Chapter 7
Progress on Polynomial Identity Testing-II

Nitin Saxena

To my grand-advisor Professor Somenath Biswas

Abstract We survey the area of algebraic complexity theory; with the focus being on the problem of polynomial identity testing (PIT). We discuss the key ideas that have gone into the results of the last few years.

Keywords Arithmetic circuit · Identity testing · Hitting-set · Rank · Lower bound · Jacobian · Concentration · Shift · Morphism

Mathematics Subject Classification (2010) Primary 68Q25, 68W30, Secondary 12Y05, 13P25

7.1 Introduction

Algebraic complexity theory is the study of computation via *algebraic* models, hence, algebraic techniques. In this article we work with only one model—*arithmetic circuit* (in short, *circuit*). A circuit $C(x_1, \ldots, x_n)$, over a ring R, computes a polynomial f in $R[x_1, \ldots, x_n]$. Its description is in the form of a rooted tree; with the *leaves* having the variables or constants as input, the internal *nodes* computing addition or multiplication, and the *root* having the f as output. The edges in C, called *wires*, carry the intermediate polynomials and could also be used to multiply by a constant (from R). By the *size*, respectively the *depth*, of C we mean the natural notions (sometimes to avoid "trivialities" we might want to take into account the bit-size needed to represent an element in R).

N. Saxena (✉)
Department of CSE, IIT Kanpur, Kanpur 208016, India
e-mail: nitin@cse.iitk.ac.in

M. Agrawal and V. Arvind (eds.), *Perspectives in Computational Complexity*,
Progress in Computer Science and Applied Logic 26, DOI: 10.1007/978-3-319-05446-9_7,

A moment's thought would suggest that a circuit is a rather compact way of representing polynomials. Example a circuit of size s could produce a polynomial of degree 2^s (hint: repeated squaring). In fact, a single product gate could multiply s linear polynomials and produce $n^{\Omega(s)}$ many monomials. Thus, a circuit is an 'exponentially' compact representation of some polynomial families (as opposed to simply writing it as a sum of monomials). Conversely, are there 'explicit' polynomial families (say n-variate n-degree) that require exponential (i.e. $2^{\Omega(n)}$) sized circuits? We "expect" almost every polynomial to be this hard, but, the question of finding an *explicit* family is open and is the main goal motivating the development of algebraic complexity.

One can try to directly give a good *lower bound* against circuits by designing an explicit polynomial family $\{f_n\}$ and prove that it requires a 'large'-sized circuit family $\{C_n\}$. The other, indirect, way is to design an efficient *hitting-set* $\mathcal{H}$ for the circuit family, i.e. if $C_n \neq 0$ then $\exists a \in \mathcal{H}, C_n(a) \neq 0$. This 'flip' from lower bounds to algorithms was first remarked by [HS80] and now it has several improved versions [KI04, Agr05, Agr06]. This is a remarkable phenomenon and is one of the primary motivations to study the question of PIT: Given a circuit C test it for zeroness, in time polynomial in size(C). The hitting-set version of PIT is also called *blackbox* PIT (contrasted with *whitebox* PIT).

The last 10 years have seen a decent growth of algebraic tools and techniques to understand the properties of polynomials that a circuit computes. The feeling is that these polynomials are special, different from general polynomials, but a strong enough algebraic 'invariant' or a combinatorial 'concept' is still lacking. There have been several articles surveying the known techniques and the history of PIT [Sax09, AS09, SY10, CKW11, Sap13]. In this survey we will attempt not to repeat what those surveys have already covered. So, we will focus only on the new ideas and assume that the reader has given at least a cursory glance at the older ones. We directly move on to the Leitfaden.

7.1.1 Survey Overview

This article deals mainly with three broad topics—the 'universality' of depth-3 circuits, the design of hitting-sets via 'faithful' morphisms and that via rank 'concentration'. A major emerging area that we skip in this article is that of PIT vis à vis GCT (geometric complexity theory) program [Mul11, Mul12a, Mul12b]; the algebraic-geometry interpretations there are interesting though any concrete PIT algorithm, or application, is yet to emerge.

Shallow circuits A depth-2 circuit (top + gate) of size s, over a field, essentially computes a sum of s monomials. Such polynomials are called *sparse* polynomials; blackbox PIT for them was solved few decades ago. So, our next stop is depth-3: Polynomials of the form

$$C = \sum_{i=1}^{k} \prod_{j=1}^{d} L_{i,j},$$

where $L_{i,j}$ are linear polynomials in $\mathbb{F}[x_1, \ldots, x_n]$. Significant research has been done with this model, but both subexponential PIT and exponential lower bounds are open here. Recently, a remarkable universality result was shown for depth-3 [GKKS13]: If an n-variate poly(n)-degree polynomial can be nontrivially computed by a circuit, then it can be nontrivially computed in depth-3. This 'squashing' of depth means that it suffices to focus on depth-3 for PIT purposes.

If we consider a depth-2 circuit (top $\times$ gate), over a *ring* R, then again we get some remarkable connections. Fix R to be the 2×2 matrix algebra $M_2(\mathbb{F})$, and consider the circuit

$$D = \prod_{i=1}^{d} L_i,$$

where L_i are linear polynomials in $R[x_1, \ldots, x_n]$. Traditionally, D is called a *width-2 algebraic branching program* (ABP). It was shown by [SSS09] that depth-3 PIT efficiently reduces to width-2 ABP PIT.

Faithful morphisms It was observed in the last few years that in all the known hitting-sets, the key idea in the proof is to work with a *homomorphism* φ and an algebraic *property* that the image of φ should preserve. [SS12] used a (Vandermonde-based) map $\varphi : \mathbb{F}[x_1, \ldots, x_n] \to \mathbb{F}[y_1, \ldots, y_k]$ that preserves the 'linear' rank of any k linear polynomials. This gave the first blackbox PIT for bounded top fanin depth-3, over any field.

Beecken et al. [BMS13] and Agrawal et al. [ASSS12] used a (Vandermonde and Kronecker-based) map $\varphi : \mathbb{F}[x_1, \ldots, x_n] \to \mathbb{F}[y_1, \ldots, y_k]$ that preserves the 'algebraic' rank (formally, *transcendence degree*) of certain k polynomials. This gave the first blackbox PIT (and lower bounds) for several well-studied classes of constant-depth circuits. One drawback of the technique is that it requires zero/large characteristic fields.

Rank concentration Inspired from the tensors, a restricted circuit model called multilinear read-once ABP (ROABP) has been intensively studied. Let R be the $w \times w$ matrix algebra $M_w(\mathbb{F})$ and let $\{S_i\}$ be a partition of $[n]$. Consider the circuit $D = \prod_{i=1}^{d} L_i$, where L_i are linear polynomials in $R[x_{S_i}]$ (i.e. the linear factors have disjoint variables). For D [FSS13] gave a hitting-set in time poly$(wn)^{\log w \cdot \log n}$, i.e. quasi-poly-time. The proof is based on the idea, following [ASS13], that after applying a small (Kronecker-based) 'shift', D gets the following property: The rank of its coefficients (viewed as $\mathbb{F}$-vectors) is concentrated in the 'low' support monomials. Thus, checking the zeroness of these low monomials is enough!

We conjecture that rank concentration, after a 'small' shift, should be attainable in any ABP D. But currently the proof techniques are not that strong. Recently, [AGKS13] have achieved rank concentration in multilinear depth-3 circuits where

the partitions (corresponding to each product gate) are 'close' to each other in the sense of 'refinement'.

7.2 Shallow Circuits, Deep Interconnections

In this section, we exhibit the key ideas behind the universality of two shallow circuits.

7.2.1 The Depth-3 Chasm

In the study of circuits one feels that low-depth should already hold the key. This feeling was confirmed in a series of work [VSBR83, AV08, Koi12, Tav13]: Any $\text{poly}(n)$-degree n-variate polynomial computed by a $\text{poly}(n)$-sized circuit C can also be computed by a $n^{O(\sqrt{n})}$-sized depth-4 circuit!

The idea for this is, in retrospect, simple—since the degree is only $\text{poly}(n)$, first, squash the depth of C to $O(\log n)$ by only a polynomial blowup in the size. This is done in a way so as to make the product gates quite *balanced*, i.e. their two inputs are roughly of the same degree. Next, identify a subcircuit C_2 by picking those gates whose output polynomial has degree at least $\sqrt{n}$, and call the remaining subcircuit C_1. We view C_2 as our circuit of interest that takes gates of C_1 as input. It can be shown that C_2 computes a polynomial of degree $\approx\sqrt{n}$ of its input variables (which are $\text{poly}(n)$ many). Obviously, each gate of C_1 also computes a polynomial of degree $\approx\sqrt{n}$ of its input variables (which are $x_1, \ldots, x_n$). Thus, C_2 finally computes a sum of $\approx\binom{\text{poly}(n)+\sqrt{n}}{\sqrt{n}}$ products, each product has $\sqrt{n}$ factors, and each factor is itself a sum of $\approx\binom{n+\sqrt{n}}{\sqrt{n}}$ degree-$\sqrt{n}$ monomials. To put it simply (and ignoring the constant factors), C can be expressed as a $\sum\prod^{\sqrt{n}}\sum\prod^{\sqrt{n}}$ circuit of size $n^{O(\sqrt{n})}$. The details of this proof can be seen in [Tav13].

The strength of depth-4 is surprising. Recently, an even more surprising reduction has been shown [GKKS13]—that to depth-3 (again, $n^{O(\sqrt{n})}$ sized). We will now sketch the proof. It ties together the known results in an unexpected way.

Essentially, the idea is to modify a $\sum\prod^{a}\sum\prod^{a}$ circuit C of size $s := n^a$ (where $a := \sqrt{n}$) by using two polynomial identities that are in a way "inverse" to each other, and are to do with powers-of-linear-forms. First, replace the product gates using Fischer's identity:

Lemma 2.1 [Fis94] *Any degree a monomial can be expressed as a linear combination of 2^{a-1} ath powers of linear polynomials, as:*

$$y_1 \cdots y_a \;=\; (2^{a-1}\cdot a!)^{-1}\cdot \sum_{r_2,\ldots,r_a\in\{\pm 1\}} \left(y_1 + \sum_{i=2}^{a} r_i y_i\right)^a \cdot (-1)^{\#\{i\,|\,r_i=-1\}}.$$

We denote this type of a circuit by the notation $\sum \bigwedge^a \sum$, where the wedge signifies the powering by a. The above identity transforms the $\sum \prod^a \sum \prod^a$ circuit C to a $\sum \bigwedge^a \sum \bigwedge^a \sum$ circuit, of size poly(s). We reuse s for this size estimate.

Next, the two power gates are 'opened' up using an identity introduced by the author:

Lemma 2.2 [Sax08] *For any a, m, there exist degree-a univariate polynomials $f_{i,j}$ such that*

$$(y_1 + \cdots + y_m)^a = \sum_{i=1}^{ma+1} \prod_{j=1}^{m} f_{i,j}(y_j).$$

Let us carefully see the jugglery on C. The $\sum \bigwedge^a \sum \bigwedge^a \sum$ circuit C has the expression $C = \sum_i T_i$, where each T_i has the form $(\sum_{j=1}^{s} \ell_{i,j}^{e_{i,j}})^a$ with linear $\ell_{i,j}$'s. We want to open up the top power gate of C. By Lemma 2.2 we get

$$T_i = \sum_{u=1}^{sa+1} \prod_{j=1}^{s} f_{u,j}(\ell_{i,j}^{e_{i,j}}).$$

Since $f_{u,j}$ is a univariate, it splits into linear polynomials when the base field $\mathbb{F}$ is *algebraically closed*. As $\ell_{i,j}$ is already a linear polynomial, we deduce that T_i, and hence C, is a $\sum \prod \sum$ circuit of size poly(s).

Finally, note that for the above arguments to work, we require $\mathbb{F}$ to be algebraically closed and char$(\mathbb{F}) > a$. Lemma 2.2 has been generalized to all characteristics by [FS13b], so it is likely that this depth-3 reduction can be extended to *all* algebraically closed fields.

The optimality of $n^{\sqrt{n}}$-size, in this reduction, is open. However, [KSS13] showed that any decent reduction in this size bound would imply *VNP* $\neq$ *VP*.

7.2.2 The Width-2 Chasm

Here we look at $\prod \sum$ circuits over a matrix algebra. Though the model $D = \prod_i L_i$, with linear $L_i \in R[x_1, \ldots, x_n]$, seems innocuous at first sight, a closer look proves the opposite! It can be shown fairly easily that a polynomial computed by a constant-depth circuit (over a field) can as well be computed by a D over a 3×3 matrix algebra [BC88]. On the other extreme, by taking $R = M_n(\mathbb{F})$ we can compute the *determinant* of a matrix in $\mathbb{F}^{n \times n}$ [MV97], hence, arithmetic *formulas* (not general circuits!) can be simulated in this model [Val79].

Perhaps surprisingly, [SSS09] showed that: A polynomial C computed by a depth-3 circuit (over a field) can be "almost"[1] computed by a D over a 2×2 matrix algebra.

[1] We are able to compute only a *multiple* of C. However, the extra factor is simply a product of poly-many linear polynomials. So, it suffices for PIT purposes.

This, togetherwith the previous subsection, makes the $\prod\sum$ circuits over $M_2(\mathbb{F})$ quite strong.

Say, we want to express the depth-3 circuit $C = \sum_{i=1}^{k} T_i$ in a 2×2 matrix product. First, we express a product $T_i = \prod_{j=1}^{d} \ell_{i,j}$ as:

$$\begin{bmatrix} \ell_{i,1} & 0 \\ 0 & 1 \end{bmatrix} \cdots \begin{bmatrix} \ell_{i,d-1} & 0 \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & \ell_{i,d} \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} T_i' & T_i \\ 0 & 1 \end{bmatrix}, \text{ where } T_i' := T_i/\ell_{i,d}.$$

Once we have such k 2×2 matrices, each containing T_i in the $(1, 2)$th place, we would like to sum the T_i's in a 'doubling' fashion (instead of one-by-one).

We describe one step of the iteration. Let $\begin{bmatrix} L_1 & L_2 f \\ 0 & L_3 \end{bmatrix}$ and $\begin{bmatrix} M_1 & M_2 g \\ 0 & M_3 \end{bmatrix}$ be encapsulating two intermediate summands f and g. With the goal of getting (a multiple of) $f + g$ we consider the following, carefully designed, product:

$$\begin{bmatrix} L_1 & L_2 f \\ 0 & L_3 \end{bmatrix} \cdot \begin{bmatrix} L_2 M_3 & 0 \\ 0 & L_1 M_2 \end{bmatrix} \cdot \begin{bmatrix} M_1 & M_2 g \\ 0 & M_3 \end{bmatrix}$$
$$= \begin{bmatrix} L_1 M_1 L_2 M_3 & L_2 M_3 L_1 M_2 (f+g) \\ 0 & L_3 M_3 L_1 M_2 \end{bmatrix}$$

After $\log k$ such iterations, we get a *multiple* of C in the $(1, 2)$-th entry of the final 2×2 matrix product. Note that the middle matrix, introduced in the LHS above, potentially doubles (in the degree of the entry polynomials) in each iteration. Thus, finally, D is a product of $\text{poly}(d2^{\log k})$ linear polynomials over $M_2(\mathbb{F})$. Thus, the size blowup is only polynomial in going from depth-3 to width-2.

7.3 Faithful Morphisms, Hitting-Sets

In algebraic complexity the study of certain maps has been fruitful—homomorphisms $\varphi : \mathcal{R} := \mathbb{F}[x_1, \ldots, x_n] \to \mathbb{F}[y_1, \ldots, y_k] =: \mathcal{R}'$ such that the algebraic 'relationship' of certain polynomials $\{f_1, \ldots, f_k\}$ does not change in the image of φ. When f_i's are linear this boils down to a linear algebra question and we can easily design φ in time $\text{poly}(n)$ (hint: employ Vandermonde matrix). This business becomes complicated when f_i's are nonlinear. Then we have to ask how are f_i's represented. If they are given via monomials then we invoke the Jacobian criterion to design φ, but the time complexity becomes exponential in k. Several variants of such faithful maps are discussed in the Ph.D thesis [Mit13]. We sketch the ideas behind two basic maps here.

7.3.1 Bounded Fanin Depth-3 Blackbox PIT

Let $C = \sum_{i\in[k]} T_i$ be a depth-3 circuit. When k is constant, C is naturally called *bounded fanin* depth-3. This case of PIT has, by now, a rich history [DS07, KS07, KS11, SS11, KS09, SS13, SS12]. Several new techniques have sprung up from this model— a locally decodable code structure, a rank-preserving map via extractors, Sylvester-Gallai configurations (higher dimensions and all fields) and rank bounds. We will sketch here the main idea behind the poly-time blackbox PIT of bounded fanin depth-3. The details are quite technical and could be seen in [SS13, SS12].

Vandermonde map We define a homomorphism Ψ_β, for a $\beta \in \mathbb{F}$, as:

$$\forall i \in [n], \quad \Psi_\beta : x_i \mapsto \sum_{j=1}^{k} \beta^{ij} y_j,$$

and $\Psi_\beta(\alpha) = \alpha$ for all $\alpha \in \mathbb{F}$. This (naturally) defines the action of Ψ_β, on *all* the elements of $\mathcal{R}$, that preserves the ring operations. We have the following nice property, as a consequence of [GR08, Lemma 6.1]:

Lemma 3.1 [Ψ_β preserves k-rank] *Let S be a subset of linear forms in $\mathcal{R}$ with* $\mathrm{rk}(S) \leq k$, *and* $|\mathbb{F}| > nk^2$. *Then* $\exists\beta \in \mathbb{F}$, $\mathrm{rk}(\psi_\beta(S)) = \mathrm{rk}(S)$.

Intuitively, Ψ_β is *faithful* to any algebraic object involving the elements in span(S). The proof of this lemma is by studying the coefficient-matrix of the linear polynomials in S, and its change under Ψ_β. This map has a role to play in bounded fanin depth-3 owing to a certain structural theorem from [SS13]—*certificate for a non-identity*.

To discuss this certificate we need a definition, that of 'paths' of 'nodes' in C (assumed to be nonzero). A *path* $\mathbf{p}$ with respect to an ideal I is a sequence of terms $\{p_1, p_2, \ldots, p_b\}$ (these are products of linear forms) with the following property. Each p_i divides T_i, and each p_i is a 'node' of T_i with respect to the ideal $\langle I, p_1, p_2, \ldots, p_{i-1}\rangle$.[2] So p_1 is a node of T_1 wrt I, p_2 is a node of T_2 wrt $\langle I, p_1\rangle$, etc.

Let us see an example of a path $(\langle 0\rangle, p_1, p_2, p_3)$ in Fig. 7.1. The oval bubbles represent the list of forms in a product gate, and the rectangles enclose forms in a node. The arrows show a path. Starting with the zero ideal, nodes $p_1 := x_1^2$, $p_2 := x_2(x_2 + 2x_1)$, and $p_3 := (x_4 + x_2)(x_4 + 4x_2 - x_1)(x_4 + x_2 + x_1)(x_4 + x_2 - 2x_1)$ form a path. Initially, the path is just the zero ideal, so x_1^2 is a node. Note how p_2 is a power of x_2 modulo radsp$\langle p_1\rangle$, and p_3 is a power of x_4 modulo radsp$\langle p_1, p_2\rangle$.

The non-identity certificate theorem [SS13, Theorem 25] states that for any non-identity C, there exists a path $\mathbf{p}$ such that modulo $\langle\mathbf{p}\rangle$, C reduces to a single nonzero multiplication term.

---

[2] By a *node* p_i we mean that some nonzero constant multiple of p_i is identical to a power-of-a-linear-form modulo radsp$\langle I, p_1, p_2, \ldots, p_{i-1}\rangle$, where radsp is the ideal generated by the set of all the linear polynomials that divide p_j, $j \in [i-1]$ and the generators of I.

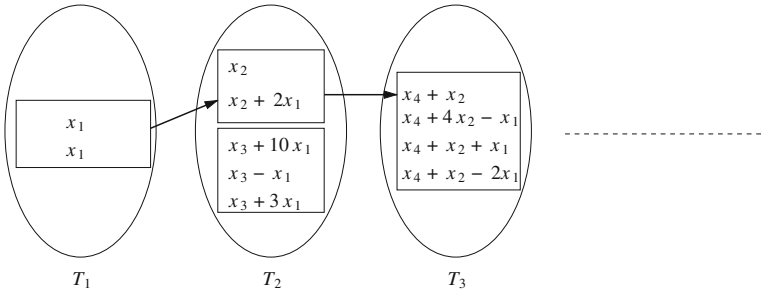

Fig. 7.1 Nodes and paths in $C = T_1 + T_2 + T_3 + \cdots$

Theorem 3.2 (Certificate for a non-identity) *Let I be an ideal generated by some multiplication terms. Let $C = \sum_{i\in[k]} T_i$ be a depth-3 circuit that is nonzero modulo I. Then $\exists i \in \{0, \ldots, k-1\}$ such that $C_{[i]}$[3] mod I has a path $\mathbf{p}$ satisfying: $C \equiv \alpha \cdot T_{i+1} \not\equiv 0 \pmod{I + \langle \mathbf{p} \rangle}$ for some $\alpha \in \mathbb{F}^*$.*

The proof of this theorem involves an extension of Chinese remaindering to ideals that are generated by multiplication terms. Once we have this structural result about depth-3, observe that we would be done if we could somehow ensure $T_{i+1} \notin \langle \mathbf{p} \rangle$ (in our application I is zero). How do we preserve this ideal non-membership under a cheap map?

Notice that the rank of the set S_0 of linear polynomials that divide the nodes in the path $\mathbf{p}$ is $<k$ (since path length is below k). Moreover, T_{i+1} factors into at most d linear polynomials, denote the set by S_1. So if we apply a map that preserves the rank of each of the d sets $S_0 \cup \{\ell\}$, $\ell \in S_1$, then, intuitively, the ideal non-membership should be preserved. As $\mathrm{rk}(S_0 \cup \{\ell\}) \leq k$ we can employ the previously discussed map Ψ_β (over a field satisfying $|\mathbb{F}| > dnk^2$). This idea could be easily turned into a proof; details are in [SS12].

Finally, what we have achieved is the construction of a map Ψ_β, in time poly(dnk), that reduces the variables of C from n to k and preserves nonzeroness. Once this is done, the poly(nd^k) blackbox PIT follows from the brute-force hitting-set.

7.3.2 Depth ≥ 3 Results

Looking at the success of bounded fanin depth-3 one wonders about the analogous depth-4 model:

$$C = \sum_{i\in[k]} \prod_{j\in[d]} f_{i,j}, \quad \text{where } f_{i,j} \text{ are sparse polynomials.} \tag{7.1}$$

[3] We mean $C_{[i]} := \sum_{j\in[i]} T_j$.

Here we are thinking of a bounded k. But now even $k = 2$ seems non-trivial! In fact, a simpler PIT case than this is an old open question in a related area [vzG83].

This *bounded top fanin* depth-4 PIT is an important open question currently. What is doable are other restricted models of depth-4. Inspired from the last subsection we ask: Is there a notion of 'rank' for general polynomials, are there easy 'faithful' maps, and finally is all this useful in PIT?

There are several notions of rank in commutative algebra. The one we [BMS13] found useful is—*transcendence degree* (trdeg). We say that a set S of polynomials $\{f_1, \ldots, f_m\} \subset \mathbb{F}[x_1, \ldots, x_n]$ is *algebraically dependent* if there exists a nonzero annihilating polynomial $A(y_1, \ldots, y_m)$, over $\mathbb{F}$, such that $A(f_1, \ldots, f_m) = 0$. The largest number of algebraically *in*dependent polynomials in S is called $\text{trdeg}(S)$. With this notion we call a homomorphism φ *faithful* if $\text{trdeg}(S) = \text{trdeg}(\varphi(S))$. The usefulness of φ (assuming that one can come up with it efficiently) was first proved in [BMS13]:

Lemma 3.3 (Faithful is useful) *Let φ be a homomorphism faithful to $\mathbf{f} = \{f_1, \ldots, f_m\} \subset \mathbb{F}[\mathbf{x}]$. Then for any $C \in \mathbb{F}[\mathbf{y}]$, $C(\mathbf{f}) = 0 \Leftrightarrow C(\varphi(\mathbf{f})) = 0$.*

This implies that we can use a faithful map to 'reduce' the number of variables n without changing the nonzeroness of C. The strategy can be used in cases where $\text{trdeg}(\mathbf{f})$ is small, say, smaller than a constant r.

The only missing piece is the efficiency of φ.[4] To do this we need three fundamental ingredients—an efficient criterion for algebraic independence (Jacobian), its behaviour under φ (chain rule), and standard maps (Vandermonde and Kronecker-based).

Lemma 3.4 (Jacobian criterion) *Let $\mathbf{f} \subset \mathbb{F}[\mathbf{x}]$ be a finite set of polynomials of degree at most d, and $\text{trdeg}(\mathbf{f}) \leq r$. If $\text{char}(\mathbb{F}) = 0$ or $\text{char}(\mathbb{F}) > d^r$, then $\text{trdeg}(\mathbf{f}) = \text{rk}_{\mathbb{F}(\mathbf{x})} \mathcal{J}_{\mathbf{x}}(\mathbf{f})$, where $\mathcal{J}_{\mathbf{x}}(\mathbf{f}) := \left(\partial f_i / \partial x_j\right)_{m \times n}$ is the* Jacobian matrix.

There are several proofs of this, see [Jac41, For91, BMS13, MSS12]. This gives us an efficient way to capture trdeg, when the characteristic is zero/large. Let us now see how the Jacobian matrix changes under φ.

Lemma 3.5 (Chain rule) $\mathcal{J}_{\mathbf{y}}(\varphi(\mathbf{f})) = \varphi\left(\mathcal{J}_{\mathbf{x}}(\mathbf{f})\right) \cdot \mathcal{J}_{\mathbf{y}}(\varphi(\mathbf{x}))$, *where φ applied to a matrix/set refers to the matrix/set obtained by applying φ to every entry.*

This is a simple consequence of the chain rule of 'derivatives'. It suggests that for φ to preserve the trdeg of the polynomials, we need to control—(1) the image of the original Jacobian under φ, and (2) the Jacobian of the image of $\mathbf{x}$. In our applications, the former is achieved by a Kronecker-based map (i.e. sparse PIT tricks, e.g. [BHLV09]) and the latter by Vandermonde map (as seen in the previous subsection).

This general 'recipe' has been successfully implemented to various circuit models. The case of the circuit $C'(\mathbf{x}) := C(\mathbf{f})$, where $\text{trdeg}(\mathbf{f}) \leq r$ and f_i's are polynomials

[4] It can be shown, from first principles, that a faithful r-variate map always *exists* [BMS13].

of sparsity at most s, was worked out in [BMS13]. The proof follows exactly the above strategy. The time complexity is polynomial in size(C') and $(s \cdot \deg(C'))^r$, where the exponential dependence comes from the sparsity estimate of $\mathcal{J}_{\mathbf{x}}(\mathbf{f})$ (and of course the final brute-force hitting-set for the r-variate $\varphi(C')$).

Agrawal et al. [ASSS12] extended the recipe to depth-4 circuits (7.1) where the number of $f_{i,j}$'s where any variable appears is bounded by r.[5] This model is called *occur-r* depth-4; it generalizes the well-studied multilinear read-r depth-4. Interestingly, slightly modified techniques also provided *exponential* lower bounds against these special models. This required proving some combinatorial properties of the derivatives of immanant (e.g. permanent, determinant).

The faithful maps recipe has been able to unify all the assorted *poly-time* hitting-sets known. However, one drawback is that it needs the characteristic to be zero/large. Baby steps in resolving that issue have been taken by [MSS12].

7.4 Rank Concentration, Shift, Hitting-Sets

The hitting-sets that we saw till now were for models where some parameter was kept bounded. But we could also study models with a 'structural' restriction, e.g. multilinearity. This route has also been successful and enlightening. We call a depth-3 circuit $C = \sum_i T_i$ *multilinear* if the linear factors in T_i involve disjoint variables. Hence, each product gate T_i induces a partition $\mathcal{P}_i$ on the variables (or indices) $[n]$. Moreover, we call C *set-multilinear* if these partitions are the same across all T_i's.

There is a large body of work on the set-multilinear model [RS05, AMS10, FS12, FS13b, ASS13, FS13a, FSS13, AGKS13]. The motivation for this model is, on the one hand, the algebraic concept of *tensors*, and, on the other hand, the interest in read-once *boolean* branching programs [Nis92, IMZ12, Vad12]. Interestingly, [FSS13] has shown (extending the ideas of [ASS13]) that the *current* situation in the arithmetic world is exponentially better than that in the boolean one!

Here we will exhibit the key ideas of [ASS13] and [AGKS13] on two *toy* cases that are already quite instructive; this saves us from the gory technical machinery that drives the more general cases.

7.4.1 Multilinear ROABP

Agrawal et al. [ASS13] gave the first quasi-poly-time hitting-set for set-multilinear depth-3 (and extensions to constant-depth, non-multilinear versions). This was generalized by [FSS13] to *any* depth; in fact, they dealt directly with the *multilinear ROABP* $D = \prod_i L_i$ over $M_w(\mathbb{F})$, where L_i's are linear polynomials in disjoint variables. Both the papers proved 'low-support rank concentration' in their models.

[5] Note that this does not mean that trdeg$(f_{i,j}|i, j)$ is bounded.

For the following discussion we fix a base commutative ring $R = H_w(\mathbb{F})$ called the *Hadamard* algebra (instead of the $w \times w$ matrix algebra). This is basically $(\mathbb{F}^k, +, \star)$, where $+$ is the vector addition and $\star$ is the coordinate-wise vector product (called the Hadamard product).

ℓ-concentration. We say that a polynomial $f \in R[x_1, \ldots, x_n]$ is *ℓ-concentrated* if

$$\mathrm{rk}_{\mathbb{F}}\{\mathrm{coef}_f(x_S) \mid S \subseteq [n], |S| < \ell\} = \mathrm{rk}_{\mathbb{F}}\{\mathrm{coef}_f(x_S) \mid S \subseteq [n]\},$$

where coef_f extracts a coefficient in f.

I.e. the coefficient-vectors of 'lower' monomials already span every possible coefficient-vector in f. We are interested in studying whether circuits compute an ℓ-concentrated polynomial for small ℓ (say, $\log n$ instead of n). By itself this is not true, e.g. the trivial circuit $D = x_1 \cdots x_n$ is not even n-concentrated. But, maybe we can transform f a bit and then attain $(\log n)$-concentration? In this case, $D' := D(x_1 + 1, \ldots, x_n + 1)$ is suddenly 1-concentrated!

It was shown by [ASS13] that any D, above R, becomes $(\log k)$-concentrated after applying a 'small' shift; the price of which is $n^{\log k}$ time. Once we have this it directly applies to the set-multilinear depth-3 model. Since, a depth-3 $C = \sum_{i \in [k]} T_i$ can be rewritten as $C = [1, \ldots, 1] \cdot D$, where $D = \begin{bmatrix} T_1 \\ \vdots \\ T_k \end{bmatrix}$ is of the promised sort over $R = H_k(\mathbb{F})$ (since D completely factorizes into disjoint-variate linear polynomials). So, ℓ-concentration in D implies an easy way to check C for zeroness—test the coefficients of the monomials below ℓ-support in C.

Glimpse of a proof We now show how to achieve ℓ-concentration, $\ell = O(\log k)$, in the following toy model:

$$D = \prod_{i \in [n]} (1 + z_i x_i), \quad \text{where } z_i \in H_k(\mathbb{F}). \tag{7.2}$$

Because of the disjointness of the factors it can be seen, as a simple exercise, that: D is ℓ-concentrated iff $D_S := \prod_{i \in S}(1 + z_i x_i)$ is ℓ-concentrated, for all $S \in \binom{[n]}{\ell}$. Thus, from now on we assume, wlog, $n = \ell$.

Shift D by formal variables $\mathbf{t}$, and normalize, to get a new circuit:

$$D' = \prod_{i \in [\ell]} (1 + z'_i x_i), \quad \text{where } z'_i \in H_k(\mathbb{F}(\mathbf{t})).$$

We can express the new coefficients as:

$$z'_i = z_i/(1 + z_i t_i), \ \forall i \in [\ell].$$

Conversely, we write:

$$z_i = z'_i/(1 - z'_i t_i), \ \forall i \in [\ell]. \tag{7.3}$$

We write z_S for $\prod_{i\in S} z_i$. Now the goal is to 'lift' an $\mathbb{F}$-dependence of z_S's to the z'_S; which ultimately shows the condition on the shift that shall yield concentration.

Consider the 2^ℓ vectors $\{z_S \mid S \subseteq [\ell]\}$. If $\ell > \log k$ then there is a nontrivial linear dependence amongst these vectors, say,

$$\sum_{S\subseteq[\ell]} \alpha_S z_S = 0, \text{ where } \alpha_S \in \mathbb{F}.$$

Rewriting this in terms of z'_S we get:

$$\sum_{S\subseteq[\ell]} \alpha_S \cdot \prod_{i\in S} z'_i/(1 - z'_i t_i) = 0.$$

$$\text{Or, } \sum_{S\subseteq[\ell]} \alpha_S \cdot z'_S \cdot \prod_{i\in[\ell]\setminus S} (1 - z'_i t_i) = 0. \tag{7.4}$$

Let us collect the 'coefficient' of $z'_{[\ell]}$ in the above expression. It comes out to,

$$\sum_{S\subseteq[\ell]} \alpha_S \cdot (-1)^{|[\ell]\setminus S|} \cdot t_{[\ell]\setminus S}. \tag{7.5}$$

If we can ensure this expression to be nonzero then Eq. (7.4) tells us that $z'_{[\ell]}$ is in the $\mathbb{F}(\mathbf{t})$-span of the 'lower' z'_S. But, ensuring the nonzeroness of Eq. (7.5) is easy—use t_i's such that all the $(\leq\ell)$-support monomials t_S are *distinct*. We can use standard sparse PIT tricks [BHLV09] for this, in time poly(n^ℓ).

What we have shown is that, after applying a Kronecker-based shift, the circuit D becomes ℓ-concentrated; all this in time $n^{O(\log k)}$. This 'recipe' of studying the generic shift, via some combinatorial properties of the 'transfer' equations (7.3), is generalized in [ASS13] to other D; and further improved in [FSS13] to multilinear ROABP. The latter use a 'primal' interpretation of the 'transfer' matrix and show that the linear transformation– corresponding to a Kronecker shift together-with the truncation of the high-support monomials –behaves like a *rank-extractor*.

It is not known how to design such hitting-sets, even for the toy case, in *poly*-time.

7.4.2 Towards Multilinear Depth-3

It is tantalizing to achieve ℓ-concentration in multilinear depth-3 (before embarking on the general depth-3!). A partial result in that direction was obtained in [AGKS13]. We will sketch their ideas in a toy model.

Consider a multilinear depth-3 circuit C with only *two* partitions being induced by the product gates—$\mathcal{P}_1 = \{\{1\}, \cdots, \{n\}\}$ and an arbitrary partition $\mathcal{P}_2$. Say, the number of the corresponding product gates is k_1 respectively k_2 (summing to k).

We can say, naturally, that $\mathcal{P}_1$ is a *refinement* of $\mathcal{P}_2$ (denoted $\mathcal{P}_1 \leq \mathcal{P}_2$) because: For every color (or part) $S \in \mathcal{P}_2$ there exist colors in $\mathcal{P}_1$ whose union is *exactly* S. In this refinement situation [AGKS13] showed that, again, a suitable shift in the $\prod\sum$ circuit D (corresponding to C) achieves ℓ-concentration in time poly$(n^{\log k})$.

Glimpse of a proof We can assume $\mathcal{P}_2$ different from $\mathcal{P}_1$, otherwise this case is no different from the last subsection. We assume that the first k_1 product gates in $C = \sum_{i\in[k]} T_i$ respect $\mathcal{P}_1$ and the rest k_2 respect $\mathcal{P}_2$. The corresponding circuit D where we desire to achieve concentration is $D = \begin{bmatrix} T_1 \\ \vdots \\ T_k \end{bmatrix}$ over $R = H_k(\mathbb{F})$. But now the linear factors of D are not necessarily in disjoint variables. Example $\begin{bmatrix} x_1x_2 \\ x_1+x_2 \end{bmatrix} = \left(x_1 + \begin{bmatrix} 0 \\ 1 \end{bmatrix} \cdot x_2\right) \cdot \left(\begin{bmatrix} 0 \\ 1 \end{bmatrix} + \begin{bmatrix} 1 \\ 0 \end{bmatrix} \cdot x_2\right)$ over $H_2(\mathbb{F})$.

To get some kind of a reduction to the set-multilinear case, we prove rank concentration in parts. First, we consider those monomials (called $\mathcal{P}_1$-*type*) that could only be produced by the 'upper' part of D (i.e. the first k_1 product gates of C). Such a monomial, say indexed by $S \subseteq [n]$, is characterized by the presence of $i, j \in S$ that are in the same color of $\mathcal{P}_2$. For a fixed such i, j we can "access" all such monomials by the derivative $\partial^2 D/\partial x_i \partial x_j =: \partial_{i,j} D$. Notice that this differentiation kills the 'lower' part of D and only the $\mathcal{P}_1$-part remains. So, we can prove $(2 + \log k_1)$-concentration in the monomials containing i, j as in Sect. 7.4.1. This proves $O(\log k_1)$-concentration in the monomials of $\mathcal{P}_1$-type.

Next, we want to understand the remaining monomials (called $\mathcal{P}_2$-type); those that could be produced by the 'lower' part of D (i.e. the last k_2 product gates of C). These, obviously, could also be produced by the upper part of D. Let us fix such a monomial, say $x_1 \cdots x_\ell$. Assume that $S_1, \ldots, S_\ell \in \mathcal{P}_2$ are the colors that contain one of the indices $1, \ldots, \ell$. Consider the subcircuit D_ℓ that in its i-th coordinate, $\forall i \in [k]$, simply drops those factors of T_i that are free of the variables $S_1 \cup \cdots \cup S_\ell$. The problem here is that D_ℓ may be a 'high' degree circuit ($\approx n$ instead of ℓ) and so we cannot use a proof like in Sect. 7.4.1.

But, notice that all the degree-$(\geq \ell)$ monomials in D_ℓ are $\mathcal{P}_1$-type; where we know how to achieve ℓ-concentration. So, we only have to care about degree-$(\leq \ell)$ $\mathcal{P}_2$-type monomials in D_ℓ. There, again, $(\log k)$-concentration can be shown using Sect. 7.4.1 and the well-behaved transfer equations.

This sketch, handling two refined partitions, can be made to work for significantly generalized models [AGKS13]. But, multilinear depth-3 PIT is still open (nothing better than exponential time known).

Remark 4.1 Using a different technique [AGKS13] also proves *constant*-concentration, hence designs *poly*-time hitting-sets, for certain constant-width ROABP. These models are arithmetic analogs of the *boolean* ones—width-2 read-once branching programs [AGHP92, NN93] and constant-width read-once permutation branching programs [KNP11].

7.5 Open Ends

The search for a strong enough technique to study arithmetic circuits continues. We collect here some easy-to-state questions that interest us.

Top fanin-2 depth-4 Find a faithful map φ that preserves the algebraic independence of two products-of-sparse polynomials $\prod_i f_i$ and $\prod_j g_j$. If we look at the relevant 2×2 Jacobian determinant, say wrt variables $X := \{x_1, x_2\}$, then the question boils down to finding a hitting-set for the special *rational* function $\sum_{i,j} \frac{\det \mathcal{J}_X(f_i, g_j)}{f_i g_j}$. Can this version of *rational sparse* PIT be done in subexponential time?

Independence over $\mathbb{F}_p$ Currently, there is no subexponential time algorithm/heuristic known to test two given circuits for algebraic independence over a 'small' finite field $\mathbb{F}_p$. The reason is that something as efficient as the Jacobian criterion is not readily available, see [MSS12].

Model in Eqn (7.2) Find a *poly*-time hitting-set for this simple model. Note that a poly-time whitebox PIT is already known [RS05].

Multilinear depth-3 Achieve $o(n)$-concentration in multilinear depth-3 circuits, in $n^{o(n)}$ time. Here, the presence of an exponential lower bound against the model [RY09] is quite encouraging.

References

[AGHP92] N. Alon, O. Goldreich, J. Håstad, R. Peralta, Simple construction of almost k-wise independent random variables. Random Struct. Algorithms **3**(3), 289–304 (1992). (Conference version in FOCS 1990)

[AGKS13] M. Agrawal, R. Gurjar, A. Korwar, N. Saxena, Hitting-sets for low-distance multilinear depth-3. Electron. Colloquium Comput. Complex. **20**, 174 (2013)

[Agr05] M. Agrawal, in *Proving lower bounds via pseudo-random generators, Proceedings of the 25th Annual Foundations of Software Technology and Theoretical Computer Science* (FSTTCS, 2005), pp. 92–105

[Agr06] M. Agrawal, *Determinant versus permanent, Proceedings of the 25th International Congress of Mathematicians (ICM)*, vol. 3 (2006), pp. 985–997

[AMS10] V. Arvind, P. Mukhopadhyay, S. Srinivasan, New results on noncommutative and commutative polynomial identity testing. Comput. Complex. **19**(4), 521–558 (2010). (Conference version in, CCC 2008)

[AS09] M. Agrawal, R. Saptharishi, Classifying polynomials and identity testing. Indian Acad. Sci. **P1**, 1–14 (2009). Platinum Jubilee

[ASS13] M. Agrawal, C. Saha, N. Saxena, in *Quasi-polynomial hitting-set for set-depth-Δ formulas* (STOC, 2013), pp. 321–330

[ASSS12] M. Agrawal, C. Saha, R. Saptharishi, N. Saxena, in *Jacobian hits circuits: hitting-sets, lower bounds for depth-D occur-k formulas & depth-3 transcendence degree-k circuits* (STOC, 2012), pp. 599–614

[AV08] M. Agrawal, V. Vinay, in *Arithmetic circuits: a chasm at depth four*. (FOCS, 2008), pp. 67–75

[BC88] M. Ben-Or, R. Cleve, in *Computing Algebraic Formulas Using a Constant Number of Registers* (STOC, 1988), pp. 254–257

[BHLV09] M. Bläser, M. Hardt, R.J. Lipton, N.K. Vishnoi, Deterministically testing sparse polynomial identities of unbounded degree. Inf. Process. Lett. **109**(3), 187–192 (2009)

[BMS13] M. Beecken, J. Mittmann, N. Saxena, Algebraic independence and blackbox identity testing. Inf. Comput. **222**, 2–19, (2013). (Conference version in ICALP 2011)

[CKW11] X. Chen, N. Kayal, A. Wigderson, Partial Derivatives in Arithmetic Complexity (and beyond). Found. Trends Theor. Comput. Sci. **6**(1–2), 1–138 (2011)

[DS07] Z. Dvir, A. Shpilka, Locally decodable codes with two queries and polynomial identity testing for depth 3 circuits. SIAM J. Comput. **36**(5), 1404–1434 (2007). (Conference version in STOC 2005)

[Fis94] I. Fischer, Sums of like powers of multivariate linear forms. Math. Mag. **67**(1), 59–61 (1994)

[For91] K. Forsman, Constructive commutative algebra in nonlinear control theory, Ph.D. thesis, Dept. of Electrical Engg., Linköping University, Sweden, 1991

[FS12] M.A. Forbes, A. Shpilka, in *On identity testing of tensors, low-rank recovery and compressed sensing* (STOC, 2012), pp. 163–172

[FS13a] M.A. Forbes, A. Shpilka, Explicit Noether Normalization for Simultaneous Conjugation via Polynomial Identity Testing, APPROX-RANDOM, 2013, pp. 527–542

[FS13b] M.A. Forbes, A Shpilka, in *Quasipolynomial-time Identity Testing of Non-Commutative and Read-Once Oblivious Algebraic Branching Programs* (FOCS, 2013)

[FSS13] M.A. Forbes, R. Saptharishi, A. Shpilka, Pseudorandomness for multilinear read-once algebraic branching programs, in any order. Electron. Colloquium Comput. Complex. **20**, 132 (2013)

[GKKS13] A. Gupta, P. Kamath, N. Kayal, R. Saptharishi, in *Arithmetic circuits: a chasm at depth three* (FOCS, 2013)

[GR08] A. Gabizon, R. Raz, Deterministic extractors for affine sources over large fields. Combinatorica **28**(4), 415–440 (2008). (Conference version in FOCS 2005)

[HS80] J. Heintz, C.-P. Schnorr, in *Testing Polynomials which Are Easy to Compute (Extended Abstract)* (STOC, 1980), pp. 262–272

[IMZ12] R. Impagliazzo, R. Meka, D. Zuckerman, in *Pseudorandomness from shrinkage* (FOCS, 2012), pp. 111–119

[Jac41] C.G.J. Jacobi, De determinantibus functionalibus. J. Reine Angew. Math. **22**(4), 319–359 (1841)

[KI04] V. Kabanets, R. Impagliazzo, Derandomizing polynomial identity tests means proving circuit lower bounds. Comput. Complex. **13**(1–2), 1–46 (2004). (Conference version in STOC 2003)

[KNP11] V. Kabanets, R. Impagliazzo, Derandomizing polynomial identity tests means proving circuit lower bounds. Comput. Complex. **13**(1–2), 1–46 (2004). (Conference version in STOC 2003)

[Koi12] P. Koiran, Arithmetic circuits: The chasm at depth four gets wider. Theor. Comput. Sci. **448**, 56–65 (2012)

[KS07] N. Kayal, N. Saxena, Polynomial identity testing for depth 3 circuits. Comput. Complex. **16**(2), 115–138 (2007). (Conference version in, CCC 2006)

[KS09] N. Kayal, S. Saraf, in *Blackbox polynomial identity testing for depth-3 circuits* (FOCS, 2009), pp. 198–207

[KS11] Z.S. Karnin, A. Shpilka, Black box polynomial identity testing of generalized depth-3 arithmetic circuits with bounded top fan-in. Combinatorica **31**(3), 333–364 (2011). (Conference version in, CCC 2008)

[KSS13] N. Kayal, C. Saha, R. Saptharishi, A super-polynomial lower bound for regular arithmetic formulas. Electron. Colloquium Comput. Complex. **20**, 91 (2013)

[Mit13] J. Mittmann, Independence in Algebraic Complexity Theory, Ph.D. thesis, Mathematisch-Naturwissenschaftlichen Fakultät der Rheinischen Friedrich-Wilhelms-Universität Bonn, Germany, Dec 2013

[MSS12] J. Mittmann, N. Saxena, P. Scheiblechner, Algebraic independence in positive characteristic—A p-adic calculus. Electron. Colloquium Comput. Complex. **TR12-014** (2012). (accepted in Trans. Amer. Math. Soc. 2013)

[Mul11] K. Mulmuley, On P versus NP and geometric complexity theory: dedicated to Sri Ramakrishna. J. ACM **58**(2), 5 (2011)

[Mul12a] K. Mulmuley, *Geometric Complexity Theory V: Equivalence between Blackbox Derandomization of Polynomial Identity Testing and Derandomization of Noether's Normalization Lemma* (FOCS, 2012), pp. 629–638

[Mul12b] K. Mulmuley, The GCT program toward the P versus NP problem. Commun. ACM **55**(6), 98–107 (2012)

[MV97] M. Mahajan, V. Vinay, Determinant: combinatorics, algorithms, and complexity. Chicago J. Theor. Comput. Sci. **5**, 730–738 (1997). (Conference version in SODA 1997)

[Nis92] N. Nisan, Pseudorandom generators for space-bounded computation. Combinatorica **12**(4), 449–461 (1992). (Conference version in STOC 1990)

[NN93] J. Naor, M, Naor, Small-bias probability spaces: efficient constructions and applications. SIAM J. Comput. **22**(4), 838–856 (1993). (Conference version in STOC 1990)

[RS05] R. Raz, A Shpilka, Deterministic polynomial identity testing in non-commutative models. Comput. Complex. **14**(1), 1–19 (2005). (Conference version in, CCC 2004)

[RY09] R. Raz, A. Yehudayoff, Lower bounds and separations for constant depth multilinear circuits. Comput. Complex. **18**(2), 171–207 (2009). (Conference version in, CCC 2008)

[Sap13] R. Saptharishi, Unified Approaches to Polynomial Identity Testing and Lower Bounds, Ph.D. thesis, Department of CSE, IIT Kanpur, India, Apr 2013

[Sax08] N. Saxena, Diagonal circuit identity testing, lower bound. ICALP **1**, 60–71 (2008)

[Sax09] N. Saxena, Progress on polynomial identity testing. Bull. EATCS **90**, 49–79 (2009)

[SS11] N. Saxena, C. Seshadhri, An almost optimal rank bound for depth-3 Identities. SIAM J. Comput. **40**(1), 200–224 (2011). (Conference version in, CCC 2009)

[SS12] N. Saxena, C. Seshadhri, Blackbox identity testing for bounded top-fanin depth-3 circuits: the field doesn't matter. SIAM J. Comput. **41**(5), 1285–1298 (2012). (Conference version in STOC 2011)

[SS13] N. Saxena, C. Seshadhri, From Sylvester-Gallai configurations to rank bounds: Improved blackbox identity test for depth-3 circuits. J. ACM **60**(5), 33 (2013). (Conference version in STOC 2010)

[SSS09] C. Saha, R. Saptharishi, N. Saxena, in *The Power of Depth 2 Circuits over Algebras* (FSTTCS, 2009), pp. 371–382

[SY10] A. Shpilka, A. Yehudayoff, Arithmetic Circuits, A survey of recent results and open questions. Found. Trends Theor. Comput. Sci. **5**(3–4), 207–388 (2010)

[Tav13] S. Tavenas, in *Improved Bounds for Reduction to Depth 4 and Depth 3* (MFCS, 2013), pp. 813–824

[Vad12] S.P. Vadhan, Pseudorandomness. Found. Trends Theor. Comput. Sci. **7**(1–3), 1–336 (2012)

[Val79] L.G. Valiant, in *Completeness classes in algebra* (STOC, 1979), pp. 249–261

[VSBR83] L.G. Valiant, S. Skyum, S.J. Berkowitz, C. Rackoff, Fast parallel computation of polynomials using few processors. SIAM J. Comput. **12**(4), 641–644 (1983)

[vzG83] J. von zur Gathen, *Factoring Sparse Multivariate Polynomials* (FOCS, 1983), pp. 172–179