Arithmetic Circuits: A Survey of Recent Results and Open Questions

Arithmetic Circuits: A Survey of Recent Results and Open Questions

Amir Shpilka

Faculty of Computer Science
Technion, Haifa 32000
Israel
shpilka@cs.technion.ac.il

Amir Yehudayoff

Faculty of Mathematics
Technion, Haifa 32000
Israel
amir.yehudayoff@gmail.com

now
the essence of knowledge
Boston – Delft

Foundations and Trends® in Theoretical Computer Science

Published, sold and distributed by:
now Publishers Inc.
PO Box 1024
Hanover, MA 02339
USA
Tel. +1-781-985-4510
www.nowpublishers.com
sales@nowpublishers.com

Outside North America:
now Publishers Inc.
PO Box 179
2600 AD Delft
The Netherlands
Tel. +31-6-51115274

The preferred citation for this publication is A. Shpilka and A. Yehudayoff, Arithmetic Circuits: A Survey of Recent Results and Open Questions, Foundation and Trends® in Theoretical Computer Science, vol 5, nos 3–4, pp 207–388, 2009

ISBN: 978-1-60198-400-5

Foundations and Trends® in Theoretical Computer Science
Volume 5 Issues 3–4, 2009

Editorial Board

Editorial Scope

Foundations and Trends® in Theoretical Computer Science will publish survey and tutorial articles in the following topics:

- Algorithmic game theory
- Computational algebra
- Computational aspects of combinatorics and graph theory
- Computational aspects of communication
- Computational biology
- Computational complexity
- Computational geometry
- Computational learning
- Computational Models and Complexity
- Computational Number Theory
- Cryptography and information security
- Data structures
- Database theory
- Design and analysis of algorithms
- Distributed computing
- Information retrieval
- Operations Research
- Parallel algorithms
- Quantum Computation
- Randomness in Computation

Information for Librarians
Foundations and Trends® in Theoretical Computer Science, 2009, Volume 5, 4 issues. ISSN paper version 1551-305X. ISSN online version 1551-3068. Also available as a combined paper and online subscription.

Foundations and Trends® in
Theoretical Computer Science
Vol. 5, Nos. 3–4 (2009) 207–388

DOI: 10.1561/0400000039

now
the essence of knowledge

Arithmetic Circuits: A Survey of Recent Results and Open Questions

Amir Shpilka[1] and Amir Yehudayoff[2]

[1] *Faculty of Computer Science, Technion, Haifa 32000, Israel, shpilka@cs.technion.ac.il*
[2] *Faculty of Mathematics, Technion, Haifa 32000, Israel, amir.yehudayoff@gmail.com*

Abstract

A large class of problems in symbolic computation can be expressed as the task of computing some polynomials; and arithmetic circuits form the most standard model for studying the complexity of such computations. This algebraic model of computation attracted a large amount of research in the last five decades, partially due to its simplicity and elegance. Being a more structured model than Boolean circuits, one could hope that the fundamental problems of theoretical computer science, such as separating P from NP, will be easier to solve for arithmetic circuits. However, in spite of the appearing simplicity and the vast amount of mathematical tools available, no major breakthrough has been seen. In fact, all the fundamental questions are still open for this model as well. Nevertheless, there has been a lot of progress in the area and beautiful results have been found, some in the last few years. As examples we mention the connection between polynomial identity testing and lower bounds of Kabanets and Impagliazzo, the lower bounds

of Raz for multilinear formulas, and two new approaches for proving lower bounds: Geometric Complexity Theory and Elusive Functions.

The goal of this monograph is to survey the field of arithmetic circuit complexity, focusing mainly on what we find to be the most interesting and accessible research directions. We aim to cover the main results and techniques, with an emphasis on works from the last two decades. In particular, we discuss the recent lower bounds for multilinear circuits and formulas, the advances in the question of deterministically checking polynomial identities, and the results regarding reconstruction of arithmetic circuits. We do, however, also cover part of the classical works on arithmetic circuits. In order to keep this monograph at a reasonable length, we do not give full proofs of most theorems, but rather try to convey the main ideas behind each proof and demonstrate it, where possible, by proving some special cases.

Contents

1

Introduction

Arithmetic circuits are the most natural and standard model for computing polynomials. In this model the inputs are variables $x_1, \ldots, x_n$, and the computation is performed using the arithmetic operations $+, \times$ and may involve constants from a field $\mathbb{F}$. The output of an arithmetic circuit is thus a polynomial (or a set of polynomials) in the input variables. The complexity measures associated with such circuits are size and depth which capture the number of operations and the maximal distance between an input and an output, respectively.

The most fundamental problems in algebraic complexity are related to the complexity of arithmetic circuits: providing efficient algorithms for algebraic problems (e.g., matrix multiplication), proving lower bounds on the size and depth of arithmetic circuits, giving efficient deterministic algorithms for polynomial identity testing, and finding efficient reconstruction algorithms for polynomials computed by arithmetic circuits (the latter problem is sometimes referred to as learning arithmetic circuits or interpolating arithmetic circuits).

In the past 50 years, we have seen a flurry of beautiful and efficient algorithms for algebraic problems. For example, Cooley and Tukey's algorithm for the Discrete Fourier Transform [38], Strassen's algorithm

and those following it for Matrix Multiplication [39, 131] (see [30] for a detailed survey of algorithms for matrix multiplication), algorithms for factoring polynomials (see [72, 146, 147] for surveys of results in this area), and Csanky's algorithm for parallel computation of determinant as well as all other linear algebra problems [40]. In this survey we shall not give details of these algorithms, but rather focus on complexity questions related to arithmetic circuits, mainly on the problem of proving lower bounds for arithmetic circuits and the question of deterministically deciding polynomial identities.

Arithmetic circuits are a highly structured model of computation compared to Boolean circuits. For example, when studying arithmetic circuits we are interested in *syntactic* computation of polynomials, whereas in the study of Boolean circuits we are interested in the *semantics* of the computation. In other words, in the Boolean case we are not interested in any specific polynomial representation of the function but rather we just want to compute some representation of it, while in the arithmetic world we focus on a specific representation of the function. As such, one may hope that the P vs. NP question will be easier to solve in this model. However, in spite of many efforts, we are still far from understanding this fundamental problem. In fact, our understanding of most problems is far from being complete. In particular, we do not have strong lower bounds for arithmetic circuits; We do not know how to deterministically and efficiently determine whether a given arithmetic circuit computes the zero polynomial; and we do not know how to efficiently reconstruct a circuit using only queries to the polynomial it computes. Although seemingly different, these three problems are strongly related to each other, and it is usually the case that a new understanding of one problem sheds light on the other problems as well.

In recent years there has been some progress on these important problems for several interesting classes of arithmetic circuits. In this monograph we aim to describe this recent progress. In particular, we shall cover the new lower bounds on the size of multilinear circuits, the new identity testing algorithms for several restricted classes of circuits and their connection to circuit lower bounds, and the recent reconstruction algorithms for depth-3 arithmetic circuits. We also present many

open questions that we view as natural "next step" questions, given our current state of knowledge.

1.1 Basic Definitions

Before any further discussion, we give the basic definitions related to arithmetic circuits.

Definition 1.1 (Arithmetic circuits). An *arithmetic circuit* Φ over the field $\mathbb{F}$ and the set of variables X (usually, $X = \{x_1, \ldots, x_n\}$) is a directed acyclic graph as follows. The vertices of Φ are called *gates*. Every gate in Φ of in-degree 0 is labeled by either a variable from X or a field element from $\mathbb{F}$. Every other gate in Φ is labeled by either $\times$ or $+$ and has in-degree 2. An arithmetic circuit is called a *formula* if it is a directed tree whose edges are directed from the leaves to the root.

Every gate of in-degree 0 is called an *input gate* (even when the gate is labeled by a field element). Every gate of out-degree 0 is called an *output gate*. Every gate labeled by $\times$ is called a *product gate* and every gate labeled by $+$ is called a *sum gate*. The *size* of Φ, denoted $|\Phi|$, is the number of edges in Φ. The depth of a gate v in Φ, denoted depth (v), is the length of the longest directed path reaching v. The depth of Φ is the maximal depth of a gate in Φ. When speaking of bounded depth circuits — circuits whose depth is bounded by a constant independent of $|X|$ — we do not have a restriction on the fan-in. For two gates u and v in Φ, if (u, v) is an edge in Φ, then u is called a *child* of v, and v is called a *parent* of u.

An arithmetic circuit computes a polynomial in a natural way: An input gate labeled by $\alpha \in \mathbb{F} \cup X$ computes the polynomial α. A product gate computes the product of the polynomials computed by its children. A sum gate computes the sum of the polynomials computed by its children.

For a gate v in Φ, define Φ_v to be the sub-circuit of Φ rooted at v. Denote by X_v the set of variables that occur in the circuit Φ_v. We usually denote by f_v the polynomial in $\mathbb{F}[X_v]$ computed by the gate v in Φ. We sometimes abuse notation and denote by Φ_v the polynomial

computed by v as well. Define the *degree* of a gate v, denoted $\deg(v)$, to be the total degree of the polynomial f_v (e.g., the total degree of $x_1^2 x_2 + x_1 + 1$ is three, whereas the individual degrees are at most two). The *degree* of Φ is the maximal degree of a gate in Φ.

It is clear that every polynomial $f \in \mathbb{F}[X]$ can be computed by an arithmetic circuit and by an arithmetic formula. The main question is how many gates are needed for the computation.

The definition above shows an evident difference between arithmetic circuits and Boolean circuits. While Boolean circuits can perform operations on the "bit representation" of the input field elements, that are not necessarily the arithmetic operations, arithmetic circuits cannot. Nevertheless, most algorithms for algebraic problems fit naturally into the framework of arithmetic circuits.

One last thing to note is that we always regard an arithmetic circuit as computing a polynomial in $\mathbb{F}[X]$ and not a function from $\mathbb{F}^{|X|}$ to $\mathbb{F}$. In general, every polynomial defines a unique function, but a function can usually be expressed as a polynomial in many ways. For example, the polynomial $x^2 - x$ is not the zero polynomial as it has nonzero coefficients. However, over the field with two elements, $\mathbb{F}_2$, it computes the zero function. This distinction is especially important when studying the identity testing problem. This is another difference between the Boolean world and the arithmetic world.

Remark 1.1. For the rest of the survey, unless otherwise stated, the results hold for arbitrary fields. In most cases, for simplicity of discussion and notation, we do not explicitly state the dependence on the field. In general, the question of which field we are working over is important and can make a difference, both from a theoretical point of view and from a practical point of view. The main examples of fields that the reader should bear in mind are prime fields and the real numbers.

1.2 Arithmetic Complexity

Arithmetic complexity classes were first defined in the seminal works of Valiant [138, 141]. Valiant gave analogous definitions for the classes P and NP in the algebraic world, and showed complete problems for

these classes. We now give a very brief overview of these classes and state the main known results. As this material was covered in many places, we do not give any proofs here. For a more detailed treatment and proofs, we refer the interested reader to Refs. [29, 30, 61].

We begin by defining the class VP, the algebraic analog of the class P. Originally, Valiant called this class the class of p-bounded polynomials (computed by "polynomially bounded" circuits), but nowadays the notation VP is used (where V is an acronym for Valiant).

Definition 1.2. A family of polynomials $\{f_n\}$ over $\mathbb{F}$ is *p-bounded* if there exists some polynomial $t : \mathbb{N} \to \mathbb{N}$ such that for every n, both the number of variables in f_n and the degree of f_n are at most $t(n)$, and there is an arithmetic circuit of size at most $t(n)$ computing f_n. The class $\mathsf{VP}_{\mathbb{F}}$ consists of all p-bounded families over $\mathbb{F}$.

The polynomial $f_n(x) = x^{2^n}$, for example, can be computed by size $O(n)$ circuits, but it is not in VP as its degree is not polynomial. One motivation for this degree restriction comes from computation over, say, the rational numbers: if the degree is too high then we cannot efficiently represent the value of the polynomial on a given input by a "standard" Boolean circuit. Also note that in the definition we do not require the circuit computing f_n to have a polynomial degree, but, as we shall later see, this property holds without loss of generality (see Theorem 2.2 below).

An interesting family in VP is the family of determinants,

$$\mathrm{DET}_n(X) = \sum_{\sigma \in S_n} \mathrm{sgn}(\sigma) \prod_{i=1}^{n} x_{i,\sigma(i)},$$

where $X = (x_{i,j})$ is an $n \times n$ matrix, S_n is the set of permutations of n elements and $\mathrm{sgn}(\sigma)$ is the signature of the permutation σ. It is a nice exercise to find a polynomial size arithmetic circuit for DET_n that does not use divisions.

Remark 1.2. For the rest of the survey we sometimes say polynomial and mean a family of polynomials, e.g., when we talk of the

determinant polynomial we actually talk about the family of determinant polynomials.

We now define VNP, the algebraic analog of the class NP.

Definition 1.3. A family of polynomials $\{f_n\}$ over $\mathbb{F}$ is *p-definable* if there exist two polynomially bounded functions $t, k : \mathbb{N} \to \mathbb{N}$ and a family $\{g_n\}$ in $\mathsf{VP}_{\mathbb{F}}$ such that for every n,

$$f_n(x_1, \ldots, x_{k(n)}) = \sum_{w \in \{0,1\}^{t(n)}} g_{t(n)}(x_1, \ldots, x_{k(n)}, w_1, \ldots, w_{t(n)}).$$

The class $\mathsf{VNP}_{\mathbb{F}}$ consists of all p-definable families over $\mathbb{F}$.

Roughly speaking, VNP is the class of polynomials f so that given a monomial, one can efficiently compute the coefficient of this monomial in f (this does not follow immediately from the definition, for more details see, e.g., Refs. [61, 141]). To better understand the connection to NP, one can think of the variables $w = (w_1, \ldots, w_{t(n)})$ as the "witness," and so summing over all witnesses is the arithmetic analog of searching for a witness in NP. The existential quantifier in the definition of NP is translated to the algebraic operation of addition. In some sense, this makes VNP a version of #P as well. The canonical example for a family in VNP is the family of permanents of $n \times n$ matrices

$$\mathrm{PERM}_n(X) = \sum_{\sigma \in S_n} \prod_{i=1}^{n} x_{i,\sigma(i)}. \tag{1.1}$$

One way to see that permanent is in VNP is by Ryser's formula that also gives the smallest known circuit computing permanent (which is also a depth-3 circuit).

Fact 1.1 ([114]). For every $n \in \mathbb{N}$, $\mathrm{PERM}_n(X) = \sum_{T \subseteq [n]} (-1)^{n-|T|} \prod_{i=1}^{n} \sum_{j \in T} x_{i,j}$.

It follows by definition that $\mathsf{VP} \subseteq \mathsf{VNP}$. Valiant's hypothesis says that VP is a strict subclass of VNP.

Valiant's hypothesis I: $\mathsf{VP} \neq \mathsf{VNP}$.

As arithmetic circuits are more structured than Boolean circuits, one could hope that proving Valiant's hypothesis should be easier than its Boolean counterpart. A very weak version of this statement was proved in Ref. [61], where it was shown that in a non-associative world, where variables are not assumed to satisfy the identity $(xy)z = x(yz)$, **Valiant's hypothesis I** holds. This non-associative statement is an evidence for the obvious: the more structured the world is, the easier it is to prove lower bounds. Specifically, in a non-associative world algorithms cannot exploit "symmetries" that follow from associativity. Indeed, in such a world it is more difficult to design algorithms and lower bounds are easier to prove.

Besides defining the classes VP and VNP, Valiant also gave complete problems for these classes. He described a reduction between families of polynomials and gave complete families with respect to it.

Definition 1.4. A polynomial $f(x_1,\ldots,x_n)$ over $\mathbb{F}$ is called a *projection* of a polynomial $g(y_1,\ldots,y_m)$ over $\mathbb{F}$ if there exists an assignment $\rho \in (\{x_1,\ldots,x_n\} \cup \mathbb{F})^m$ such that $f(x_1,\ldots,x_n) \equiv g(\rho_1,\ldots,\rho_m)$. In other words, f can be derived from g by a simple substitution. This definition can be extended to projections between families of polynomials. The family $\{f_n\}$ is a *p-projection* of the family $\{g_n\}$ if there exists a polynomially bounded $t : \mathbb{N} \to \mathbb{N}$ such that for every n, f_n is a projection of $g_{t(n)}$.

Both VP and VNP are closed under projections, e.g., if f is in VP then any projection of f is also in VP. Valiant showed that permanent is complete for the class VNP.

Theorem 1.1 ([138]). For any field $\mathbb{F}$ such that $\mathrm{char}(\mathbb{F}) \neq 2$, the family $\{\mathrm{PERM}_n\}$ is VNP-complete. Namely, any family in VNP is a p-projection of it.

Valiant's hypothesis I is thus equivalent to proving a super-polynomial lower bound on the size of circuits computing the permanent. We note that a stronger version of Theorem 1.1 was proved in

Ref. [61], where it was shown that permanent is VNP-complete even in a very weak computational world where the variables are not assumed to be commutative nor associative.

Valiant also showed that determinant is VP-complete with respect to *quasi-polynomial* projections.

Theorem 1.2 ([138]). The family $\{\mathrm{DET}_n\}$ is VP-complete with respect to quasi-polynomial projections. That is, for any family $\{f_n\}$ in VP there exists a function $t : \mathbb{N} \to \mathbb{N}$ satisfying[1] $t(n) = n^{O(\log n)}$ such that f_n is a projection of $\mathrm{DET}_{t(n)}$. In fact, if we change the definition of VP to VQP by replacing polynomial by quasi-polynomial (i.e., $2^{\mathrm{polylog}(n)}$), then determinant is VQP-complete.

This theorem follows immediately from the next two theorems that show that arithmetic circuits are "shallow," and that determinant can "simulate" small formulas.

Theorem 1.3 ([143]). Let f be a degree r polynomial computed by a size s circuit. Then f can be computed by a circuit of size $\mathrm{poly}(r, s)$ and depth $O(\log r(\log r + \log s))$.

Theorem 1.3 was proved in a seminal work of Valiant et al. [143]. It is commonly rephrased as $\mathsf{VP} = \mathsf{VNC}^2$, where VNC^k denotes polynomial size and polynomial degree arithmetic circuits of depth $O(\log^k n)$. Clearly, $\mathsf{VNC}^1 \subseteq \mathsf{VNC}^2 \subseteq \ldots \subseteq \mathsf{VP}$, and Theorem 1.3 shows that in fact the chain halts after two steps. Since determinant is in VP, Theorem 1.3 implies that determinant has a formula of quasi-polynomial size (more generally, every polynomial in VNC^2 has a formula of quasi-polynomial size).

Theorem 1.4 ([138]). For any polynomial f in $\mathbb{F}[X]$ that can be computed by a formula of size s over $\mathbb{F}$, there is a matrix A of dimensions $(s+1) \times (s+1)$ whose entries are in $X \cup \mathbb{F}$ such that $\mathrm{DET}(A) = f$.

---

[1] Unless stated otherwise, logarithms are in base two.

As determinant is complete for VQP, an algebraic analog of the P vs. NP question is the question of "embedding" permanent in determinant.

Valiant's hypothesis II: VNP $\not\subset$ VQP.

This hypothesis is also known as *Valiant's extended hypothesis*. Stated differently, the hypothesis is that the permanent does not belong to VQP. Thus, in order to prove Valiant's extended hypothesis it suffices to prove that one cannot represent PERM_n as the determinant of a matrix of dimension quasi-polynomial in n. Currently, the best lower bounds on the dimension of such a matrix are given by the following theorem of [31, 92].

Theorem 1.5 ([31, 92]). Let $\mathbb{F}$ be a field of characteristic different than two and let $X = (x_{i,j})_{i,j\in[n]}$ be a matrix of variables. Then, any matrix A whose entries are linear functions in $\{x_{i,j}\}_{i,j\in[n]}$ over $\mathbb{F}$ such that $\mathrm{DET}(A) = \mathrm{PERM}_n(X)$ must be of dimension at least $n^2/2$.

Here is a rough sketch of the idea behind Mignon and Ressayre's proof of Theorem 1.5. Compute the rank of the Hessian matrix, i.e., the matrix of second partial derivatives, of both $\mathrm{PERM}_n(X)$ and $\mathrm{DET}(A)$. This rank for $\mathrm{PERM}_n(X)$ is at least (roughly) n^2, whereas for $\mathrm{DET}(A)$ this rank is of order D, where D is the dimension of A.

Valiant's extended hypothesis gives a way for reformulating a question about circuits as a purely algebraic question: the VQP vs. VNP problem is equivalent to the problem of embedding the permanent inside the determinant. One advantage of this formulation is that the combinatorial structure of circuits does not appear in it.

Open Problem 1. Improve the lower bound on the dimension of a matrix A with entries that are linear functions in $\{x_{i,j}\}_{i,j\in[n]}$ such that $\mathrm{DET}(A) = \mathrm{PERM}_n(X)$.

1.3 Arithmetic Circuit Classes

In addition to the general model of arithmetic circuits, introduced in Section 1.1, we will be considering several other, more restricted,

classes of arithmetic circuits. In particular, we will be interested in bounded depth arithmetic circuits, and even more specifically in depth-3 and depth-4 circuits, in multilinear circuits, noncommutative circuits and more. We shall now define some of these classes and discuss their importance.

The model of bounded depth circuits was already defined in Section 1.1. Two important subclasses of bounded depth circuits that we shall focus on in this monograph are depth-3 circuits, also known as $\Sigma\Pi\Sigma$ circuits and depth-4 circuits known as $\Sigma\Pi\Sigma\Pi$ circuits. A $\Sigma\Pi\Sigma$ circuit is a depth-3 circuit with an addition gate at the top, a middle layer of multiplication gates, and then a level of addition gates at the bottom. A $\Sigma\Pi\Sigma$ circuit with s multiplication gates compute polynomials of the form $\sum_{i=1}^{s}\prod_{j=1}^{d_i}\ell_{i,j}(x_1,\ldots,x_n)$, where the $\ell_{i,j}$'s are linear functions. Although a very restricted model this is the first class for which we do not have any strong lower bounds, over fields of characteristic zero (see Section 3.5). Moreover, in Section 3.8.2 we discuss a result of Raz [105] showing that strong lower bounds for (a restricted subclass of) $\Sigma\Pi\Sigma$ circuits imply super-polynomial lower bound on the formula complexity of permanent.

Similar to depth-3 circuits, a $\Sigma\Pi\Sigma\Pi$ circuit is composed of four alternating layers of addition and multiplication gates. Thus, a size s $\Sigma\Pi\Sigma\Pi$ circuit computes a polynomial of the form $\sum_{i=1}^{s}\prod_{j=1}^{d_i}f_{i,j}(x_1,\ldots,x_n)$, where the $f_{i,j}$'s are polynomials of degree at most s having at most s monomials (i.e., they are s-sparse polynomials). The importance of $\Sigma\Pi\Sigma\Pi$ circuits stems for two main reasons. Depth-4 is the first depth for which we do not have strong lower bounds for any field of characteristic different than 2 (over $\mathbb{F}_2$ lower bounds follow from the results of Razborov and Smolensky [112, 130]). The best known lower bounds, due to Raz [103], are smaller than n^2 (see Section 3.5). Another important reason is that, with respect to proving exponential lower bounds, $\Sigma\Pi\Sigma\Pi$ circuits are as interesting as general arithmetic circuits. Namely, an n-variate degree n polynomial can be computed by a sub-exponential arithmetic circuit if and only if it can be computed by a sub-exponential $\Sigma\Pi\Sigma\Pi$ circuit. This result, due to Agrawal and Vinay [5], is discussed in Section 2.4. Furthermore, derandomizing the polynomial identity testing problem for such circuits is almost equivalent to derandomizing it for general arithmetic circuits.

Thus, in order to understand the main open problems in arithmetic circuit complexity, one can focus on depth-4 circuits, instead of general arithmetic circuits, without loss of generality.

Another important model that we discuss in this monograph is *multilinear* circuits. A polynomial $f \in \mathbb{F}[X]$ is called *multilinear* if the individual degree of each variable in f is at most one. An arithmetic circuit Φ is called *multilinear* if every gate in Φ computes a multilinear polynomial. An arithmetic circuit Φ is called *syntactically multilinear* if for every product gate $v = v_1 \times v_2$ in Φ, the two sets X_{v_1} and X_{v_2} are disjoint (recall that X_u is the set of variables that occur in the circuit Φ_u). Syntactically multilinear circuits are clearly multilinear but the other direction is not true in general.

While being a very restricted model of computation, multilinear circuits and formulas form a very interesting class as for many multilinear polynomials, e.g., permanent and iterated matrix multiplication, the currently best arithmetic circuits computing them are multilinear. Indeed, computing a multilinear polynomial with a circuit that is not multilinear requires some "non-intuitive" cancellations of monomials. We do not however, that such "clever" cancellations occur, e.g., in small arithmetic circuits computing the determinant. In particular, we do not know today of polynomial size multilinear circuits computing the determinant. Being a natural model for computing multilinear polynomials, multilinear circuits are an interesting and an important class of circuits and we discuss the best results known for them.

In addition to bounded depth circuits and multilinear circuits we shall also study monotone circuits, noncommutative circuits, circuits with bounded coefficients and read-once formulas. We shall give the relevant definitions when we first discuss each of these classes.

1.4 Road Map

Here is a short overview of the content of this survey.

1.4.1 Structural Results

Due to its algebraic nature, the model of arithmetic circuits is more structured than the model of Boolean circuits. As such, we are able to prove results in the arithmetic world that in the Boolean case are

still open. In Section 2 we discuss some of the works on the structure of arithmetic circuits. These structural properties of arithmetic circuits are also used as starting points to proving lower bounds. We now discuss three examples of such structural results and their connection to lower bounds.

A striking result due to [143] is that in the arithmetic world $\mathsf{VP} = \mathsf{VNC}^2$ (see Theorem 1.3). This is in contrast to the Boolean world, where it is conjectured that $\mathsf{P} \neq \mathsf{NC}$. Subsequently, Agrawal and Vinay [5] proved a depth-4 version of this statement, showing that in order to prove exponential lower bounds on the size of general arithmetic circuits one just needs to prove exponential lower bounds on the size of depth-4 circuits.

A surprising result due to Baur and Strassen [16], that strongly relies on the underlying algebraic structure, states that computing a polynomial $f(x_1, \ldots, x_n)$ is essentially equivalent to simultaneously computing f and all of its n partial derivatives $\frac{\partial f}{\partial x_1}, \ldots, \frac{\partial f}{\partial x_n}$. Thus, proving a lower bound on the size of a circuit computing a set of polynomials is as difficult as proving a lower bound for a single polynomial. Alternatively, perhaps more optimistically, proving lower bounds should not be so difficult, as instead of proving a lower bound on the computation of a single polynomial we can try and prove a lower bound for circuits computing many polynomials. This principle actually turned out to be useful in at least two cases: showing that divisions are not necessary in computing polynomials by general arithmetic circuits [133] and proving lower bounds for multilinear circuits [107].

An interesting fact is that arithmetic circuits computing homogeneous polynomials can be transformed to be homogeneous, with only a small overhead. Recently, Raz [105] proved that for formulas, this transformation can be done at a smaller cost than what was known before. In particular, Raz showed that if one can prove (very) strong lower bounds on tensor rank then one obtains super-polynomial lower bounds on formula-size. Since tensor rank is no other than the size of the smallest set-multilinear depth-3 circuit computing the "tensor," Raz's result says that a very strong lower bound for the (very restricted) model of set-multilinear depth-3 circuits implies a lower bound for general formulas.

1.4.2 Lower Bounds for Arithmetic Circuits

One of the biggest challenges of algebraic complexity is proving lower bounds on circuit-size. Unlike the case of Boolean circuits, super-linear lower bounds on the size of general arithmetic circuits are known [16, 133]. Contrarily, no strong lower bounds are known for bounded depth arithmetic circuits. In particular, no super-quadratic lower bound is known even for circuits of depth 4, when $\text{char}(\mathbb{F}) \neq 2$.

In Section 3 we survey the known lower bounds and discuss some proofs in more detail. In particular, we explain Strassen's degree bound that gives a super-linear lower bound for general circuits [133] and Kalorkoti's quadratic lower bound on the size of general formulas [70]. We discuss the lower bounds for the size of bounded depth circuits [122, 103]. We then consider in detail depth-3 circuits, which is the "first" model for which proving lower bounds seems to be a difficult task.

In this section we also explain the following two-step "technique" for proving lower bound for arithmetic circuits. The first step is based on the fact that polynomials computed by small arithmetic circuits can be presented as a sum of a small number of products of "simpler" polynomials (this is one of the structural theorems that we prove). The second step is using the so-called partial derivative method to bound the complexity of such polynomials. By applying these two steps, we derive lower bounds for various classes of arithmetic circuits, such as monotone arithmetic circuits [68, 109, 121, 135] and multilinear formulas [102, 104, 108].

Finally, we present several approaches for proving lower bounds on circuit-size, and discuss the possibility of generalizing the *Natural Proofs* approach of Razborov and Rudich [111] to the algebraic setting.

1.4.3 Polynomial Identity Testing

Polynomial identity testing (PIT) is the problem of deciding whether a given arithmetic circuit computes the identically zero polynomial. Many randomized algorithms are known for this problem yet its deterministic complexity is still far from understood. Recently, it was discovered that this problem is strongly related to the question of proving lower bounds [69].

In Section 4 we first survey and sketch the proofs of randomized algorithms for PIT. We then discuss the relation between lower bounds and derandomization of PIT algorithms. One of the surprising results in this context is that a deterministic (black-box) polynomial-time algorithms for PIT of depth-4 arithmetic circuits implies a (quasi-polynomial time) derandomization of the problem for general arithmetic circuits.

We then present several deterministic algorithms for restricted classes of arithmetic circuits. We do not cover all known algorithms but rather present what we view as the most notable techniques in the area. Specifically, we give one of the many algorithms for sparse polynomials [86]. We show a polynomial-time algorithm for PIT of noncommutative formulas that is based on the partial derivative method [106]. We then describe two algorithms for depth-3 circuits with a bounded top fan-in. The first is the local ring algorithm of [81] that works in the non-black-box model (which we refer to as the *white-box model*) and the second is the algorithm of [43, 76] that is based on the *rank* method (with the strengthening of [80, 117, 118]). After that, we present two results for depth-4 circuits. The first is by [116] that gave a polynomial time PIT for the so-called *diagonal* circuits, based on the ideas of [106]. The second result is by [75] that gave a PIT algorithm for depth-4 multilinear circuits with bounded top fan-in, based on ideas from [76] and [127]. Finally, we present the algorithm of [126, 127] for identity testing of sums of read-once formulas that strengthen some of the results for depth-3 circuits and that influenced [75].

1.4.4 Reconstruction of Arithmetic Circuits

In Section 5 we consider the problem of reconstructing arithmetic circuits, which is the algebraic analog of the learning problem of Boolean circuits. This problem is clearly related to PIT, as an identity testing algorithm for a circuit class gives a way of distinguishing between different circuits from that class and can thus be helpful in designing a learning algorithm.

We discuss the similarities and differences between the reconstruction problem and analogous problems in the Boolean world. We then

give some hardness results on the reconstruction problem. After that we discuss several known reconstruction algorithms. First, we explain how to reconstruct sparse polynomials. Then we discuss the multiplicity automata technique of [17] and its extension for arithmetic circuits [85]. Basically, this technique can be thought of as learning via partial derivatives. At the end, we move to depth-3 circuits with a bounded top fan-in and sketch the algorithms of [77, 125] that are based on ideas from the identity testing algorithm of [43, 77].

1.5 Additional Reading

We decided to focus this survey on recent results in arithmetic circuit complexity, mainly on lower bounds and identity testing algorithms, and so many beautiful results in algebraic complexity, both new and old, were left out. We now mention some of the topics that are not discussed in this monograph and give references to relevant papers. Most of these topics are discussed in the comprehensive book [30] and the (unfortunately, still relevant) survey of Strassen [134].

One important area that we do not cover is algorithms for algebraic problems, an area that has been yielding many beautiful works. A partial list of algorithms include Cooley and Tukey's FFT algorithm [38], fast matrix multiplication [39] (and the new algorithmic approach of [36, 37]), efficient polynomial factorization (see the surveys [72, 146] and the recent [84]) and the deterministic primality testing algorithm of [4].

Another topic that we do not really discuss is that of linear and bilinear complexity. Here, one is interested in the complexity of computing linear transformations and bilinear forms using linear or bilinear circuits, respectively. The complexity of computing univariate polynomials is another topic that we decided not to include. The interested reader is referred to the aforementioned book [30] and survey [134].

Several other models of algebraic computations also received a lot of attention. Among them we mention the Blum–Shub–Smale model of computing over the reals and algebraic decision trees, more information can be found in [9, 21, 30].

References

[1] S. Aaronson, "Arithmetic natural proofs theory is sought," http://scottaaronson.com/blog/?p=336, 2008.

[2] M. Agrawal, "Proving lower bounds via pseudo-random generators," in *Proceedings of the 25th FSTTCS*, vol. 3821 of *LNCS*, pp. 92–105, 2005.

[3] M. Agrawal and S. Biswas, "Primality and identity testing via Chinese remaindering," *Journal of the ACM*, vol. 50, pp. 429–443, 2003.

[4] M. Agrawal, N. Kayal, and N. Saxena, "Primes is in P," *Annals of Mathematics*, vol. 160, pp. 781–793, 2004.

[5] M. Agrawal and V. Vinay, "Arithmetic circuits: A chasm at depth four," in *Proceedings of the 49th Annual FOCS*, pp. 67–75, 2008.

[6] N. Alon, "Combinatorial nullstellensatz," *Combinatorics, Probability and Computing*, vol. 8, pp. 7–29, 1999.

[7] S. A. Amitsur and J. Levitzki, "Minimal identities for algebras," *Proceedings of the American Mathematical Society*, vol. 1, pp. 449–463, 1950.

[8] M. Anderson, D. van Melkebeek, and I. Volkovich, "Derandomizing polynomial identity testing for multilinear constant-read formulae," *Electronic Colloquium on Computational Complexity (ECCC)*, vol. 135, 2010. http://www.eccc.uni-trier.de/report/2010/189/.

[9] S. Arora and B. Barak, *Computational Complexity: A Modern Approach*. Cambridge University Press, 2009.

[10] S. Arora, C. Lund, R. Motwani, M. Sudan, and M. Szegedy, "Proof verification and the hardness of approximation problems," *Journal of the ACM*, vol. 45, pp. 501–555, 1998.

[11] S. Arora and S. Safra, "Probabilistic checking of proofs: A new characterization of NP," *Journal of the ACM*, vol. 45, pp. 70–122, 1998.

[12] V. Arvind and P. Mukhopadhyay, "The monomial ideal membership problem and polynomial identity testing," in *Proceedings of the 18th ISAAC*, pp. 800–811, 2007.

[13] V. Arvind and P. Mukhopadhyay, "Derandomizing the isolation lemma and lower bounds for circuit size," in *APPROX-RANDOM*, pp. 276–289, 2008.

[14] V. Arvind, P. Mukhopadhyay, and S. Srinivasan, "New results on noncommutative and commutative polynomial identity testing," in *Proceedings of the 23rd Annual CCC*, pp. 268–279, 2008.

[15] L. Babai, L. Fortnow, and C. Lund, "Non-deterministic exponential time has two-prover interactive protocols," *Computational Complexity*, vol. 1, pp. 3–40, 1991.

[16] W. Baur and V. Strassen, "The complexity of partial derivatives," *Theoretical Compter Science*, vol. 22, pp. 317–330, 1983.

[17] A. Beimel, F. Bergadano, N. H. Bshouty, E. Kushilevitz, and S. Varricchio, "Learning functions represented as multiplicity automata," *Journal of the ACM*, vol. 47, pp. 506–530, 2000.

[18] M. Ben-Or and P. Tiwari, "A deterministic algorithm for sparse multivariate polynominal interpolation," in *Proceedings of the 20th Annual STOC*, pp. 301–309, 1988.

[19] M. Bläser, "A $5/2n^2$-lower bound for the rank of $n \times n$-matrix multiplication over arbitrary fields," in *Proceedings of the 40th Annual FOCS*, pp. 45–50, 1999.

[20] M. Bläser, M. Hardt, R. J. Lipton, and N. K. Vishnoi, "Deterministically testing sparse polynomial identities of unbounded degree," *Information Processing Letters*, vol. 109, pp. 187–192, 2009.

[21] L. Blum, F. Cucker, M. Shub, and S. Smale, *Complexity and Real Computation*. Springer, 1997.

[22] M. Blum, A. K. Chandra, and M. N. Wegman, "Equivalence of free boolean graphs can be tested in polynomial time," *Information Processing Letters*, vol. 10, pp. 80–82, 1980.

[23] A. Bogdanov and H. Wee, "More on noncommutative polynomial identity testing," in *Proceedings of the 20th Annual IEEE Conference on Computational Complexity*, pp. 92–99, 2005.

[24] A. Borodin, J. von zur Gathen, and J. E. Hopcroft, "Fast parallel matrix and GCD computations," *Information and Control*, vol. 52, pp. 241–256, 1982.

[25] M. R. Brown and D. P. Dobkin, "An improved lower bound on polynomial multiplication," *IEEE Transactions on Computers*, vol. 29, pp. 337–340, 1980.

[26] D. Bshouty and N. H. Bshouty, "On interpolating arithmetic read-once formulas with exponentiation," *Journal of Computer and System Sciences*, vol. 56, pp. 112–124, 1998.

[27] N. H. Bshouty and R. Cleve, "Interpolating arithmetic read-once formulas in parallel," *SIAM Journal on Computing*, vol. 27, pp. 401–413, 1998.

[28] N. H. Bshouty, T. R. Hancock, and L. Hellerstein, "Learning arithmetic read-once formulas," *SIAM Journal on Computing*, vol. 24, pp. 706–735, 1995.

[29] P. Bürgisser, "On the structure of valiant's complexity classes," *Discrete Mathematics & Theoretical Computer Science*, vol. 3, pp. 73–94, 1999.

[30] P. Bürgisser, M. Clausen, and M. A. Shokrollahi, *Algebraic Complexity Theory*. Springer, 1997.
[31] J. Cai, X. Chen, and D. Li, "A quadratic lower bound for the permanent and determinant problem over any characteristic != 2," in *Proceedings of the 40th Annual STOC*, pp. 491–498, 2008.
[32] S. Chari, P. Rohatgi, and A. Srinivasan, "Randomness-optimal unique element isolation with applications to perfect matching and related problems," *SIAM Journal on Computing*, vol. 24, pp. 1036–1050, 1995.
[33] B. Chazelle, "A spectral approach to lower bounds with applications to geometric searching," *SIAM Journal on Computing*, vol. 27, pp. 545–556, 1998.
[34] Z. Chen and M. Kao, "Reducing randomness via irrational numbers," *SIAM Journal on Computing*, vol. 29, pp. 1247–1256, 2000.
[35] S. Chien and A. Sinclair, "Algebras with polynomial identities and computing the determinant," *SIAM Journal on Computing*, vol. 37, pp. 252–266, 2007.
[36] H. Cohn, R. D. Kleinberg, B. Szegedy, and C. Umans, "Group-theoretic algorithms for matrix multiplication," in *Proceedings of the 46th Annual FOCS*, pp. 379–388, 2005.
[37] H. Cohn and C. Umans, "A group-theoretic approach to fast matrix multiplication," in *Proceedings of the 44th Annual FOCS*, pp. 438–449, 2003.
[38] J. W. Cooley and J. W. Tukey, "An algorithm for the machine calculation of complex fourier series," *Mathematics of Computation*, vol. 19, pp. 297–301, 1965.
[39] D. Coppersmith and S. Winograd, "Matrix multiplication via arithmetic progression," *Journal of Symbolic Computation*, vol. 9, pp. 251–280, 1990.
[40] L. Csanky, "Fast parallel matrix inversion algorithms," *SIAM Journal on Computing*, vol. 5, pp. 618–623, 1976.
[41] R. A. DeMillo and R. J. Lipton, "A probabilistic remark on algebraic program testing," *Information Processing Letters*, vol. 7, pp. 193–195, 1978.
[42] Z. Dvir, "On matrix rigidity and locally self-correctable codes," in *Proceedings of the 25th Annual CCC*, pp. 291–298, 2010.
[43] Z. Dvir and A. Shpilka, "Locally decodable codes with 2 queries and polynomial identity testing for depth 3 circuits," *SIAM Journal on Computing*, vol. 36, pp. 1404–1434, 2006.
[44] Z. Dvir, A. Shpilka, and A. Yehudayoff, "Hardness-randomness tradeoffs for bounded depth arithmetic circuits," *SIAM Journal on Computing*, vol. 39, pp. 1279–1293, 2009.
[45] M. Edelstein and L. M. Kelly, "Bisecants of finite collections of sets in linear spaces," *Canadanian Journal of Mathematics*, vol. 18, pp. 375–280, 1966.
[46] L. Fortnow and A. R. Klivans, "Efficient learning algorithms yield circuit lower bounds," *Journal of Computer System Science*, vol. 75, pp. 27–36, 2009.
[47] A. Gabizon and R. Raz, "Deterministic extractors for affine sources over large fields," *Combinatorica*, vol. 28, pp. 415–440, 2008.
[48] O. Goldreich, S. Goldwasser, and S. Micali, "How to construct random functions," *Journal of the ACM*, vol. 33, pp. 792–807, 1986.
[49] D. Grigoriev and M. Karpinski, "The matching problem for bipartite graphs with polynomially bounded permanents is in NC (extended abstract)," in *Proceedings of the 28th Annual FOCS*, pp. 166–172, 1987.

[50] D. Grigoriev and M. Karpinski, "An exponential lower bound for depth 3 arithmetic circuits," in *Proceedings of the 30th Annual STOC*, pp. 577–582, 1998.

[51] D. Grigoriev, M. Karpinski, and M. F. Singer, "Fast parallel algorithms for sparse multivariate polynomial interpolation over finite fields," *SIAM Journal on Computing*, vol. 19, pp. 1059–1063, 1990.

[52] D. Grigoriev and A. A. Razborov, "Exponential complexity lower bounds for depth 3 arithmetic circuits in algebras of functions over finite fields," *Applicable Algebra in Engineering, Communication and Computing*, vol. 10, pp. 465–487, 2000.

[53] J. Håstad, "Almost optimal lower bounds for small depth circuits," in *Proceedings of the 18th Annual STOC*, pp. 6–20, 1986.

[54] J. Håstad, "Tensor rank is np-complete," *Journal of Algorithms*, vol. 11, pp. 644–654, 1990.

[55] T. R. Hancock and L. Hellerstein, "Learning read-once formulas over fields and extended bases," in *Proceedings of the 4th Annual COLT*, pp. 326–336, 1991.

[56] J. Heintz and C. P. Schnorr, "Testing polynomials which are easy to compute (extended abstract)," in *Proceedings of the 12th annual STOC*, pp. 262–272, 1980.

[57] J. Heintz and M. Sieveking, "Lower bounds for polynomials with algebraic coefficients," *Theoretical Computer Science*, vol. 11, pp. 321–330, 1980.

[58] S. Hoory, N. Linial, and A. Wigderson, "Expander graphs and their applications," *Bulletin of the American Mathematical Society*, vol. 43, pp. 439–561, 2006.

[59] J. E. Hopcroft, R. Motwani, and J. D. Ullman, *Introduction to Automata Theory, Languages, and Computation.* Pearson Education, 2nd ed., 2000.

[60] P. Hrubeš, A. Wigderson, and A. Yehudayoff, "Non-commutative circuits and the sum-of-squares problem," in *Proceedings of the 42nd Annual ACM Symposium on Theory of Computing (STOC)*, pp. 667–676, 2010.

[61] P. Hrubeš, A. Wigderson, and A. Yehudayoff, "Relationless completeness and separations," in *Proceedings of the 25th Conference on Computational Complexity*, pp. 280–290, 2010.

[62] P. Hrubeš and A. Yehudayoff, "Arithmetic complexity in algebraic extensions," *Manuscript*, 2009.

[63] P. Hrubeš and A. Yehudayoff, "Homogeneous formulas and symmetric polynomials," *CoRR*, abs/0907.2621, 2009.

[64] P. Hrubeš and A. Yehudayoff, "Monotone separations for constant degree polynomials," *Information Processing Letters*, vol. 110, pp. 1–3, 2009.

[65] R. Impagliazzo, V. Kabanets, and A. Wigderson, "In search of an easy witness: Exponential time vs. probabilistic polynomial time," *Journal of Computer and System Sciences*, vol. 65, pp. 672–694, 2002.

[66] R. Impagliazzo and A. Wigderson, "P=BPP unless E has subexponential circuits: derandomizing the XOR lemma," in *Proceedings of the 29th STOC*, pp. 220–229, 1997.

[67] M. Jansen, Y. Qiao, and J. Sarma, "Deterministic identity testing of read-once algebraic branching programs," *CoRR*, abs/0912.2565, 2009.
[68] M. Jerrum and M. Snir, "Some exact complexity results for straight-line computations over semi-rings," Technical Report CRS-58–80, University of Edinburgh, 1980.
[69] V. Kabanets and R. Impagliazzo, "Derandomizing polynomial identity tests means proving circuit lower bounds," *Computational Complexity*, vol. 13, pp. 1–46, 2004.
[70] K. Kalorkoti, "A lower bound for the formula size of rational functions," *SIAM Journal of Computing*, vol. 14, pp. 678–687, 1985.
[71] E. Kaltofen, "Factorization of polynomials given by straight-line programs," in *Randomness in Computation,* vol. 5 of *Advances in Computing Research*, (S. Micali, ed.), pp. 375–412, 1989.
[72] E. Kaltofen, "Polynomial factorization: A success story," in *ISSAC*, pp. 3–4, 2003.
[73] E. Kaltofen and B. M. Trager, "Computing with polynomials given by black boxes for their evaluations: Greatest common divisors, factorization, separation of numerators and denominators," *Journal of Symbolic Computation*, vol. 9, pp. 301–320, 1990.
[74] M. Kaminski, "A lower bound on the complexity of polynomial multiplication over finite fields," *SIAM Journal on Computing*, vol. 34, pp. 960–992, 2005.
[75] Z. S. Karnin, P. Mukhopadhyay, A. Shpilka, and I. Volkovich, "Deterministic identity testing of depth 4 multilinear circuits with bounded top fan-in," in *Proceedings of the 42nd Annual STOC*, pp. 649–658, 2010.
[76] Z. S. Karnin and A. Shpilka, "Deterministic black box polynomial identity testing of depth-3 arithmetic circuits with bounded top fan-in," in *Proceedings of the 23rd Annual CCC*, pp. 280–291, 2008.
[77] Z. S. Karnin and A. Shpilka, "Reconstruction of generalized depth-3 arithmetic circuits with bounded top fan-in," in *Proceedings of the 24th Annual CCC*, pp. 274–285, 2009.
[78] R. Karp, E. Upfal, and A. Wigderson, "Constructing a perfect matching is in random NC," *Combinatorica*, vol. 6, pp. 35–48, 1, 1986.
[79] N. Kayal, "Derandomizing some number-theoretic and algebraic algorithms," PhD thesis, Indian Institute of Technology, Kanpur, India, 2007.
[80] N. Kayal and S. Saraf, "Blackbox polynomial identity testing for depth 3 circuits," in *Proceedings of the 50th Annual FOCS*, pp. 198–207, 2009.
[81] N. Kayal and N. Saxena, "Polynomial identity testing for depth 3 circuits," *Computational Complexity*, vol. 16, pp. 115–138, 2007.
[82] M. J. Kearns and L. G. Valiant, "Cryptographic limitations on learning boolean formulae and finite automata," *Journal of the ACM*, vol. 41, pp. 67–95, 1994.
[83] M. J. Kearns and U. V. Vazirani, *An Introduction to Computational Learning Theory*. Cambridge, MA, USA: MIT Press, 1994.
[84] K. S. Kedlaya and C. Umans, "Fast modular composition in any characteristic," in *Proceedings of the 49th Annual Symposium on Foundations of Computer Science (FOCS)*, pp. 146–155, 2008.

[85] A. Klivans and A. Shpilka, "Learning restricted models of arithmetic circuits," *Theory of Computing*, vol. 2, pp. 185–206, 2006.
[86] A. Klivans and D. Spielman, "Randomness efficient identity testing of multivariate polynomials," in *Proceedings of the 33rd Annual STOC*, pp. 216–223, 2001.
[87] A. R. Klivans and A. A. Sherstov, "Cryptographic hardness for learning intersections of halfspaces," *Journal of Computer and System Sciences*, vol. 75, pp. 2–12, 2009.
[88] P. Koiran, "Arithmetic circuits: The chasm at depth four gets wider," *CoRR*, abs/1006.4700, 2010.
[89] D. Lewin and S. Vadhan, "Checking polynomial identities over any field: Towards a derandomization?," in *Proceedings of the 30th Annual STOC*, pp. 428–437, 1998.
[90] L. Lovasz, "On determinants, matchings, and random algorithms," in *Fundamentals of Computing Theory*, (L. Budach, ed.), Akademia-Verlag, 1979.
[91] C. Lund, L. Fortnow, H. Karloff, and N. Nisan, "Algebraic methods for interactive proof systems," *Journal of the ACM*, vol. 39, pp. 859–868, 1992.
[92] T. Mignon and N. Ressayre, "A quadratic bound for the determinant and permanent problem," *International Mathematics Research Notices*, vol. 79, pp. 4241–4253, 2004.
[93] P. Morandi, *Graduate Texts in Mathematics 167: Field and Galois Theory*. Springer-Verlag, New York, 1996.
[94] J. Morgenstern, "Note on a lower bound on the linear complexity of the fast Fourier transform," *Journal of the ACM*, vol. 20, pp. 305–306, 1973.
[95] K. Mulmuley and M. A. Sohoni, "Geometric complexity theory i: An approach to the P vs. NP and related problems," *SIAM Journal on Computing*, vol. 31, pp. 496–526, 2001.
[96] K. Mulmuley and M. A. Sohoni, "Geometric complexity theory ii: Towards explicit obstructions for embeddings among class varieties," *SIAM Journal on Computing*, vol. 38, pp. 1175–1206, 2008.
[97] K. Mulmuley, U. Vazirani, and V. Vazirani, "Matching is as easy as matrix inversion," *Combinatorica*, vol. 7, pp. 105–113, 1987.
[98] N. Nisan, "Lower bounds for non-commutative computation," in *Proceedings of the 23rd Annual STOC*, pp. 410–418, 1991.
[99] N. Nisan and A. Wigderson, "Hardness vs. randomness," *Journal of Computer System Sciences*, vol. 49, pp. 149–167, 1994.
[100] N. Nisan and A. Wigderson, "Lower bound on arithmetic circuits via partial derivatives," *Computational Complexity*, vol. 6, pp. 217–234, 1996.
[101] R. Raz, "On the complexity of matrix product," *SIAM Journal on Computing*, vol. 32, pp. 1356–1369, 2003.
[102] R. Raz, "Separation of multilinear circuit and formula size," *Theory of Computing*, vol. 2, pp. 121–135, 2006.
[103] R. Raz, "Elusive functions and lower bounds for arithmetic circuits," in *Proceedings of the 40th Annual ACM Symposium on Theory of Computing (STOC)*, pp. 711–720, 2008.

[104] R. Raz, "Multi-linear formulas for permanent and determinant are of super-polynomial size," *Journal of the ACM*, vol. 56, 2009.
[105] R. Raz, "Tensor-rank and lower bounds for arithmetic formulas," in *Proceedings of the 42nd Annual STOC*, pp. 659–666, 2010.
[106] R. Raz and A. Shpilka, "Deterministic polynomial identity testing in non commutative models," *Computational Complexity*, vol. 14, pp. 1–19, 2005.
[107] R. Raz, A. Shpilka, and A. Yehudayoff, "A lower bound for the size of syntactically multilinear arithmetic circuits," *SIAM Journal on Computing*, vol. 38, pp. 1624–1647, 2008.
[108] R. Raz and A. Yehudayoff, "Balancing syntactically multilinear arithmetic circuits," *Computational Complexity*, vol. 17, pp. 515–535, 2008.
[109] R. Raz and A. Yehudayoff, "Multilinear formulas, maximal-partition discrepancy and mixed-sources extractors," in *Proceedings of the 49th Annual FOCS*, pp. 273–282, 2008.
[110] R. Raz and A. Yehudayoff, "Lower bounds and separations for constant depth multilinear circuits," *Computational Complexity*, vol. 18, pp. 171–207, 2009.
[111] A. A. Razboeov and S. Rudich, "Natural proofs," *Journal of Computer and System Sciences*, vol. 55, pp. 24–35, 1997.
[112] A. A. Razborov, "Lower bounds for the size of circuits with bounded depth with basis $\{\wedge, \oplus\}$," *Matematicheskie Zametki*, pp. 598–607, 1987. in Russian.
[113] O. Regev, "On lattices, learning with errors, random linear codes, and cryptography," *Journal of the ACM*, vol. 56, 2009.
[114] H. J. Ryser, *Combinatorial Mathematics*, vol. 14. Carus Mathematical Monographs, 1963.
[115] S. Saraf and I. Volkovich, "Black-box identity testing of depth-4 multilinear circuits," *Manuscript*, 2010.
[116] N. Saxena, "Diagonal circuit identity testing and lower bounds," in *ICALP (1)*, pp. 60–71, 2008.
[117] N. Saxena and C. Seshadhri, "An almost optimal rank bound for depth-3 identities," in *Proceedings of the 24th Annual CCC*, pp. 137–148, 2009.
[118] N. Saxena and C. Seshadhri, "From Sylvester-Gallai configurations to rank bounds: Improved black-box identity test for deph-3 circuits," in *Proceedings of the 51st Annual FOCS*, pp. 21–30, 2010.
[119] J. T. Schwartz, "Fast probabilistic algorithms for verification of polynomial identities," *Journal of the ACM*, vol. 27, pp. 701–717, 1980.
[120] A. Shamir, "IP = PSPACE," *Journal of the ACM*, vol. 39, pp. 869–877, 1992.
[121] E. Shamir and M. Snir, "Lower bounds on the number of multiplications and the number of additions in monotone computations," Technical Report RC-6757, IBM, 1977.
[122] V. Shoup and R. Smolensky, "Lower bounds for polynomial evaluation and interpolation problems," in *SFCS '91: Proceedings of the 32nd Annual Symposium on Foundations of Computer Science*, pp. 378–383, Washington, DC, USA: IEEE Computer Society, 1991.
[123] A. Shpilka, "Affine projections of symmetric polynomials," *Journal of Computer and System Sciences*, vol. 65, pp. 639–659, 2002.

[124] A. Shpilka, "Lower bounds for matrix product," *SIAM Journal on Computing*, vol. 32, pp. 1185–1200, 2003.
[125] A. Shpilka, "Interpolation of depth-3 arithmetic circuits with two multiplication gates," *SIAM Journal on Computing*, vol. 38, pp. 2130–2161, 2009.
[126] A. Shpilka and I. Volkovich, "Read-once polynomial identity testing," in *Proceedings of the 40th Annual STOC*, pp. 507–516, 2008.
[127] A. Shpilka and I. Volkovich, "Improved polynomial identity testing for read-once formulas," in *APPROX-RANDOM*, pp. 700–713, 2009.
[128] A. Shpilka and I. Volkovich, "On the relation between polynomial identity testing and finding variable disjoint factors," in *ICALP (1)*, pp. 408–419, 2010.
[129] A. Shpilka and A. Wigderson, "Depth-3 arithmetic circuits over fields of characteristic zero," *Computational Complexity*, vol. 10, pp. 1–27, 2001.
[130] R. Smolensky, "Algebraic methods in the theory of lower bounds for Boolean circuit complexity," in *Proceedings of the 19th Annual STOC*, pp. 77–82, 1987.
[131] V. Strassen, "Gaussian elimination is not optimal," *Numerische Mathematik*, vol. 13, pp. 354–356, 1969.
[132] V. Strassen, "Die berechnungskomplexiät von elementarsymmetrischen funktionen und von interpolationskoeffizienten," *Numerische Mathematik*, vol. 20, pp. 238–251, 1973.
[133] V. Strassen, "Vermeidung von divisionen," *The Journal für die Reine und Angewandte Mathematik*, vol. 264, pp. 182–202, 1973.
[134] V. Strassen, "Algebraic complexity theory," in *Handbook of Theoretical Computer Science*, vol. A: *Algorithms and Complexity (A)*, pp. 633–672, Elsevier and MIT Press, 1990.
[135] P. Tiwari and M. Tompa, "A direct version of Shamir and Snir's lower bounds on monotone circuit depth," *Information Processing Letters*, vol. 49, pp. 243–248, 1994.
[136] S. Toda, "PP is as hard as the polynomial time hierarchy," *SIAM Journal on Computing*, vol. 20, pp. 865–877, 1991.
[137] L. G. Valiant, "Graph-theoretic arguments in low-level complexity," in *Lecture notes in Computer Science*, vol. 53, pp. 162–176, Springer, 1977.
[138] L. G. Valiant, "Completeness classes in algebra," in *Proceedings of the 11th Annual STOC*, pp. 249–261, 1979.
[139] L. G. Valiant, "The complexity of computing the permanent," *Theoretical Computer Science*, vol. 8, pp. 189–201, 1979.
[140] L. G. Valiant, "Negation can be exponentially powerful," *Theoretical Computer Science*, vol. 12, pp. 303–314, November 1980.
[141] L. G. Valiant, "Reducibility by algebraic projections," *L'Enseignement Mathematique*, vol. 28, pp. 253–268, 1982.
[142] L. G. Valiant, "A theory of the learnable," *Communications of the ACM*, vol. 27, pp. 1134–1142, 1984.
[143] L. G. Valiant, S. Skyum, S. Berkowitz, and C. Rackoff, "Fast parallel computation of polynomials using few processors," *SIAM Journal on Computing*, vol. 12, pp. 641–644, November 1983.

[144] E. Viola, "The sum of small-bias generators fools polynomials of degree," *Computational Complexity*, vol. 18, pp. 209–217, 2009.
[145] J. von zur Gathen, "Feasible arithmetic computations: Valiant's hypothesis," *Journal of Symbolic Computation*, vol. 4, pp. 137–172, 1987.
[146] J. von zur Gathen, "Who was who in polynomial factorization," in *ISSAC*, p. 2, 2006.
[147] J. von zur Gathen and J. Gerhard, *Modern Computer Algebra*. Cambridge University Press, 1999.
[148] R. Zippel, "Probabilistic algorithms for sparse polynomials," in *Symbolic and Algebraic Computation*, pp. 216–226, 1979.