kro82] Leopold Kronecker. *Grundzüge einer arithmetischen Theorie der algebraischen Grössen*. G. Reimer, Berlin, 1882. 31

[KS01] Adam R. Klivans and Daniel A. Spielman. Randomness Efficient Identity Testing of Multivariate Polynomials. In *Proceedings of the 33rd Annual ACM Symposium on Theory of Computing (STOC)*, pages 216–223, 2001. 2, 30, 33, 34, 48

[KS07] Neeraj Kayal and Nitin Saxena. Polynomial Identity Testing for Depth 3 Circuits. *Computational Complexity*, 16(2):115–138, 2007. 57, 115

[KS09] Neeraj Kayal and Shubhangi Saraf. Blackbox Polynomial Identity Testing for Depth 3 Circuits. In *Proceedings of the 50th Annual IEEE Symposium on Foundations of Computer Science (FOCS)*, pages 198–207, 2009. 57, 115

[KS11a] Zohar S. Karnin and Amir Shpilka. Black box polynomial identity testing of generalized depth-3 arithmetic circuits with bounded top fan-in. *Combinatorica*, 31(3):333–364, 2011. 3, 5, 57, 71, 112, 114

[KS11b] Neeraj Kayal and Chandan Saha. On the Sum of Square Roots of Polynomials and Related Problems. In *Proceedings of the 26th Annual IEEE Conference on Computational Complexity (CCC)*, pages 292–299, 2011. 119

[Lad75] Richard E. Ladner. The Circuit Value Problem is Log Space Complete for P. *ACM SIGACT News*, 7(1):18–20, 1975. 26

[Lan02] Serge Lang. *Algebra*. Springer-Verlag, New York, revised third edition, 2002. 135

[Len91] Hendrik W. Lenstra Jr. Finding isomorphisms between finite fields. *Mathematics of Computation*, 56(193):329–347, 1991. 20, 120

[LFKN92] Carsten Lund, Lance Fortnow, Howard Karloff, and Noam Nisan. Algebraic Methods for Interactive Proof Systems. *Journal of the ACM*, 39(4):859–868, 1992. 2

[Lov79] László Lovász. On determinants, matchings, and random algorithms. In *Fundamentals of Computation Theory (FCT)*, pages 565–574, 1979. 2

[Lov89] László Lovász. Singular spaces of matrices and their applications in combinatorics. *Bol. Soc. Braz. Mat.*, 20(1):87–99, 1989. 2

[LP11] Hendrik W. Lenstra Jr. and Carl Pomerance. Primality testing with Gaussian periods. Manuscript, available at `http://www.math.dartmouth.edu/~carlp/aks041411.pdf`, April 2011. 20

[L'v84] M. S. L'vov. Calculation of invariants of programs interpreted over an integrality domain. *Kibernetika*, 4:23–28, 1984. 4

[LV98] Daniel Lewin and Salil Vadhan. Checking Polynomial Identities over any Field: Towards a Derandomization? In *Proceedings of the 30th Annual ACM Symposium on Theory of Computing (STOC)*, pages 438–447, 1998. 30

[Mic10] Mateusz Michałek. A Short Proof of Combinatorial Nullstellensatz. *Amer. Math. Monthly*, 117(9):821–823, 2010. 28

[MM82] Ernst W. Mayr and Albert R. Meyer. The complexity of the word problems for commutative semigroups and polynomial ideals. *Advances in Mathematics*, 46(3):305–329, 1982. 123

[Mor96] Patrick Morandi. *Field and Galois Theory*. Springer-Verlag, New York, 1996. 135, 139

[MRK88] Gary L. Miller, Vijaya Ramachandran, and Erich Kaltofen. Efficient Parallel Evaluation of Straight-Line Code and Arithmetic Circuits. *SIAM J. on Computing*, 17(4):687–695, 1988. 25, 26

[MSS12] Johannes Mittmann, Nitin Saxena, and Peter Scheiblechner. Algebraic Independence in Positive Characteristic – A p-Adic Calculus. Manuscript, available at `http://arxiv.org/pdf/1202.4301.pdf`, February 2012. 4, 6, 71, 127

[Mul12] Ketan D. Mulmuley. Geometric Complexity Theory V: Equivalence between blackbox derandomization of polynomial identity

testing and derandomization of Noether's Normalization Lemma. Manuscript, available at `http://arxiv.org/pdf/1209.5993v2.pdf`, November 2012. 2

[MVV87] Ketan D. Mulmuley, Umesh V. Vazirani, and Vijay V. Vazirani. Matching is as easy as matrix inversion. *Combinatorica*, 7(1):105–113, 1987. 33

[Nar12] Władysław Narkiewicz. *Rational Number Theory in the 20th Century: From PNT to FLT*. Springer-Verlag, London, 2012. 10

[Ore22] Øystein Ore. Über höhere Kongruenzen. *Norsk Mat. Forenings Skrifter Ser. I*, 7:15, 1922. 27

[Ost75] Alexander M. Ostrowski. On multiplication and factorization of polynomials, I. Lexicographic orderings and extreme aggregates of terms. *Aequationes Mathematicae*, 13(3):201–228, 1975. 53

[Pap94] Christos H. Papadimitriou. *Computational Complexity*. Addison Wesley, Reading, Massachusetts, 1994. 130

[Per27] Oskar Perron. *Algebra I (Die Grundlagen)*. Walter de Gruyter, Berlin, 1927. 4, 74

[Pie10] Tito Piezas. A Collection of Algebraic Identities, 2010. Website, available at `https://sites.google.com/site/tpiezas/Home`. 10

[Pło05] Arkadiusz Płoski. Algebraic Dependence of Polynomials After O. Perron and Some Applications. In Svetlana Cojocaru, Gerhard Pfister, and Victor Ufnarovski, editors, *Computational Commutative and Non-Commutative Algebraic Geometry*, pages 167–173. IOS Press, 2005. 74, 78

[Rag69] R. Raghavendran. Finite Associative Rings. *Compositio Mathematica*, 21(2):195–229, 1969. 144

[Rob00] Alain M. Robert. *A Course in p-adic Analysis*. Springer-Verlag, New York, 2000. 144

[RS62] J. Barkley Rosser and Lowell Schoenfeld. Approximate formulas for some functions of prime numbers. *Illinois J. Math.*, 6(1):64–94, 1962. 130

[RS05] Ran Raz and Amir Shpilka. Deterministic polynomial identity testing in non-commutative models. *Computational Complexity*, 14(1):1–19, 2005. 41, 66

[Sah08] Chandan Saha. A Note on Irreducible Polynomials and Identity Testing. Manuscript, available at `http://www.cse.iitk.ac.in/users/csaha/PID_CR.pdf`, May 2008. 20

[Sax08] Nitin Saxena. Diagonal Circuit Identity Testing and Lower Bounds. In *Proceedings of the 35th International Colloquium on Automata, Languages and Programming (ICALP)*, volume 5125 of *Lecture Notes in Computer Science*, pages 60–71, 2008. 2, 67

[Sax09] Nitin Saxena. Progress on Polynomial Identity Testing. *Bulletin of the European Association for Theoretical Computer Science (EATCS)*, 99:49–79, 2009. 9

[Sch80] Jacob T. Schwartz. Fast Probabilistic Algorithms for Verification of Polynomial Identities. *Journal of the ACM*, 27(4):701–717, 1980. 1, 27

[Sch00] Andrzej Schinzel. *Polynomials with special regard to reducibility.* Cambridge University Press, Cambridge, 2000. 110

[Sha92] Adi Shamir. IP = PSPACE. *Journal of the ACM*, 39(4):869–877, 1992. 2

[Sin80] David Singmaster. Divisiblity of binomial and multinomial coefficients by primes and prime powers. *A Collection of Manuscripts Related to the Fibonacci Sequence, 18th Anniversary Volume of the Fibonacci Association*, pages 98–113, 1980. 145

[Sol02] Michael Soltys. Berkowitz's algorithm and clow sequences. *The Electronic Journal of Linear Algebra*, 9:42–54, 2002. 132

[SS10] Nitin Saxena and C. Seshadhri. From Sylvester-Gallai Configurations to Rank Bounds: Improved Black-box Identity Test for Depth-3 Circuits. In *Proceedings of the 51st Annual IEEE Symposium on Foundations of Computer Science (FOCS)*, pages 21–29, 2010. Full version available at `http://arxiv.org/pdf/1002.0145v2.pdf`. 57, 60, 115

[SS11a] Nitin Saxena and C. Seshadhri. An Almost Optimal Rank Bound for Depth-3 Identities. *SIAM J. on Computing*, 40(1):200–224, 2011. 57, 115

[SS11b] 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 Annual ACM Symposium on Theory of Computing (STOC)*, pages 431–440, 2011. 2, 3, 57, 58, 59

[SSS11] Chandan Saha, Ramprasad Saptharishi, and Nitin Saxena. A Case of Depth-3 Identity Testing, Sparse Factorization and Duality. Technical Report TR11-021, Electronic Colloquium on Computational Complexity (ECCC), 2011. 67, 113

[Stu96] Bernd Sturmfels. *Gröbner Bases and Convex Polytopes*. American Mathematical Society, Providence, Rhode Island, 1996. 94

[SV11] Shubhangi Saraf and Ilya Volkovich. Black-Box Identity Testing of Depth-4 Multilinear Circuits. In *Proceedings of the 43rd Annual ACM Symposium on Theory of Computing (STOC)*, pages 421–430, 2011. 2

[SY10] Amir Shpilka and Amir Yehudayoff. Arithmetic Circuits: A Survey of Recent Results and Open Questions. *Foundations and Trends in Theoretical Computer Science*, 5(3–4):207–388, 2010. 9, 35

[Val79] Leslie G. Valiant. The complexity of computing the permanent. *Theoretical Computer Science*, 8(2):189–201, 1979. 6, 131

[vdE00] Arno van den Essen. *Polynomial Automorphisms and the Jacobian Conjecture*. Birkhäuser Verlag, Basel, 2000. 75

[VSBR83] Leslie G. Valiant, Sven Skyum, Stuart J. Berkowitz, and Charles Rackoff. Fast Parallel Computation of Polynomials Using Few Processors. *SIAM J. on Computing*, 12(4):641–644, 1983. 17

[vzGG03] Joachim von zur Gathen and Jürgen Gerhard. *Modern Computer Algebra*. Cambridge University Press, Cambridge, second edition, 2003. 69

[vzGK85] Joachim von zur Gathen and Erich Kaltofen. Factoring Sparse Multivariate Polynomials. *Journal of Computer and System Sciences*, 31(2):265–287, 1985. 113

[Wan03] Zhe-Xian Wan. *Lectures on finite fields and Galois rings*. World Scientific, Singapore, 2003. 119, 144

[Wit37] Ernst Witt. Zyklische Körper und Algebren der Charakteristik p vom Grad p^n. *Journal für die reine und angewandte Mathematik*, 176:126–140, 1937. 142

[Zen93] Jiang Zeng. A Bijective Proof of Muir's Identity and the Cauchy-Binet Formula. *Linear Algebra and its Applications*, 184(15):79–82, 1993. 132

[Zie95] Günter M. Ziegler. *Lectures on Polytopes*. Springer Verlag, New York, 1995. 53

[Zip79] Richard Zippel. Probabilistic algorithms for sparse polynomials. In *Proceedings of the International Symposium on Symbolic and Algebraic Manipulation (EUROSAM)*, pages 216–226, 1979. 1, 27

[Zip90] Richard Zippel. Interpolating Polynomials from their Values. *Journal of Symbolic Computation*, 9:375–403, 1990. 48

Index

Publications

(1) Malte Beecken, Johannes Mittmann, and Nitin Saxena. Algebraic Independence and Blackbox Identity Testing. In *Proceedings of the 38th International Colloquium on Automata, Languages and Programming (ICALP)*, volume 6756 of *Lecture Notes in Computer Science*, pages 137–148, 2011. (Best paper award in Track A of ICALP 2011.)

(2) Malte Beecken, Johannes Mittmann, and Nitin Saxena. Algebraic independence and blackbox identity testing. *Information and Computation*, 222:2–19, 2013. (ICALP 2011's special issue.)

(3) Johannes Mittmann, Nitin Saxena, and Peter Scheiblechner. Algebraic Independence in Positive Characteristic – A p-Adic Calculus. Submitted, `http://arxiv.org/pdf/1202.4301.pdf`, 2012.