

# three Arithmetic circuits: A chasm at depth four

Ankit Gupta\*, Prithish Kamath†, Neeraj Kayal‡, Ramprasad Saptharishi§

\*Microsoft Research India  
ankitgupta.iitkanpur@gmail.com  
†Microsoft Research India  
prithish.kamath@gmail.com  
‡Microsoft Research India  
neeraka@microsoft.com  
§Chennai Mathematical Institute  
ramprasad@cmi.ac.in

**Abstract**—We show that, over  $\mathbb{Q}$ , if an  $n$ -variate polynomial of degree  $d = n^{O(1)}$  is computable by an arithmetic circuit of size  $s$  (respectively by an arithmetic branching program of size  $s$ ) then it can also be computed by a depth three circuit (i.e. a  $\Sigma\Pi\Sigma$ -circuit) of size  $\exp(O(\sqrt{d} \log n \log d \log s))$  (respectively of size  $\exp(O(\sqrt{d} \log n \log s))$ ). In particular this yields a  $\Sigma\Pi\Sigma$  circuit of size  $\exp(O(\sqrt{d} \cdot \log d))$  computing the  $d \times d$  determinant  $\text{Det}_d$ . It also means that if we can prove a lower bound of  $\exp(\omega(\sqrt{d} \cdot \log d))$  on the size of any  $\Sigma\Pi\Sigma$ -circuit computing the  $d \times d$  permanent  $\text{Perm}_d$  then we get superpolynomial lower bounds for the size of any arithmetic branching program computing  $\text{Perm}_d$ . We then give some further results pertaining to derandomizing polynomial identity testing and circuit lower bounds.

The  $\Sigma\Pi\Sigma$  circuits that we construct have the property that (some of) the intermediate polynomials have degree much higher than  $d$ . Indeed such a counterintuitive construction is unavoidable - it is known that in any  $\Sigma\Pi\Sigma$  circuit  $C$  computing either  $\text{Det}_d$  or  $\text{Perm}_d$ , if every multiplication gate has fanin at most  $d$  (or any constant multiple thereof) then  $C$  must have size at least  $\exp(\Omega(d))$ .

## I. INTRODUCTION

**Arithmetic Circuits.** The most natural way to compute a polynomial function  $f(x_1, x_2, \dots, x_n)$  starting from its inputs  $x_1, x_2, \dots, x_n$  is via a sequence of basic arithmetic operations consisting of addition, multiplication and subtraction. Such a computation can be visualized as an arithmetic circuit. We typically allow the incoming edges to a  $+$  gate to be labelled with constants from the underlying field  $\mathbb{F}$  so that a  $+$  gate can in fact

compute an arbitrary  $\mathbb{F}$ -linear combination of its inputs. Two relevant complexity measures for an arithmetic circuit are its size (the total number of arithmetic operations involved) and its depth (the maximum length of a path from an input to the output). The goal here is to understand the optimal complexity (in terms of size and depth) of computing a given polynomial family. Two closely related families of polynomials, the determinant and the permanent defined as

$$\text{Det}_d = \sum_{\sigma \in S_d} \text{sign}(\sigma) \cdot \prod_{i=1}^d x_{i, \sigma(i)}$$

$$\text{Perm}_d = \sum_{\sigma \in S_d} \prod_{i=1}^d x_{i, \sigma(i)}$$

are of particular interest as they feature in many different areas of mathematics and computer science. Although these two polynomials look very similar, they have strikingly different complexities. The determinant and permanent are in fact complete problems for the classes VP and VNP respectively, which are algebraic analogues of P and NP [Val79]. A grand challenge in this direction is to show that  $\text{Perm}_d$  cannot be computed by arithmetic circuits of polynomial size.

**Depth Reduction.** Circuits with low depth correspond to computations which are highly parallelizable and therefore it is natural to try to minimize the depth of a circuit while allowing the size to increase somewhat. Csanky [Csa76] showed that  $\text{Det}_d$  can be computed by circuits of size  $d^{O(1)}$  having only  $(\log d)^{O(1)}$  depth. Subsequently Valiant, Skyum,

Berkowitz and Rackoff [VSB83] discovered a remarkable generalization. They showed that if a polynomial  $f$  of degree  $d$  can be computed by a circuit of size  $s$  then it can in fact be computed by a circuit of depth  $O(\log d \cdot \log s)$  and size  $s^{O(1)}$ . Pushing this line of investigation of size-depth tradeoffs further, recent work has considered reduction to circuits of even smaller depth while allowing the addition and multiplication gates to have arbitrary (unbounded) fanin. In this direction, the work of Agrawal and Vinay [AV08] and a subsequent strengthening by Koiran [Koi12] showed that if  $f$  has circuits of size  $s = d^{O(1)}$  then  $f$  can in fact be computed by depth four circuits of size  $2^{O(\sqrt{d} \cdot \log^2 d)}$ .<sup>1</sup> Despite the large blowup, the reason that such reductions to constant depth circuits are interesting is that these reductions ‘explain’ the lack of progress towards lower bounds even for constant-depth arithmetic circuits.<sup>2</sup> Viewed optimistically, such a reduction entails that one *merely* needs to prove a (good enough) lower bound for depth four circuits in order to prove lower bounds for arbitrary circuits. Indeed, motivated by this, we recently proved lower bounds for depth four circuits which comes very close to the threshold required<sup>3</sup>. In a similar spirit Raz [Raz10] showed that close-to-optimal lower bounds for small degree tensors<sup>4</sup> imply superpolynomial lower bounds on formula size<sup>5</sup>.

**Depth Three Circuits.** Being the shallowest non-trivial subclass of arithmetic circuits, depth three arithmetic circuits, also denoted as  $\Sigma\Pi\Sigma$  circuits, have been intensely investigated. Such a circuit  $C$

<sup>1</sup>A simple but nonconstructive counting argument shows that over any field  $\mathbb{F}$ , most  $n$ -variate polynomials of degree  $d$  require circuits of size  $\Omega\left(\sqrt{\binom{n+d}{d}}\right)$

<sup>2</sup>Note that in contrast to arithmetic circuits, exponential lower bounds are known for constant depth boolean circuits with  $\wedge, \vee$  gates of unbounded fanin.

<sup>3</sup>Specifically, [GKKS13] shows a lower bound of  $\exp(\Omega(\sqrt{d}))$  on the size of  $\Sigma\Pi^{[O(\sqrt{d})]}\Sigma\Pi^{[\sqrt{d}]}$  computing  $\text{Perm}_d$ . In comparison, Koiran showed that a lower bound of  $\exp(\omega(\sqrt{d} \log^2 d))$  on the size of  $\Sigma\Pi^{[O(\sqrt{d})]}\Sigma\Pi^{[\sqrt{d}]}$  computing  $\text{Perm}_d$  entails superpolynomial lower bounds for general circuits computing  $\text{Perm}_d$ .

<sup>4</sup>A subclass of  $\Sigma\Pi\Sigma$  also known as set-multilinear  $\Sigma\Pi\Sigma$  circuits

<sup>5</sup>Specifically, Raz showed that for  $d = d(n) \leq \frac{\log n}{\log \log n}$ , any explicit example of a tensor  $A : [n]^d \mapsto \mathbb{C}$  with tensor rank  $\geq n^{d(1-o(1))}$  implies an explicit superpolynomial lower bound for the size of general arithmetic formulas. Because of the restriction on the degree  $d$ , Raz’s result does not seem to be applicable to the permanent

computes a polynomial in the following manner:

$$C(\mathbf{x}) = \sum_{i=1}^s \prod_{j=1}^{d_i} \ell_{ij}(\mathbf{x}), \quad (1)$$

where each  $\ell_{ij}(\mathbf{x})$  is an affine form over the input variables.  $\Sigma\Pi\Sigma$  circuits (more specifically tensors) arise naturally in the investigation of the complexity of polynomial multiplication and matrix multiplication<sup>6</sup>. Moreover, the optimal formula/circuit for some well known families of polynomials are in fact depth three circuits. In particular, the best known circuit for computing the permanent  $\text{Perm}_d$  is known as Ryser’s formula [Rys63] which is a (homogeneous<sup>7</sup>) depth three circuit of size  $O(d^2 \cdot 2^d)$ <sup>8</sup>. For more on  $\Sigma\Pi\Sigma$  circuits, we refer the reader to the thesis of Shpilka [Shp01] and the references therein.

**Circuit Lower bounds.** While there has been significant progress in upper bounds, progress in proving lower bounds for arithmetic circuits has been much slower. This is generally considered to be one of the most challenging problems in computer science. The difficulty of the problem has led researchers to focus on natural subclasses of arithmetic circuits. We refer the interested reader to the recent surveys by Shpilka and Yehudayoff [SY10] and Chen, Kayal and Wigderson [CKW11] for more on lower bounds for various subclasses of arithmetic circuits. Bounded depth circuits being one such natural subclass has received a lot of attention. The simplest nontrivial such subclass is that of  $\Sigma\Pi\Sigma$  circuits. Nisan and Wigderson [NW97]

<sup>6</sup>For example it can be shown that the product of two  $n \times n$  matrices can be computed with  $\tilde{O}(n^\omega)$  arithmetic operations if and only if the polynomial

$$M_n = \sum_{i \in [n]} \sum_{j \in [n]} \sum_{k \in [n]} x_{ij} \cdot y_{jk} \cdot z_{ki}$$

can be computed by a  $\Sigma\Pi\Sigma$  circuit where the top fanin  $s$  is at most  $\tilde{O}(n^\omega)$ .

<sup>7</sup>Recall that a multivariate polynomial is said to be homogeneous if all its monomials have the same total degree. An arithmetic circuit is said to be *homogeneous* if the polynomial computed at every internal node of the circuit is a homogeneous polynomial. It is a folklore result (cf. the survey by Shpilka and Yehudayoff [SY10]) that as far as computation by polynomial-sized arithmetic circuits of unbounded depth is concerned one can assume without loss of generality that the circuit is homogeneous. Specifically, if a homogeneous polynomial  $f$  of degree  $d$  can be computed by an (unbounded depth) arithmetic circuit of size  $s$ , then it can also be computed by a *homogeneous* circuit of size  $O(d^2 \cdot s)$ .

<sup>8</sup>To the best of our knowledge, no  $\Sigma\Pi\Sigma$  circuit of size smaller than  $2^{O(d \log d)}$  computing  $\text{Det}_d$  was previously known.

showed that over any field  $\mathbb{F}$ , any homogeneous  $\Sigma\Pi\Sigma$  circuit computing the determinant  $\text{Det}_d$  must be of size  $2^{\Omega(d)}$ . Grigoriev and Karpinski [GK98], and Grigoriev and Razborov [GR00] showed that any  $\Sigma\Pi\Sigma$  arithmetic circuit over any *fixed* finite field computing  $\text{Det}_d$  must be of size at least  $2^{\Omega(d)}$ . This also implies that any  $\Sigma\Pi\Sigma$  arithmetic circuit *over integers* computing  $\text{Det}_d$  must be of size at least  $2^{\Omega(d)}$ . Raz and Yehudayoff give  $2^{\Omega(d)}$  lower bounds for *multilinear*  $\Sigma\Pi\Sigma$  circuits<sup>9</sup>. But without any restrictions, even a superpolynomial lower bound for  $\Sigma\Pi\Sigma$  circuits (over an infinite field) has remained elusive. The best known lower bound in the general  $\Sigma\Pi\Sigma$  case is the quadratic lower bound due to Shpilka and Wigderson [SW01]. Avi Wigderson [Wig07] highlighted this frontier in arithmetic complexity by concluding his plenary talk on ‘P, NP and mathematics’ at ICM 2006 with the problem of proving superpolynomial lower bounds for  $\Sigma\Pi\Sigma$  circuits computing the determinant.

**Our contribution.** The  $2^{\Omega(d)}$  lower bounds for various restrictions of  $\Sigma\Pi\Sigma$  circuits mentioned above seemed to suggest (at least to us) that any  $\Sigma\Pi\Sigma$  circuit computing the determinant  $\text{Det}_d$  needs to be of size at least  $2^{\Omega(d)}$ . Surprisingly, we show that this is not true - there do indeed exist much smaller  $\Sigma\Pi\Sigma$  circuits computing the determinant. Specifically we show that over  $\mathbb{Q}$ , the field of rational numbers, there exists a  $\Sigma\Pi\Sigma$  circuit of size  $2^{O(\sqrt{d} \cdot \log d)}$  computing the determinant. To the best of our knowledge, no  $\Sigma\Pi\Sigma$  circuit of size smaller than even  $2^{O(d \cdot \log d)}$  was previously known. More generally, we show:

**Theorem I.1.** *Let  $f(\mathbf{x}) \in \mathbb{Q}[\mathbf{x}]$  be an  $n$ -variate polynomial of degree  $d = n^{O(1)}$  computed by an arithmetic circuit of size  $s$ . Then it can also be computed by a  $\Sigma\Pi\Sigma$  circuit of size  $2^{O(\sqrt{d \log n \log d \log s})}$ .*

*Further, if  $f$  is computable by an arithmetic branching program of size  $s$ , then it can also be computed by an  $\Sigma\Pi\Sigma$  circuit of size  $2^{O(\sqrt{d \log n \log s})}$ .*

Note that  $\text{Det}_d$  can be computed by an ABP of size  $d^{O(1)}$  (cf. [Ber84], [MV97]) and hence we immediately get the  $\Sigma\Pi\Sigma$  circuit for it as mentioned above. We note here that in particular, the above theorem shows that a  $\Sigma\Pi\Sigma$  lower bound of  $2^{\Omega(d \log n)}$  for any explicit  $n$ -variate polynomial  $f$  of degree  $d$

entails a  $2^{\Omega(d \log n)}$  lower bound on the size of any arithmetic circuit computing  $f$ .

**Comparison with prior work.** Prior work by [AV08], [Koi12] and [Tav13] reduce the depth to four and we build upon their work to reduce the depth even further to three. Most closely related is the work by Raz [Raz10]. While both our work and [Raz10] have the same high-level message, namely that strong enough lower bounds for  $\Sigma\Pi\Sigma$  circuits imply more general superpolynomial lower bounds, we make here significant quantitative improvements. We state this from the perspective of obtaining lower bounds. Firstly, Raz’s result would yield only superpolynomial *formula* lower bounds while ours can yield circuit lower bounds. Secondly, Raz requires the degree of the output polynomial to be rather small:  $d \leq \frac{\log n}{\log \log n}$  while our results are valid for much larger  $d$ , say  $d = n^{\Omega(1)}$ . Most importantly, Raz requires almost optimal  $\Sigma\Pi\Sigma$  lower bounds of about  $2^{(d \log n) \cdot (1 - o(1))}$  while for us a much weaker lower bound of  $2^{\omega(\sqrt{d} \log n)}$  will suffice.  $\Sigma\Pi\Sigma$  circuits have been intensely investigated - initially for their connection to tensor rank and more recently as a special case of the polynomial identity testing problem. Given this intense investigation of  $\Sigma\Pi\Sigma$  circuits, it is natural to wonder as to why these results were not obtained before. We feel that this may be because our construction is significantly counterintuitive - the intermediate terms are of degree much higher than the degree of the output polynomial and moreover we need the field to have zero or large characteristic. Finally, we remark here that as a tool for proving lower bounds, our result is somewhat incomparable to [Koi12] - while the reduction of the depth further should facilitate the task of proving lower bounds, the fact that the resulting  $\Sigma\Pi\Sigma$  circuit is nonhomogeneous hinders it. Overall, it is not clear to us as to which of these two kinds of circuits is a better starting point.

**Further Results.** In Section V we then present some further consequences and reductions. Following [AV08] we show that a blackbox derandomization of polynomial identity testing for  $\Sigma\Pi\Sigma$  circuits leads to a quasipolynomial identity test for general circuits. We also explore the relation of  $\Sigma\Pi\Sigma$  circuits with a subclass of circuits that arise in our proof.

<sup>9</sup>The results of Raz and Yehudayoff are more general.

## II. PROOF OVERVIEW

**Quick Sketch.** The depth reduction proceeds through a series of transformations to the circuit - first decreasing the depth, then replacing the multiplication ( $\times$ ) gates with exponentiation gates at the expense of increasing the depth slightly and then decreasing the depth once again to three. We will flesh out this quick sketch after introducing some relevant notation.

**Notation.** Bounded depth arithmetic circuits consist of alternating layers of addition and multiplication gates. We will denote an arithmetic circuit of depth  $d$  by a sequence of  $d$  symbols wherein each symbol (either  $\Sigma$  or  $\Pi$ ) denotes the nature of the gates at the corresponding layer and the leftmost symbol indicates the nature of the gate at the output layer. For example, a  $\Pi\Sigma$  circuit with  $n$  input variables computes a polynomial in the following way:

$$C(\mathbf{x}) = \prod_{i \in [d]} \left( \sum_{j \in [n]} a_{ij} x_j + a_{i0} \right)$$

where each  $a_{ij} \in \mathbb{F}$  is a field element

while a  $\Sigma\Pi\Sigma$  circuit computes a polynomial as in equation (1). Some of the intermediate circuits that we construct will have the feature that all the incoming edges to a multiplication gate come from a single gate  $g$  (thus computing  $g^e$ , if there are  $e$  wires entering the multiplication gate). We will refer to such circuits as *powering circuits* and use  $\wedge$  instead of  $\Pi$  to denote a layer of multiplication gates in such circuits. So for example, a  $\Sigma\wedge\Sigma$  circuit computes a polynomial in the following manner:

$$C(\mathbf{x}) = \sum_{i \in [s]} \ell_i(\mathbf{x})^{e_i}$$

where each  $\ell_i \in \mathbb{F}[\mathbf{x}]$  is an affine form.

In doing the transformations it is useful to keep track of the fanin to various gates, especially multiplication gates. Towards this end, we extend the above notation and allow integer superscripts on  $\Pi$  symbols (respectively  $\Sigma$  and  $\wedge$  symbols) which denotes an upper bound on the fanin of any gate in the corresponding layer. So for example a  $\Sigma\Pi^{[a]}\Sigma\Pi^{[b]}$  circuit computes a polynomial of the

following form:

$$C = \sum_{i \in [s]} \prod_{j \in [a]} Q_{ij}$$

with  $\deg Q_{ij} \leq b$  for all  $i \in [s], j \in [a]$

while a  $\Sigma\wedge^{[a]}\Sigma$  circuit computes a polynomial a following manner:

$$C(\mathbf{x}) = \sum_{i \in [s]} \ell_i(\mathbf{x})^{e_i}$$

where, each  $e_i \leq a$ , and  
each  $\ell_i \in \mathbb{F}[\mathbf{x}]$  is an affine form.

With this notation in place we are ready to give a more detailed overview.

**Proof Overview.** Let  $f(\mathbf{x}) \in \mathbb{Q}[\mathbf{x}]$  be a polynomial of degree  $d$  computed by an arithmetic branching program of size  $s$ . The first step is to obtain from  $C$  a depth-4 circuit  $C_1$  computing  $f$ . Specifically,  $C_1$  is a  $\Sigma\Pi^{[a]}\Sigma\Pi^{[d/a]}$  circuit (for a suitably chosen  $a$ ) of size  $s_1 = 2^{O(\sqrt{d \log s \log n})}$ . This is achieved via Koiran's [Koi12] strengthening of the Agrawal-Vinay [AV08] depth reduction.

The second step is to use  $C_1$  to obtain a depth-5 *powering circuit*  $C_2$ . Specifically,  $C_2$  is a  $\Sigma\wedge^{[a]}\Sigma\wedge^{[d/a]}\Sigma$  circuit of size  $s_2 = 2^{O(\sqrt{d \log s \log n})}$ . The main ingredient of this step is a lemma of Fischer [Fis94] showing how a monomial can be computed by a  $\Sigma\wedge\Sigma$  circuit. In other words, Fischer's lemma shows to compute a product as a sum of powers of sums. By applying this lemma to every multiplication gate, we can convert the circuit  $C_1$  to a  $\Sigma\wedge\Sigma\wedge\Sigma$  circuit  $C_2$ . It is worth noting that Fischer's lemma is not true over fields of small characteristic.

The final step is to convert the  $\Sigma\wedge\Sigma\wedge\Sigma$  circuit  $C_2$  to a  $\Sigma\Pi\Sigma$  circuit  $C_3$ , and this is done by invoking the "duality trick" of Saxena [Sax08] and factoring the resulting univariate polynomials to get a  $\Sigma\Pi\Sigma$  circuit over an extension of  $\mathbb{Q}$  of not too large degree. Finally, from this we derive the required  $\Sigma\Pi\Sigma$  circuit over  $\mathbb{Q}$ . Overall in the last step we increase the degree of the intermediate polynomials substantially - to  $2^{O(\sqrt{d \log n \log s})}$ . Our construction ensures that all the high ( $> d$ ) degree monomials so generated ultimately cancel out. The resulting  $\Sigma\Pi\Sigma$  circuit  $C_3$  is of size  $s_3 = 2^{O(\sqrt{d \log n \log s})}$ .

### III. PRELIMINARIES

This section would deal with the preliminaries required for the rest of the paper. As usual  $[n]$  denotes the set of first  $n$  positive integers. For the ease of book-keeping, we define the size of a circuit as the number of wires<sup>10</sup> in the circuit.

**Algebraic Branching Programs (ABPs).** An ABP is a layered graph with edges going from layer  $i$  to  $i + 1$ . Every edge  $e$  is labelled by a linear polynomial  $\ell_e$ . The first layer has only one vertex called the *source* and the last layer has only one vertex called the *sink*. For any path  $\gamma = (e_1, \dots, e_d)$  from source to sink, the weight of  $\gamma$  is defined as  $\text{wt}(\gamma) = \ell_{e_1} \dots \ell_{e_d}$ . The ABP is said to compute the polynomial  $\sum_{\gamma} \text{wt}(\gamma)$ , where  $\gamma$  runs over all source-sink paths.

An ABP is said to be *homogeneous* if all edge labels are homogeneous linear forms, and naturally computes a homogeneous polynomial.

We shall say that a (possibly non-homogeneous) polynomial is computed by a homogeneous ABP if each of its homogeneous parts can be computed by a homogenous ABP. It is a well-known fact (cf. [SY10]) that if a degree  $d$  polynomial can be computed by a size  $s$  (possibly non-homogeneous) ABP, then it can be computed by a homogeneous ABP of size  $sd^2$ .

The following conversion from circuits to ABPs is attributed by Koiran [Koi12] to Malod and Portier [MP08] but can also be easily deduced directly from [VSB83].

**Lemma III.1.** *Let  $f$  be a polynomial of degree  $d$  computed by a circuit of size  $s$ . Then there is a homogeneous ABP of depth  $d$  and size  $s' = 2^{O(\log s \cdot \log d)}$  computing  $f$ .*

The following bound on a binomial coefficients is an easy consequence of Stirling's approximation.

**Lemma III.2.** (cf. [AV08], lemma 2.2 for a proof) *For any  $n, k$ ,*

$$\binom{n+k}{k} = 2^{O(k \log n)}$$

<sup>10</sup>One could alternatively define the size of a circuit as the number of nodes but defining it this way is more natural for us as it simplifies the bookkeeping - for example in tracking the size of an exponentiation gate.

### IV. THE DEPTH-REDUCTION

Let us recall the statement of our main result for branching programs.

**Theorem I.1 (restated).** *Let  $f(\mathbf{x}) \in \mathbb{Q}[\mathbf{x}]$  be an  $n$ -variate polynomial of degree  $d = n^{O(1)}$  computed by an arithmetic circuit of size  $s$ . Then it can also be computed by a  $\Sigma\Pi\Sigma$  circuit of size  $2^{O(\sqrt{d \log n \log s})}$ .*

We first observe that the corresponding depth reduction for general circuits (as given in the statement of this theorem in Section I) follows immediately from the above statement via an application of Lemma III.1 - we first convert the given circuit to a slightly larger ABP and then apply the depth reduction for ABPs. The rest of this section is devoted to the proof of the above theorem. So let  $f$  be an  $n$ -variate polynomial of degree  $d$  computed by an arithmetic circuit of size  $s$ . As mentioned in Section II, the depth reduction roughly proceeds through the following steps:

- **Step 1:** Arithmetic branching programs  $\longrightarrow \Sigma\Pi^{[a]}\Sigma\Pi^{[d/a]}$  circuits
- **Step 2:**  $\Sigma\Pi^{[a]}\Sigma\Pi^{[d/a]}$  circuits  $\longrightarrow \Sigma\wedge^{[a]}\Sigma\wedge^{[d/a]}\Sigma$  circuits
- **Step 3:**  $\Sigma\wedge^{[a]}\Sigma\wedge^{[d/a]}\Sigma$  circuits  $\longrightarrow \Sigma\Pi\Sigma$  circuits

In the rest of this section we shall provide the details on how to perform each of the above steps while keeping track of the loss in size incurred at each step.

A. *Step 1: General circuits to  $\Sigma\Pi^{[O(a)]}\Sigma\Pi^{[d/a]}$  circuit*

The first step is a direct consequence of the depth-reduction result of Koiran [Koi12].

**Theorem IV.1** ([Koi12]). *Let  $f$  be an  $n$ -variate polynomial of degree  $d$  computed by an arithmetic branching program of size  $s$ . Then, for all  $a$  there is an equivalent homogeneous  $\Sigma\Pi^{[a]}\Sigma\Pi^{[(d/a)]}$  circuit computing  $f$  of size  $s^a + (s^2 d) \cdot \binom{n+(d/a)}{(d/a)}$ .*

Choosing  $a = \sqrt{\frac{d \log n}{\log s}}$  (and using the bound of Lemma III.2) gives:

**Corollary IV.2.** *Let  $f$  be an  $n$ -variate degree  $d$  polynomial computed by arithmetic branching program of size  $s$ . Then, there is an equivalent homogeneous  $\Sigma\Pi^{[a]}\Sigma\Pi^{[d/a]}$  (for  $a = \sqrt{\frac{d \log n}{\log s}}$ ) circuit  $C_1$  computing  $f$  of size  $s_1 = \exp(O(\sqrt{d \log n \log s}))$ .*

**B. Step 2:**  $\Sigma\Pi^{[a]}\Sigma\Pi^{[(d/a)]}$  circuit to  $\Sigma\wedge^{[a]}\Sigma\wedge^{[d/a]}\Sigma$  circuit

The next step relies on a construction of Fischer [Fis94] to write a monomial as a sum of powers of linear functions which we describe below.

**Lemma IV.3** ([Fis94]). *For any  $n$ , the monomial  $x_1 \cdots x_n$  can be expressed as a linear combination of  $2^{n-1}$  powers of linear forms through the following:*

$$n! \cdot x_1 \cdots x_n = \sum_{S \subseteq [n]} \left( \sum_{i \in S} x_i \right) (-1)^{n-|S|}$$

The proof of the above lemma is a simple inclusion-exclusion argument and can also be seen in [Shp02].

Since any degree  $d$  monomial is a projection of  $x_1 \cdots x_d$ , a corollary of the above lemma is that every degree  $d$  monomial can be expressed as a sum of  $2^{d-1}$  powers of linear forms. It is also worth noting that the above lemma is not true in low characteristic. For example, in a field  $\mathbb{F}$  of characteristic 2,  $(x + \alpha y + \beta)^2 = x^2 + \alpha^2 y^2 + \beta^2$  and hence the monomial  $x \cdot y$  cannot be expressed as a sum of squares of affine forms. With this lemma, we can now proceed to the transformation in step 2.

**Lemma IV.4.** *Let  $f$  be an  $n$ -variate degree  $d$  polynomial computed by a homogeneous  $\Sigma\Pi^{[a]}\Sigma\Pi^{[b]}$  circuit of size  $s_1$ . Then, there is an equivalent  $\Sigma\wedge^{[a]}\Sigma\wedge^{[b]}\Sigma$  circuit of size  $(s_1^3 abn) \cdot 2^{a+b}$  computing  $f$ .*

*Proof:* A  $\Sigma\Pi^{[a]}\Sigma\Pi^{[b]}$  circuit  $C$  of size  $s_1$  computes a polynomial of the form

$$C = \sum_{i \in [s_1]} \prod_{j \in [a]} Q_{ij}$$

where,  $Q_{ij}$  has degree at most  $b$

Since the size of the circuit is  $s_1$ , each of the  $Q_{ij}$ 's have at most  $s_1$  monomials. Further their degree is at most  $b$  and hence we may apply Lemma IV.3 to

each monomial and express  $Q_{ij}$  as a  $\Sigma\wedge^{[b]}\Sigma$  circuit of size  $(bs_1n) \cdot 2^b$ .

Now applying Lemma IV.3 to each term  $T_i = \prod_{j \in [a]} Q_{ij}$  (where some of the  $Q_{ij}$ 's could be 1), we can express it as a sum of at most  $2^a$   $a$ -th powers of linear combinations of the  $Q_{ij}$ 's. Thus each  $T_i$  can be expressed as a  $\Sigma\wedge^{[a]}\Sigma\wedge^{[b]}\Sigma$  circuit of size  $(a2^a) \cdot (s_1) \cdot (bs_1n2^b)$ . Since there are at most  $s_1$  terms  $T_i$ , we get overall a  $\Sigma\wedge^{[a]}\Sigma\wedge^{[b]}\Sigma$  circuit of size at most  $(s_1^3 abn) \cdot 2^{a+b}$ . ■

Combining this with corollary IV.2 we immediately get:

**Corollary IV.5.** *Let  $f$  be an  $n$ -variate polynomial of degree  $d$  computed by an arithmetic circuit of size  $s$ . Then there is an equivalent  $\Sigma\wedge^{[a]}\Sigma\wedge^{[d/a]}\Sigma$  (for  $a = \sqrt{\frac{d \log n}{\log s}}$ ) circuit  $C_2$  computing  $f$  of size  $s_2 = \exp(O(\sqrt{d \log n \log s}))$ .*

**C. Step 3:**  $\Sigma\wedge^{[a]}\Sigma\wedge^{[d/a]}\Sigma$  circuits to  $\Sigma\Pi\Sigma$  circuits

The final step of the proof uses the *duality trick* of Saxena [Sax08]. The statement given below is slightly different from the statement in [Sax08], but can be easily inferred from the proof.

**Lemma IV.6** ([Sax08]). *For every  $m, d > 0$  and distinct  $\alpha_1, \dots, \alpha_{md+1} \in \mathbb{Q}$ , there exists  $\beta_1, \dots, \beta_{md+1} \in \mathbb{Q}$  such that*

$$(u_1 + \cdots + u_m)^d = \sum_{i=1}^{md+1} \beta_i \prod_{j=1}^m E_d(\alpha_i \cdot u_j)$$

where  $E_d(u) \stackrel{\text{def}}{=} 1 + \frac{u}{1!} + \cdots + \frac{u^d}{d!}$ .

In order to make our exposition self-contained we reproduce the following proof from [Sax08].

*Proof:* Let  $\ell \stackrel{\text{def}}{=} (u_1 + u_2 + \cdots + u_m)$ .

Then since,

$$e^{\ell z} = 1 + \frac{\ell}{1!} z + \cdots + \frac{\ell^d}{d!} z^d + \cdots$$

we have that  $\frac{\ell^d}{d!}$  equals the coefficient of  $z^d$  in  $e^{\ell z}$ . Therefore,

$$\begin{aligned} \ell^d &= d! \cdot \{ \text{coeff of } z^d \text{ in } e^{\ell z} \} \\ &= d! \cdot \{ \text{coeff of } z^d \text{ in } e^{u_1 z} \cdot e^{u_2 z} \cdots e^{u_m z} \} \\ &= d! \cdot \{ \text{coeff of } z^d \text{ in } E_d(u_1 z) \cdots E_d(u_m z) \} \end{aligned}$$

Now let  $F(\mathbf{u}, z) := E_d(u_1 z) \cdots E_d(u_m z)$ . Viewing  $F$  as a univariate

polynomial in  $z$  of degree  $(md)$ , we see via interpolation that the coefficient of  $z^d$  in  $F$  can be obtained as a linear combination of  $F(\mathbf{u}, \alpha_1), \dots, F(\mathbf{u}, \alpha_{md+1})$ . That is, there exist  $\delta_1, \dots, \delta_{md+1}$  such that

$$\text{coeff of } z^d \text{ in } F(\mathbf{u}, z) = \sum_{i \in [md+1]} \delta_i F(\mathbf{u}, \alpha_i).$$

Taking  $\beta_i = \delta_i \cdot d!$  then completes the proof.  $\blacksquare$

With the above lemma, we can proceed to step 3. First we obtain a  $\Sigma\Pi\Sigma$  circuit over  $\mathbb{C}$ , the field of complex numbers. We shall subsequently convert the  $\Sigma\Pi\Sigma$  circuit over  $\mathbb{C}$  to one over  $\mathbb{Q}$ .

**Lemma IV.7.** *Let  $f$  be a polynomial computed by a  $\Sigma \wedge^{[a]} \Sigma \wedge^{[b]} \Sigma$  circuit of size  $s_2$  over  $\mathbb{Q}$ . Then, there is an equivalent  $\Sigma\Pi\Sigma$  circuit  $C_3$  over  $\mathbb{C}$  of size  $s_3 = O(s_2^3 a^2 b n)$  computing  $f$ . The circuit  $C_3$  has top fan-in  $O(s_2^2 a)$  and formal degree at most  $O(s_2 a b)$ .*

*Proof:* A  $\Sigma \wedge^{[a]} \Sigma \wedge^{[b]} \Sigma$  circuit  $C$  computes a polynomial of the form  $C = T_1 + \dots + T_{s_2}$  where each  $T_i = (\ell_{i1}^b + \dots + \ell_{is_2}^b)^a$  for some linear forms  $\ell_{ij}$ 's. Applying Lemma IV.6 to each such term  $T = (\ell_1^b + \dots + \ell_{s_2}^b)^a$ , we can write  $T$  as

$$\begin{aligned} T &= \sum_{i=1}^{s_2 a + 1} \beta_i \prod_{j=1}^{s_2} E_a(\alpha_i \cdot \ell_j^b) \\ &= \sum_{i=1}^{s_2 a + 1} \beta_i \prod_{j=1}^{s_2} f_i(\ell_j) \\ &\quad \text{where } f_i(t) \stackrel{\text{def}}{=} E_a(\alpha_i \cdot t^b) \end{aligned}$$

Since each  $f_i(t)$  is a univariate polynomial of degree at most  $ba$ , it splits as a product of linear factors over  $\mathbb{C}$ , yielding a depth-3 circuit of the form,

$$T = \sum_{i=1}^{s_2 a + 1} \prod_{j=1}^{s_2} \prod_{k=1}^{ab} (\ell_j - \gamma_{ik}) \quad (2)$$

Thus,  $f$  can be computed by a  $\Sigma\Pi\Sigma$  circuit of top fan-in  $s_2 \cdot (s_2 a + 1) = O(s_2^2 a)$  and degree  $O(s_2 a b)$ , thereby yielding an overall size of

$$\begin{aligned} s_3 &= s_2 \cdot (s_2 a + 1) \cdot O(s_2 a b) \cdot (n + 1) \\ &= O(s_2^3 a^2 b n) \end{aligned}$$

1) *Obtaining a  $\Sigma\Pi\Sigma$  circuit over rationals:* The circuit thus obtained from Lemma IV.7 involve coefficients that are roots of the univariates  $f_i(t) = E_a(\alpha_i \cdot t^b)$ . The following lemma shows that all these coefficients come from an algebraic extension of  $\mathbb{Q}$  of relatively small degree<sup>11</sup>.

**Lemma IV.8.** *Let  $\gamma_1, \dots, \gamma_a$  be roots of  $E_a(t)$ , and let  $\omega$  be a principal  $b$ -th root of unity. Then, the field  $\mathbb{Q}(\gamma_1^{1/b}, \dots, \gamma_a^{1/b}, \omega)$  contain the roots of every  $E_a(\alpha \cdot t^b)$  for every  $\alpha \in \mathbb{Q}$  such that  $\alpha^{1/b} \in \mathbb{Q}$ .*

*Proof:* The roots of  $E_a(\alpha \cdot t^b)$  are precisely  $(\frac{\gamma_i}{\alpha})^{1/b} \omega^j$  for every  $i \in [a], j \in [b]$ . Since  $\alpha^{1/b} \in \mathbb{Q}$ , each of these roots are in  $\mathbb{Q}(\gamma_1^{1/b}, \dots, \gamma_a^{1/b}, \omega)$ .  $\blacksquare$

Since we are free to choose the  $\alpha_i$ 's in Lemma IV.7, we can choose distinct  $\alpha_i$ 's so that  $\alpha_i^{1/b} \in \mathbb{Q}$ . Hence, the coefficients in the depth-3 circuit obtained from Lemma IV.7 come from  $\mathbb{K} := \mathbb{Q}(\gamma_1^{1/b}, \dots, \gamma_a^{1/b}, \omega)$  where  $\gamma_1, \dots, \gamma_a$  are roots of  $E_a(x)$ . Note that  $\mathbb{K}$  is an extension over  $\mathbb{Q}$  of degree at most  $(ab)^{O(a)} \cdot b$  (since each  $\gamma_i^{1/b}$  is a root of a polynomial over  $\mathbb{Q}$  of degree at most  $ab$ ).

The following lemma below gives a generic way of converting a circuit involving coefficients from a small extension to a circuit over the base field.

**Lemma IV.9.** *Let  $f(\mathbf{x}) \in \mathbb{Q}[\mathbf{x}]$  be computed by a  $\Sigma\Pi\Sigma$  circuit of top fanin  $s_3$  and formal degree  $D$  with coefficients coming from a finite extension field  $\mathbb{K}/\mathbb{Q}$ . Then, there is an equivalent  $\Sigma\Pi\Sigma$  circuit computing  $f$  of size  $\text{poly}(s_3, D, [\mathbb{K} : \mathbb{Q}])$  with coefficients coming from  $\mathbb{Q}$ .*

With this lemma, using the fact that the degree of the extension containing all coefficients is  $2^{O(a \log d)}$  and Lemma IV.7, we immediately get our main theorem.

*Proof of Lemma IV.9.* Since  $\mathbb{K}$  is a finite extension of  $\mathbb{Q}$ , there exists an element  $\theta \in \mathbb{K}$  such that  $\mathbb{K} = \mathbb{Q}(\theta)$ <sup>12</sup>. Hence, if  $m = [\mathbb{K} : \mathbb{Q}]$ , then  $\mathbb{K}$  is the vector space over  $\mathbb{Q}$  with  $\{1, \theta, \theta^2, \dots, \theta^{m-1}\}$  as a basis and the minimum polynomial of  $\theta$  has degree  $m$ . Therefore, any polynomial  $g(\mathbf{x}) \in \mathbb{K}[\mathbf{x}]$  can be uniquely written as  $g_0 + g_1 \theta + \dots + g_{m-1} \theta^{m-1}$

<sup>11</sup>basic facts about field extensions, their degrees, etc. can be found in Chapter 5 of [Her75].

<sup>12</sup>follows from the Primitive Element Theorem (Theorem 5.5.1 in [Her75]).

where each  $g_i \in \mathbb{Q}[\mathbf{x}]$ ; we shall use  $g^{[i]}$  to denote  $g_i$ .

If  $f = T_1 + \dots + T_{s_3}$  where each  $T_i$  is a product of linear polynomials over  $\mathbb{K}$ , then  $f = T_1^{[0]} + \dots + T_{s_3}^{[0]}$ . Hence it suffices to show that  $T^{[0]}$  can be expressed as a small depth-3 circuit over  $\mathbb{Q}$ .

Let  $T = \ell_1 \dots \ell_D \in \mathbb{K}[\mathbf{x}]$ . Then,

$$\begin{aligned} T &= \prod_{i=1}^D (\ell_i^{[0]} + \ell_i^{[1]}\theta + \dots + \ell_i^{[m-1]}\theta^{m-1}) \\ &= T^{[0]} + T^{[1]}\theta + \dots + T^{[m-1]}\theta^{m-1} \end{aligned}$$

Consider the polynomial obtained from above by replacing  $\theta$  by a formal variable  $y$ :

$$\begin{aligned} \tilde{T}(\mathbf{x}, y) &= \prod_{i=1}^D (\ell_i^{[0]} + \ell_i^{[1]}y + \dots + \ell_i^{[m-1]}y^{m-1}) \\ &= \tilde{T}_0 + \tilde{T}_1 y + \dots + \tilde{T}_{(m-1)D} y^{(m-1)D} \end{aligned}$$

Therefore, using interpolation, every  $\tilde{T}_i$  can be written as a linear combinations of the set  $\{\tilde{T}(\mathbf{x}, \alpha_i) : 1 \leq i \leq (m-1)D + 1\}$ . Since each such evaluation is a product of  $D$  linear polynomials over  $\mathbb{Q}$ , we have that each  $\tilde{T}_i$  can be expressed as a depth-3 circuit of top fanin  $(m-1)D + 1$  and formal degree  $D$ .

To obtain  $T^{[0]}, \dots, T^{[m-1]}$  from  $\tilde{T}_0, \dots, \tilde{T}_{(m-1)D}$ , we can express each  $\theta^i$  for  $m \leq i \leq (m-1)D$  as a linear combination of  $1, \dots, \theta^{m-1}$  to obtain that each  $T^{[i]}$  is the appropriate linear combination of  $\tilde{T}_0, \dots, \tilde{T}_{(m-1)D}$ . Therefore, in particular,  $T^{[0]}$  can be expressed as a depth-3 circuit over  $\mathbb{Q}$  of top fanin  $((m-1)D) \cdot ((m-1)D + 1)$  and formal degree  $D$ . Hence,  $f$  can be expressed as a depth-3 circuit over  $\mathbb{Q}$  of top fanin  $O(s_3 m^2 D^2)$  and formal degree  $D$ .  $\square$

## V. FURTHER CONSEQUENCES

### A. Depth reduction to PIT lift

Any depth reduction to a class  $\mathcal{C}$  of circuits provides a framework for lifting a polynomial time black-box PIT for the class  $\mathcal{C}$  to black-box PITs for general circuits with *slightly worse* running time. Such a lift in the context of the depth reduction in Theorem I.1 on exactly the same lines as in [AV08].

**Theorem V.1.** *If there is a polynomial time black-box PIT for the class of depth-3 circuits, then there*

*is a  $2^{(\log n)^{O(1)}}$  time black-box PIT for general circuits computing a low degree polynomial.*

Saha, Saptharishi and Saxena [SSS09] showed that PIT for width-2 branching programs completely capture PIT for depth-3 circuits. A corollary for the above theorem is that black-box PIT for width-2 ABPs would imply quasi-polynomial time black-box PIT for general circuits.

**Corollary V.2.** *If there is a polynomial time black-box PIT for the class of width-2 ABPs over  $\mathbb{Q}$ , then there is a  $2^{(\log n)^{O(1)}}$  time black-box PIT for general circuits computing a low degree polynomial.*

### B. Reduction from $\Sigma\Pi\Sigma$ circuits to $\Sigma\wedge\Sigma\wedge\Sigma$ circuits

For the purpose of proving super-polynomial circuit lower bounds over  $\mathbb{Q}$ , we can equivalently work with any of  $\Sigma\Pi\Sigma$  or  $\Sigma\wedge\Sigma\wedge\Sigma$  circuits. We give a partial converse of Lemma IV.7.

**Lemma V.3.** *Let  $f$  be an  $N$ -variate degree  $n$  polynomial over any characteristic zero field computed by a  $\Sigma\Pi\Sigma$  circuit with top fan-in  $s$  and product gates with fan-in at most  $d$ . Then, there exists an equivalent  $\Sigma\wedge\Sigma\wedge\Sigma$  circuit of size  $\text{poly}(N, d, s) \cdot 2^{O(\sqrt{n} \cdot \log n)}$ .*

## VI. CONCLUSION

Very recently, Tavenas [Tav13] has improved the depth-reduction to depth-4 circuits (Step 1 of our result) by showing that any  $n$ -variate homogeneous polynomial of degree  $d$  that is computable by a arithmetic circuit of size  $s$  can be equivalently computed by a  $\Sigma\Pi^{[15\sqrt{d}]} \Sigma\Pi^{[\sqrt{d}]}$  of size  $\exp(O(\sqrt{d} \log n \log s))$ . He further observed that plugging in this improvement in Step 1 of our result yields an improved reduction to depth-3 as well.

We saw that powering circuits are useful as an intermediate step in doing depth reduction of general circuits. We feel that proving lower bounds for powering circuits will also be useful as a good intermediate step towards proving lower bounds for general circuits. Towards this we recall a problem posed in [CKW11] in the form of a more specific conjecture.

**Conjecture VI.1.** *Over any field  $\mathbb{F}$  of characteristic 0, any depth- $\Delta$  powering circuit with  $\text{poly}(d)$ -*



bounded degree computing the monomial  $x_1 \cdots x_d$  must be of size at least  $2^{d^{\Omega(1/\Delta)}}$  size.

Also, step 1 and step 2 of the depth-reduction reduces any circuit to a depth-5 powering circuit with formal degree bounded by the degree of the polynomial. It is only step 3 that results in the blow-up in degree. Hence, proving a  $2^{\omega(\sqrt{d} \log d)}$  lower bound for low (formal) degree depth-5 powering circuits computing  $\text{Perm}_d$  would yield super-polynomial formula lower bound. Proving such a lower bound for homogeneous depth-5 powering circuits might be an easier task than proving lower bounds for non-homogeneous depth-3 circuits (where we have no degree bound). We pose the following problem as the next potential step towards proving super-polynomial formula lower bounds for  $\text{Perm}_d$ .

**Problem VI.2. Lower Bounds for  $\Sigma \wedge \Sigma \wedge \Sigma$  circuits.** Show that for any expression of the form

$$\text{Perm}_d = \sum_{i \in [s]} \left( \sum_{j \in [t]} \ell_{ij}^{\sqrt{d}} \right)^{\sqrt{d}}$$

then one must have  $s \cdot t = 2^{\omega(\sqrt{d})}$ .

We already know of a  $2^{\Omega(\sqrt{d})}$  lower bound [GKKS13] on  $s$ , independent of how large  $t$  is. Presumably using the internal structure of the polynomials, say the fact that each of the inner terms have a *low partial derivative space*, we should be able to prove better lower bounds. We believe that any technique to solve Problem VI.2 would be very insightful towards the grander goal of proving super-polynomial circuit lower bounds.

**Summary.**  $\Sigma \Pi \Sigma$  circuits have been intensely investigated. Some recent work led to both structural results on  $\Sigma \Pi \Sigma$  identities as well as deterministic blackbox algorithms for various subclasses of  $\Sigma \Pi \Sigma$  circuits. We also note here that the Sylvester-Gallai configurations that arose in this line of work, has led to some beautiful and productive series of works [BDYW11], [DSW12] in understanding such geometric configurations culminating in essentially optimal upper and lower bounds on the dimension of such configurations. Because of these developments, we are inclined towards interpreting Theorem I.1 in an optimistic manner - of proving lower bounds for  $\Sigma \Pi \Sigma$  circuits as yet another potential route to obtaining lower bounds for arbitrary arithmetic circuits.

*Acknowledgements:* We are thankful to Avi Wigderson for several useful comments and suggestions on the initial draft of this write-up. We would also like to thank Klim Efremenko for pointing out some typos in the initial draft.

## REFERENCES

- [AV08] Manindra Agrawal and V. Vinay. Arithmetic circuits: A chasm at depth four. In *FOCS*, pages 67–75, 2008.
- [BDYW11] B. Barak, Z. Dvir, A. Yehudayoff, and A. Wigderson. Rank bounds for design matrices with applications to combinatorial geometry and locally correctable codes. In *STOC*, pages 519–528, 2011.
- [Ber84] Stuart J. Berkowitz. On computing the determinant in small parallel time using a small number of processors. *Inf. Process. Lett.*, 18(3):147–150, 1984.
- [CKW11] Xi Chen, Neeraj Kayal, and Avi Wigderson. Partial derivatives in arithmetic complexity. *Foundations and Trends in Theoretical Computer Science*, 2011.
- [Csa76] L. Csanky. Fast parallel inversion algorithm. *SIAM Journal on Computing*, 5:618–623, 1976.
- [DSW12] Zeev Dvir, Shubhangi Saraf, and Avi Wigderson. Improved rank bounds for design matrices and a new proof of Kelly’s theorem. *Electronic Colloquium on Computational Complexity (ECCC)*, 19:138, 2012.
- [Fis94] I. Fischer. Sums of like powers of multivariate linear forms. *Mathematics Magazine*, 67(1):59–61, 1994.
- [GK98] Dima Grigoriev and Marek Karpinski. An exponential lower bound for depth 3 arithmetic circuits. In *STOC*, pages 577–582, 1998.
- [GKKS13] Ankit Gupta, Pritish Kamath, Neeraj Kayal, and Ramprasad Satharishi. Approaching the chasm at depth four. In *Proceedings of the Conference on Computational Complexity (CCC)*, 2013.
- [GR00] Dima Grigoriev and Alexander A. Razborov. Exponential lower bounds for depth 3 arithmetic circuits in algebras of functions over finite fields. *Appl. Algebra Eng. Commun. Comput.*, 10(6):465–487, 2000.
- [Her75] I.N. Herstein. *Topics in Algebra*. Wiley, second edition, 1975.

- [Koi12] Pascal Koiran. Arithmetic circuits: The chasm at depth four gets wider. *Theoretical Computer Science*, 448:56–65, 2012.
- [MP08] Guillaume Malod and Natacha Portier. Characterizing valiant’s algebraic complexity classes. *J. Complexity*, 24(1):16–38, 2008.
- [MV97] Meena Mahajan and V. Vinay. A combinatorial algorithm for the determinant. In *SODA*, pages 730–738, 1997.
- [NW97] N. Nisan and A. Wigderson. Lower bounds on arithmetic circuits via partial derivatives. *Computational Complexity*, 6(3):217–234, 1997.
- [Raz10] Ran Raz. Tensor-rank and lower bounds for arithmetic formulas. In *STOC*, pages 659–666, 2010.
- [Rys63] H. J. Ryser. *Combinatorial mathematics*. *Math. Assoc. of America*, 14, 1963.
- [Sax08] Nitin Saxena. Diagonal Circuit Identity Testing and Lower Bounds. In *ICALP (1)*, pages 60–71, 2008.
- [Shp01] Amir Shpilka. *Lower Bounds for Small Depth Arithmetic and Boolean Circuits*. PhD thesis, The Hebrew University, 2001.
- [Shp02] Amir Shpilka. Affine projections of symmetric polynomials. *J. of Computer and System Sciences*, 65(4):639–659, 2002.
- [SSS09] Chandan Saha, Ramprasad Satharishi, and Nitin Saxena. The Power of Depth 2 Circuits over Algebras. In *FSTTCS*, pages 371–382, 2009.
- [SW01] A. Shpilka and A. Wigderson. Depth-3 arithmetic circuits over fields of characteristic zero. *Computational Complexity*, 10(1):1–27, 2001.
- [SY10] Amir Shpilka and Amir Yehudayoff. Arithmetic circuits: A survey of recent results and open questions. *Foundations and Trends in Theoretical Computer Science*, 5:207–388, March 2010.
- [Tav13] Sébastien Tavenas. Improved bounds for reduction to depth 4 and 3. In *Mathematical Foundations of Computer Science (MFCS)*, 2013.
- [Val79] Leslie G. Valiant. Completeness Classes in Algebra. In *STOC*, pages 249–261, 1979.
- [VSBR83] Leslie G. Valiant, Sven Skyum, S. Berkowitz, and Charles Rackoff. Fast Parallel Computation of Polynomials Using Few Processors. *SIAM J. Comput.*, 12(4):641–644, 1983.
- [Wig07] Avi Wigderson. P, NP and Mathematics - A computational complexity perspective. In *Proceedings of the ICM 06 (Madrid)*, volume 1, pages 665–712. EMS Publishing House, Zurich, 2007.