Algebraic Independence and Blackbox Identity Testing*

Malte Beecken, Johannes Mittmann, and Nitin Saxena

Hausdorff Center for Mathematics, Bonn, Germany
{malte.beecken,johannes.mittmann,nitin.saxena}@hcm.uni-bonn.de

Abstract. Algebraic independence is an advanced notion in commutative algebra that generalizes independence of linear polynomials to higher degree. The transcendence degree (trdeg) of a set $\{f_1, \ldots, f_m\} \subset \mathbb{F}[x_1, \ldots, x_n]$ of polynomials is the maximal size r of an algebraically independent subset. In this paper we design blackbox and efficient linear maps φ that reduce the number of variables from n to r but maintain $\text{trdeg}\{\varphi(f_i)\}_i = r$, assuming f_i's sparse and small r. We apply these fundamental maps to solve several cases of blackbox identity testing:

1. Given a circuit C and sparse subcircuits $f_1, \ldots, f_m$ of trdeg r such that $D := C(f_1, \ldots, f_m)$ has polynomial degree, we can test blackbox D for zeroness in $\text{poly}(\text{size}(D))^r$ time.
2. Define a $\Sigma\Pi\Sigma\Pi_\delta(k, s, n)$ circuit C to be of the form $\sum_{i=1}^{k} \prod_{j=1}^{s} f_{i,j}$, where $f_{i,j}$ are sparse n-variate polynomials of degree at most δ. For $k = 2$, we give a $\text{poly}(\delta sn)^{\delta^2}$ time blackbox identity test.
3. For a general depth-4 circuit we define a notion of rank. Assuming there is a rank bound R for minimal simple $\Sigma\Pi\Sigma\Pi_\delta(k, s, n)$ identities, we give a $\text{poly}(\delta snR)^{Rk\delta^2}$ time blackbox identity test for $\Sigma\Pi\Sigma\Pi_\delta(k, s, n)$ circuits. This partially generalizes the state of the art of depth-3 to depth-4 circuits.

The notion of trdeg works best with large or zero characteristic, but we also give versions of our results for arbitrary fields.

1 Introduction

Polynomial identity testing (PIT) is the problem of checking whether a given n-variate arithmetic circuit computes the zero polynomial in $\mathbb{F}[x_1, \ldots, x_n]$. It is a central question in complexity theory as circuits model computation and PIT leads us to a better understanding of circuits. There are several classical randomized algorithms known [9,28,30,8,19,4] that solve PIT. The basic Schwartz-Zippel test is: Given a circuit $C(x_1, \ldots, x_n)$, check $C(\overline{a}) = 0$ for a random $\overline{a} \in \overline{\mathbb{F}}^n$. Finding a deterministic polynomial time test, however, has been more difficult and is currently open. Derandomization of PIT is well motivated by a host of algorithmic applications, eg. bipartite matching [20] and matrix completion [21], and

* The first two authors are grateful to the Bonn International Graduate School in Mathematics for research funding.

L. Aceto, M. Henzinger, and J. Sgall (Eds.): ICALP 2011, Part II, LNCS 6756, pp. 137–148, 2011.

connections to sought-after super-polynomial lower bounds [13,14]. Especially, *blackbox* PIT (i.e. circuit C is given as a blackbox and we could only make oracle queries) has direct connections to lower bounds for the permanent [2,3]. Clearly, finding a blackbox PIT test for a family of circuits $\mathcal{F}$ boils down to efficiently designing a *hitting set* $\mathcal{H} \subset \overline{\mathbb{F}}^n$ such that: Given a nonzero $C \in \mathcal{F}$, there exists an $\overline{a} \in \mathcal{H}$ that *hits* C, i.e. $C(\overline{a}) \neq 0$.

The attempts to solve blackbox PIT have focused on restricted circuit families. A natural restriction is *constant depth.* Agrawal & Vinay [5] showed that a blackbox PIT algorithm for depth-4 circuits would (almost) solve PIT for general circuits (and prove exponential circuit lower bounds for permanent). The currently known blackbox PIT algorithms work only for further restricted depth-3 and depth-4 circuits. The case of *bounded top fanin* depth-3 circuits has received great attention and has blackbox PIT algorithms [27]. The analogous case for depth-4 circuits is open. However, with the additional restriction of *multilinearity* on all the multiplication gates, there is a blackbox PIT algorithm [24]. The latter is somewhat subsumed by the PIT algorithms for constant-read multilinear formulas [6]. To save space we would not go into the rich history of PIT and instead refer to the survey [29].

A recurring theme in the blackbox PIT research on depth-3 circuits has been that of *rank.* If we consider a $\Sigma\Pi\Sigma(k,d,n)$ circuit $C = \sum_{i=1}^k \prod_{j=1}^d \ell_{i,j}$, where $\ell_{i,j}$ are linear forms in $\mathbb{F}[x_1, \ldots, x_n]$, then $\mathrm{rk}(C)$ is defined to be the linear rank of the set of forms $\{\ell_{i,j}\}_{i,j}$ each viewed as a vector in $\mathbb{F}^n$. This raises the natural question: Is there a generalized notion of rank for depth-4 circuits as well, and more importantly, one that is useful in blackbox PIT? We answer this question affirmatively in this paper. Our notion of rank is via *transcendence degree* (short, trdeg), which is a basic notion in commutative algebra. To show that this notion applies to PIT requires relatively advanced algebra and new tools that we build.

Consider polynomials $\{f_1, \ldots, f_m\}$ in $\mathbb{F}[x_1, \ldots, x_n]$. They are called *algebraically independent* (over $\mathbb{F}$) if there is no nonzero polynomial $F \in \mathbb{F}[y_1, \ldots, y_m]$ such that $F(f_1, \ldots, f_m) = 0$. When those polynomials are *algebraically dependent* then such an F exists and is called an *annihilating polynomial* of $f_1, \ldots, f_m$. The *transcendence degree*, $\mathrm{trdeg}\{f_1, \ldots, f_m\}$, is the maximal number r of algebraically independent polynomials in the set $\{f_1, \ldots, f_m\}$. Though intuitive, it is nontrivial to prove that r is at most n.

The notion of trdeg has appeared in complexity theory in several contexts. Kalorkoti [15] used it to prove an $\Omega(n^3)$ formula size lower bound for $n \times n$ determinant. In the works [10,11] studying the *entropy* of polynomial mappings $(f_1, \ldots, f_m) : \mathbb{F}^n \to \mathbb{F}^m$, trdeg is a natural measure of entropy when the field has large or zero characteristic. Finally, the complexity of the annihilating polynomial is studied in [17]. However, our work is the first to study trdeg in the context of PIT.

1.1 Our Main Results

Our first result shows that a general arithmetic circuit is sensitive to the trdeg of its input.

Theorem 1. *Let C be an m-variate circuit. Let $f_1, \ldots, f_m$ be ℓ-sparse, δ-degree, n-variate polynomials with trdeg r. Suppose we have oracle access to the n-variate d-degree circuit $C' := C(f_1, \ldots, f_m)$. There is a blackbox* $\mathrm{poly}(\mathrm{size}(C') \cdot d\ell\delta)^r$ *time test to check $C' = 0$ (assuming a zero or larger than δ^r characteristic).*

We also give an algorithm that works for all fields but has a worse time complexity. Note that the above theorem seems nontrivial even for a constant m, say $C' = C(f_1, f_2, f_3)$, as the output of C' may not be sparse and f_i's are of arbitrary degree and arity. In such a case r is constant too and the theorem gives a polynomial time test. Another example, where r is constant but both m and n are variable, is: $f_i := (x_1^i + x_2^2 + \cdots + x_n^2)x_n^i$ for $i \in [m]$. (Hint: $r \leq 3$.)

Our next two main results concern depth-4 circuits. We use the notation $\Sigma\Pi\Sigma\Pi_\delta(k, s, n)$ to denote circuits (over a field $\mathbb{F}$) of the form,

$$C := \sum_{i=1}^{k} \prod_{j=1}^{s} f_{i,j} \tag{1}$$

where $f_{i,j}$'s are sparse n-variate polynomials of maximal degree δ. Note that when $\delta = 1$ this notation agrees with that of a $\Sigma\Pi\Sigma$ circuit. Currently, the PIT methods are not even strong enough to study $\Sigma\Pi\Sigma\Pi_\delta(k, s, n)$ circuits with both *top* fanin k and *bottom* fanin δ *bounded*. It is in this spectrum that we make exciting progress.

Theorem 2. *Let C be a $\Sigma\Pi\Sigma\Pi_\delta(2, s, n)$ circuit over an arbitrary field. There is a blackbox* $\mathrm{poly}(\delta s n)^{\delta^2}$ *time test to check $C = 0$.*

Finally, we define a notion of rank for depth-4 circuits and show its usefulness. For a circuit C, as in (1), we define its *rank*, $\mathrm{rk}(C) := \mathrm{trdeg}\{f_{i,j} \mid i \in [k], j \in [s]\}$. Define $T_i := \prod_{j=1}^{s} f_{i,j}$, for all $i \in [k]$, to be the *multiplication terms* of C. We call C *simple* if $\{T_i | i \in [k]\}$ are coprime polynomials. We call C *minimal* if there is no $I \subsetneq [k]$ such that $\sum_{i \in I} T_i = 0$. Define $R_\delta(k, s)$ to be the smallest r such that: Any $\Sigma\Pi\Sigma\Pi_\delta(k, s, n)$ circuit C that is simple, minimal and zero has $\mathrm{rk}(C) < r$.

Theorem 3. *Let $r := R_\delta(k, s)$ and the characteristic be zero or larger than δ^r. There is a blackbox* $\mathrm{poly}(\delta r s n)^{rk\delta^2}$ *time identity test for $\Sigma\Pi\Sigma\Pi_\delta(k, s, n)$ circuits.*

We give a lower bound of $\Omega(\delta k \log s)$ on $R_\delta(k, s)$ and conjecture an upper bound (better than the trivial ks).

1.2 Organization and Our Approach

A priori it is not clear whether the problem of deciding algebraic independence of given polynomials $\{f_1, \ldots, f_m\}$, over a field $\mathbb{F}$, is even computable. Perron [22] proved that for $m = (n + 1)$ and any field, the annihilating polynomial has degree only exponential in n. We generalize this to any m in Sect. 2.1, hence, deciding algebraic independence (over any field) is computable (alternatively, Gröbner bases can be used). When the characteristic is zero or large, there is a more efficient criterion due to Jacobi (Sect. 2.2). For using trdeg in PIT we would need to relate it to the *Krull dimension* of algebras (Sect. 2.3).

The central concept that we develop is that of a *faithful homomorphism*. This is a linear map φ from $R := \mathbb{F}[x_1, \ldots, x_n]$ to $\mathbb{F}[z_1, \ldots, z_r]$ such that for polynomials $f_1, \ldots, f_m \in R$ of trdeg r, the images $\varphi(f_1), \ldots, \varphi(f_m)$ are also of trdeg r. Additionally, to be useful, φ should be constructible in a blackbox and efficient way. We give such constructions in Sects. 3.1 and 3.2. The proofs here use Perron's and Jacobi's criterion, but require new techniques as well. The reason why such a φ is useful in PIT is because it preserves the nonzeroness of the circuit $C(f_1, \ldots, f_m)$ (Theorem 11). We prove this by an elegant application of Krull's *principal ideal theorem*.

Once the fundamental machinery is set up, we prove Theorem 1 in Sect. 4 by designing a hitting set using the basic Schwartz-Zippel lemma.

Finally, we apply the faithful homomorphisms to depth-4 circuits. The proof of Theorem 2 is provided in Sect. 5.2 by showing that the maps also preserve gcd's. The rank-based hitting set is constructed in Sect. 5.3 proving Theorem 3.

Due to space constraints most of the proofs are omitted. They can be found in the full version of this paper [7].

2 Preliminaries: Perron, Jacobi and Krull

Let $n \in \mathbb{Z}^+$ and let K be a field of characteristic $\mathrm{ch}(K)$. Throughout this paper, $K[\boldsymbol{x}] = K[x_1, \ldots, x_n]$ is a polynomial ring in n variables over K. $\overline{K}$ denotes the *algebraic closure* of the field. We denote the multiplicative *group of units* of an algebra A by A^*. We use the notation $[n] := \{1, \ldots, n\}$. For $0 \leq r \leq n$, $\binom{[n]}{r}$ denotes the set of r-subsets of $[n]$.

2.1 Perron's Criterion (Arbitrary Characteristic)

An effective criterion for algebraic independence can be obtained by a degree bound for annihilating polynomials. The following theorem provides such a bound for the case of $n + 1$ polynomials in n variables.

Theorem 4 (Perron's theorem [23, Thm. 1.1]). *Let $f_i \in K[\boldsymbol{x}]$ be a polynomial of degree $\delta_i \geq 1$, for $i \in [n+1]$. Then there exists a non-zero polynomial $F \in K[y_1, \ldots, y_{n+1}]$ such that $F(f_1, \ldots, f_{n+1}) = 0$ and $\deg(F) \leq (\prod_i \delta_i)/\min_i\{\delta_i\}$.*

In the following corollary we give a degree bound in the general situation, where more variables than polynomials are allowed. Moreover, the bound is in terms of the trdeg of the polynomials instead of the number of variables. We hereby improve [17, Theorem 11] and generalize it to arbitrary characteristic.

Corollary 5 (Degree bound for annihilating polynomials). *Let $f_1, \ldots, f_m \in K[\boldsymbol{x}]$ be algebraically dependent polynomials of maximal degree δ and* trdeg *r. Then there exists a non-zero polynomial $F \in K[y_1, \ldots, y_m]$ of degree at most δ^r such that $F(f_1, \ldots, f_m) = 0$.*

2.2 Jacobi's Criterion (Large or Zero Characteristic)

In large or zero characteristic, the well-known Jacobian criterion yields a more efficient criterion for algebraic independence. The case of large characteristic was dealt with in [10]. By virtue of Theorem 4 our proof could tolerate a slightly smaller characteristic.

Theorem 6 (Jacobian criterion). *Let $f_1, \ldots, f_m \in K[\boldsymbol{x}]$ be polynomials of degree at most δ and* trdeg *r. Assume that* $\mathrm{ch}(K) = 0$ *or* $\mathrm{ch}(K) > \delta^r$*. Then* $\mathrm{rk}_L(\partial_{x_j} f_i)_{i,j} = r$*, where $L = K(\boldsymbol{x})$.*

2.3 Krull Dimension of Affine Algebras

In this section, we want to highlight the connection between transcendence degree and the Krull dimension of affine algebras. This will enable us to use Krull's principal ideal theorem which is stated below.

In this paper, a *K-algebra A* is always a commutative ring containing K as a subring. The most important example of a K-algebra is $K[\boldsymbol{x}]$. Let A, B be K-algebras. A map $A \to B$ is called a *K-algebra homomorphism* if it is a ring homomorphism that fixes K element-wise.

We want to extend the definition of algebraic independence to algebras. Let $a_1, \ldots, a_m \in A$ and consider the K-algebra homomorphism $\rho : K[\boldsymbol{y}] \to A$, $F \mapsto F(a_1, \ldots, a_m)$, where $K[\boldsymbol{y}] = K[y_1, \ldots, y_m]$. If $\ker(\rho) = \{0\}$, then $\{a_1, \ldots, a_m\}$ is called algebraically independent over K. If $\ker(\rho) \neq \{0\}$, then $\{a_1, \ldots, a_m\}$ is called algebraically dependent over K. For a subset $S \subseteq A$, we define $\mathrm{trdeg}_K S$ as the supremum of $|T|$ over all finite and algebraically independent $T \subseteq S$. The image of $K[\boldsymbol{y}]$ under ρ is the subalgebra of A generated by $a_1, \ldots, a_m$ and is denoted by $K[a_1, \ldots, a_m]$. An algebra of this form is called an *affine K-algebra*, and it is called an *affine K-domain* if it is an integral domain.

The *Krull dimension* of A, denoted by $\dim(A)$, is defined as the supremum over all $r \geq 0$ for which there is a chain $\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_r$ of prime ideals $\mathfrak{p}_i \subset A$. It measures how far A is from a field.

Theorem 7 (Dimension and trdeg [18, Prop. 5.10]). *Let $A = K[a_1, \ldots, a_m]$ be an affine K-algebra. Then* $\dim(A) = \mathrm{trdeg}_K A = \mathrm{trdeg}_K\{a_1, \ldots, a_m\}$.

Corollary 8. *Let A, B be K-algebras and let $\varphi : A \to B$ be a K-algebra homomorphism. If A is an affine algebra, then so is $\varphi(A)$ and we have* $\dim(\varphi(A)) \leq \dim(A)$*. If, in addition, φ is injective, then* $\dim(\varphi(A)) = \dim(A)$.

Theorem 9 (Krull's Hauptidealsatz [12, Cor. 13.11]). *Let A be an affine K-domain and let $a \in A \setminus (A^* \cup \{0\})$. Then* $\dim(A/\langle a \rangle) = \dim(A) - 1$.

3 Faithful Homomorphisms: Reducing the Variables

Let $f_1, \ldots, f_m \in K[\boldsymbol{x}]$ be polynomials and let $r := \mathrm{trdeg}\{f_1, \ldots, f_m\}$. Intuitively, r variables should suffice to define $f_1, \ldots, f_m$ without changing their algebraic relations. So let $K[\boldsymbol{z}] = K[z_1, \ldots, z_r]$ be a polynomial ring with $1 \le r \le n$. We want to find a homomorphism $K[\boldsymbol{x}] \to K[\boldsymbol{z}]$ that preserves the transcendence degree of $f_1, \ldots, f_m$. First we give this property a name.

Definition 10. Let $\varphi : K[\boldsymbol{x}] \to K[\boldsymbol{z}]$ be a K-algebra homomorphism. We say φ is *faithful to* $\{f_1, \ldots, f_m\}$ if $\operatorname{trdeg}\{\varphi(f_1), \ldots, \varphi(f_m)\} = \operatorname{trdeg}\{f_1, \ldots, f_m\}$.

The following theorem shows that a faithful homomorphism φ is useful for us. In particular, for a circuit C, we have $C(f_1, \ldots, f_m) = 0$ if and only if $\varphi(C(f_1, \ldots, f_m)) = 0$.

Theorem 11 (Faithful is useful). *Let $A = K[f_1, \ldots, f_m] \subseteq K[\boldsymbol{x}]$. Then φ is faithful to $\{f_1, \ldots, f_m\}$ if and only if $\varphi|_A : A \to K[\boldsymbol{z}]$ is injective.*

Proof. We denote $\varphi_A = \varphi|_A$ and $r = \operatorname{trdeg}\{f_1, \ldots, f_m\}$. If φ_A is injective, then $r = \dim(A) = \dim(\varphi_A(A)) = \operatorname{trdeg}\{\varphi(f_1), \ldots, \varphi(f_m)\}$ by Theorem 7 and Corollary 8. Thus φ is faithful to $\{f_1, \ldots, f_m\}$.

Conversely, let φ be faithful to $\{f_1, \ldots, f_m\}$. Then $\dim(\varphi_A(A)) = r$. Now assume for the sake of contradiction that φ_A is not injective. Then there exists an $f \in A \setminus \{0\}$ such that $\varphi_A(f) = 0$. We have $f \notin K$, because φ fixes K elementwise, and hence $f \notin A^* \cup \{0\}$. Since A is an affine domain, Theorem 9 implies $\dim(A/\langle f \rangle) = r - 1$. Since $f \in \ker(\varphi_A)$, the K-algebra homomorphism $\overline{\varphi}_A : A/\langle f \rangle \to K[\boldsymbol{z}]$, $a + \langle f \rangle \mapsto \varphi_A(a)$ is well-defined and φ_A factors as $\varphi_A = \overline{\varphi}_A \circ \eta$, where $\eta : A \to A/\langle f \rangle$ is the canonical surjection. But then Corollary 8 implies

$$r = \dim(\varphi_A(A)) = \dim(\overline{\varphi}_A(\eta(A))) \le \dim(\eta(A)) = \dim(A/\langle f \rangle) = r - 1 \ ,$$

a contradiction. It follows that φ_A is injective. □

3.1 A Kronecker-Inspired Map (Arbitrary Characteristic)

The following lemma shows that even *linear* faithful homomorphisms exist for all subsets of polynomials (provided K is large enough, for eg. move to $\overline{K}$ or a large enough field extension [1]). It is a generalization of [17, Claim 11.1] to arbitrary characteristic.

Lemma 12 (Existence). *Let K be an infinite field and let $f_1, \ldots, f_m \in K[\boldsymbol{x}]$ be polynomials of* trdeg *r. Then there exists a linear K-algebra homomorphism $\varphi : K[\boldsymbol{x}] \to K[\boldsymbol{z}]$ which is faithful to $\{f_1, \ldots, f_m\}$.*

Below we want to make this lemma effective. This will be accomplished by substituting constants for all but r of the variables $x_1, \ldots, x_n$. We define a parametrized homomorphism Φ in three steps. First, we decide which variables we want to keep and map them to $z_1, \ldots, z_r$. To the remaining variables we apply a *Kronecker substitution* using a new variable t, i.e. we map the i-th variable to t^{D^i} (for a large D). In the second step, the exponents of t will be reduced modulo some number. Finally, a constant will be substituted for t.

Let $I = \{j_1, \dots, j_r\} \in \binom{[n]}{r}$ be an index set and let $[n] \setminus I = \{j_{r+1}, \dots, j_n\}$ be its complement such that $j_1 < \dots < j_r$ and $j_{r+1} < \dots < j_n$. Let $D \geq 2$ and define the K-algebra homomorphism

$$\Phi_{I,D} : K[\boldsymbol{x}] \to K[t, \boldsymbol{z}], \qquad x_{j_i} \mapsto \begin{cases} z_i, & \text{for } i = 1, \dots, r, \\ t^{D^{i-r}}, & \text{for } i = r+1, \dots, n \end{cases} .$$

Now let $p \geq 1$. For an integer $a \in \mathbb{Z}$, we denote by $\lfloor a \rceil_p$ the integer $b \in \mathbb{Z}$ satisfying $0 \leq b < p$ and $a = b \pmod{p}$. We define the K-algebra homomorphism

$$\Phi_{I,D,p} : K[\boldsymbol{x}] \to K[t, \boldsymbol{z}], \qquad x_{j_i} \mapsto \begin{cases} z_i, & \text{for } i = 1, \dots, r, \\ t^{\lfloor D^{i-r} \rceil_p}, & \text{for } i = r+1, \dots, n \end{cases} .$$

Note that, for $f \in K[\boldsymbol{x}]$, $\Phi_{I,D,p}(f)$ is a representative of the residue class $\Phi_{I,D}(f) \pmod{\langle t^p - 1 \rangle_{K[t,\boldsymbol{z}]}}$. Finally let $c \in \overline{K}$ and define the $\overline{K}$-algebra homomorphism $\Phi_{I,D,p,c} : \overline{K}[\boldsymbol{x}] \to \overline{K}[\boldsymbol{z}]$, $f \mapsto \big(\Phi_{I,D,p}(f)\big)(c, \boldsymbol{z})$. The following lemma bounds the number of bad choices for the parameters p and c.

Lemma 13 (Φ is faithful). *Let $f_1, \dots, f_m \in K[\boldsymbol{x}]$ be polynomials of degree at most δ and* trdeg *at most r. Let $D > \delta^{r+1}$. Then there exist an index set $I \in \binom{[n]}{r}$ and a prime $p \leq (n + \delta^r)^{8\delta^{r+1}} (\log_2 D)^2 + 1$ such that any subset of $\overline{K}$ of size $\delta^r rp$ contains c such that $\Phi_{I,D,p,c}$ is faithful to $\{f_1, \dots, f_m\}$.*

In large or zero characteristic, a more efficient version of this lemma can be given (for the same homomorphism Φ). The reason is that we can work with the Jacobian criterion instead of the degree bound for annihilating polynomials. However, we omit the statement of this result here, because we can give a more holistic construction in that case. This will be presented in the following section.

3.2 A Vandermonde-Inspired Map (Large or Zero Characteristic)

To prove Theorem 3, we will need a homomorphism that is faithful to several sets of polynomials simultaneously. The homomorphism Φ constructed in the previous section does not meet this requirement, because its definition depends on a *fixed* subset of the variables $x_1, \dots, x_n$. In this section we will devise a construction, that treats the variables $x_1, \dots, x_n$ in a uniform manner. It is inspired by the *Vandermonde matrix*, i.e. $(t^{ij})_{i,j}$.

We define a parametrized homomorphism Ψ in three steps. Let $K[\boldsymbol{z}] = K[z_0, z_1, \dots, z_r]$, where $1 \leq r \leq n$. Let $D_1, D_2 \geq 2$ and let $D = (D_1, D_2)$. Define the K-algebra homomorphism

$$\Psi_D : K[\boldsymbol{x}] \to K[t, \boldsymbol{z}], \qquad x_i \mapsto t^{D_1^i} + t^{D_2^i} z_0 + \sum_{j=1}^{r} t^{i(n+1)^j} z_j \ ,$$

where $i = 1, \dots, n$. This map (linear in the z's) should be thought of as a variable reduction from n to $r + 1$. The coefficients of $z_1, \dots, z_r$ bear resemblance to a row of a Vandermonde matrix, while that of z_0 (and the constant coefficient) resembles Kronecker substitution. This definition is carefully tuned so that Ψ finally preserves both the trdeg (proven here) and gcd of polynomials (proven in Sect. 5.2). Next let $p \geq 1$ and define the K-algebra homomorphism

$$\Psi_{D,p} : K[\boldsymbol{x}] \to K[t, \boldsymbol{z}], \qquad x_i \mapsto t^{\lfloor D_1^i \rfloor_p} + t^{\lfloor D_2^i \rfloor_p} z_0 + \sum_{j=1}^{r} t^{\lfloor i(n+1)^j \rfloor_p} z_j \ ,$$

where $i = 1, \ldots, n$. Note that, for $f \in K[\boldsymbol{x}]$, $\Psi_{D,p}(f)$ is a representative of the residue class $\Psi_D(f) \pmod{\langle t^p - 1 \rangle_{K[t,\boldsymbol{z}]}}$. Finally let $c \in \overline{K}$ and define the $\overline{K}$-algebra homomorphism $\Psi_{D,p,c} : \overline{K}[\boldsymbol{x}] \to \overline{K}[\boldsymbol{z}]$, $f \mapsto \big(\Psi_{D,p}(f)\big)(c, \boldsymbol{z})$. The following lemma bounds the number of bad choices for the parameters p and c. The proof uses the Jacobian criterion, therefore the lemma has a restriction on $\mathrm{ch}(K)$.

Lemma 14 (Ψ is faithful). *Let $f_1, \ldots, f_m \in K[\boldsymbol{x}]$ be polynomials of sparsity at most ℓ, degree at most δ and* trdeg *at most r. Assume that $\mathrm{ch}(K) = 0$ or $\mathrm{ch}(K) > \delta^r$. Let $D = (D_1, D_2)$ such that $D_1 \geq \max\{\delta r + 1, (n+1)^{r+1}\}$ and $D_2 \geq 2$. Then there exists a prime $p \leq (2nr\ell)^{2(r+1)}(\log_2 D_1)^2 + 1$ such that any subset of $\overline{K}$ of size $\delta r p$ contains c such that $\Psi_{D,p,c}$ is faithful to $\{f_1, \ldots, f_m\}$.*

By trying larger p and c, we can find a Ψ that is faithful to several subsets of polynomials simultaneously. This is an advantage of Ψ over Φ, in addition to being more efficiently constructible.

4 Circuits with Sparse Inputs of Low Transcendence Degree (Proving Theorem 1)

We can now proceed with the first PIT application of faithful homomorphisms. We consider arithmetic circuits of the form $C(f_1, \ldots, f_m)$, where C is a circuit computing a polynomial in $K[\boldsymbol{y}] = K[y_1, \ldots, y_m]$ and $f_1, \ldots, f_m$ are subcircuits computing polynomials in $K[\boldsymbol{x}]$. Thus, $C(f_1, \ldots, f_m)$ computes a polynomial in the subalgebra $K[f_1, \ldots, f_m]$.

Let $C(f_1, \ldots, f_m)$ be of maximal degree d, and let $f_1, \ldots, f_m$ be of maximal degree δ, maximal sparsity ℓ and maximal transcendence degree r. First, we use the faithful homomorphism Ψ from Sect. 3.2 to transform $C(f_1, \ldots, f_m)$ into an r-variate circuit. Then a hitting set for r-variate degree-d polynomials, given by the classical Schwartz-Zippel lemma, is used. The final hitting set construction is efficient for r constant and ℓ, d polynomial in the input size.

Let $n, d, r, \delta, \ell \geq 1$ and let $K[\boldsymbol{z}] = K[z_0, z_1, \ldots, z_r]$. We introduce the following parameters. Define $D = (D_1, D_2)$ by $D_1 := (2\delta n)^{r+1}$ and $D_2 := 2$, and $p_{\max} := (2nr\ell)^{2(r+1)} \lceil \log_2 D_1 \rceil^2 + 1$. Pick arbitrary $H_1, H_2 \subset \overline{K}$ of sizes $\delta r p_{\max}$ resp. $d+1$. Finally, denote $\Psi_{D,p,c}^{(i)} := \Psi_{D,p,c}(x_i) \in \overline{K}[\boldsymbol{z}]$ for $i = 1, \ldots, n$ and define the subset

$$\mathcal{H}_{d,r,\delta,\ell} = \Big\{ \big(\Psi_{D,p,c}^{(1)}(\boldsymbol{a}), \ldots, \Psi_{D,p,c}^{(n)}(\boldsymbol{a})\big) \;\big|\; p \in [p_{\max}],\ c \in H_1,\ \boldsymbol{a} \in H_2^{r+1} \Big\} \subset \overline{K}^n \ .$$

The following theorem shows that, over large or zero characteristic, this is a hitting set for the class of circuits under consideration. A version of this theorem for arbitrary characteristic can be found in [7].

Theorem 15. *Assume that* $\mathrm{ch}(K) = 0$ *or* $\mathrm{ch}(K) > \delta^r$*. Then* $\mathcal{H}_{d,r,\delta,\ell}$ *is a hitting set for the class of degree-*d *circuits with inputs being* ℓ*-sparse, degree-*δ *subcircuits of* trdeg *at most* r*. It can be constructed in* $\mathrm{poly}(dr\delta\ell n)^r$ *time.*

5 Depth-4 Circuits with Bounded Top and Bottom Fanin

The second PIT application of faithful homomorphisms is for $\Sigma\Pi\Sigma\Pi_\delta(k, s, n)$ circuits. Our hitting set construction is efficient when the top fanin k and the bottom fanin δ are both bounded. Except for top fanin 2, our hitting set will be *conditional* in the sense that its efficiency depends on a good rank upper bound for depth-4 identities.

5.1 Gcd, Simple Parts and the Rank Bounds

Let $C = \sum_{i=1}^{k} \prod_{j=1}^{s} f_{i,j}$ be a $\Sigma\Pi\Sigma\Pi_\delta(k, s, n)$ circuit, as defined in Sect. 1.1. Note that the parameters bound the circuit degree, $\deg(C) \le \delta s$. We define $\mathcal{S}(C) := \{f_{i,j} \mid i \in [k] \text{ and } j \in [s]\}$. It is the set of *sparse polynomials* of C (wlog we assume them all to be nonzero). The following definitions are natural generalizations of the corresponding concepts for depth-3 circuits. Recall $T_i := \prod_j f_{i,j}$, for $i \in [k]$, are the multiplication terms of C. The *gcd part* of C is defined as $\gcd(C) := \gcd(T_1, \ldots, T_k)$ (we fix a unique representative among the associated gcds). The *simple part* of C is defined as $\mathrm{sim}(C) := C/\gcd(C) \in \Sigma\Pi\Sigma\Pi_\delta(k, s, n)$. For a subset $I \subseteq [k]$ we denote $C_I := \sum_{i\in I} T_i$.

Recall that if C is simple then $\gcd(C) = 1$ and if it is minimal then $C_I \ne 0$ for all non-empty $I \subsetneq [k]$. Also, recall that $\mathrm{rk}(C)$ is $\mathrm{trdeg}_K\, \mathcal{S}(C)$, and that $R_\delta(k, s)$ strictly upper bounds the rank of any minimal and simple $\Sigma\Pi\Sigma\Pi_\delta(k, s, n)$ identity. Clearly, $R_\delta(k, s)$ is at most $|\mathcal{S}(C)| \le ks$ (note: $\mathcal{S}(C)$ cannot all be independent in an identity). On the other hand, we could prove a lower bound on $R_\delta(k, s)$ by constructing identities.

From the simple and minimal $\Sigma\Pi\Sigma$ identities constructed in [26], we obtain the lower bound $R_1(k, s) = \Omega(k)$ if $\mathrm{ch}(K) = 0$, and $R_1(k, s) = \Omega(k \log_p s)$ if $\mathrm{ch}(K) = p > 0$. These identities can be lifted to $\Sigma\Pi\Sigma\Pi_\delta(k, s, n)$ identities by replacing each variable x_i by a product $x_{i,1} \cdots x_{i,\delta}$ of new variables. These examples demonstrate: $R_\delta(k, s) = \Omega(\delta k)$ if $\mathrm{ch}(K) = 0$, and $R_\delta(k, s) = \Omega(\delta k \log_p s)$ if $\mathrm{ch}(K) = p > 0$. This leads us to the following natural conjecture.

Conjecture 16. *We have* $R_\delta(k, s) = \mathrm{poly}(\delta k)$*, if* $\mathrm{ch}(K) = 0$*, and* $R_\delta(k, s) = \mathrm{poly}(\delta k \log_p s)$*, if* $\mathrm{ch}(K) = p > 0$.

The following lemma is a vast generalization of [16, Theorem 3.4] to depth-4 circuits. It suggests how a bound for $R_\delta(k, s)$ can be used to construct a hitting set for $\Sigma\Pi\Sigma\Pi_\delta(k,s,n)$ circuits. The φ in the statement below should be thought of as a linear map that reduces the number of variables from n to $R_\delta(k,s)+1$.

Lemma 17 (Rank is useful). *Let C be a $\Sigma\Pi\Sigma\Pi_\delta(k,s,n)$ circuit, let $r := R_\delta(k,s)$ and let $\varphi : K[\boldsymbol{x}] \to K[\boldsymbol{z}] = K[z_0,z_1,\dots,z_r]$ be a linear K-algebra homomorphism that, for all $I \subseteq [k]$, satisfies $\varphi(\mathrm{sim}(C_I)) = \mathrm{sim}(\varphi(C_I))$ and $\mathrm{rk}(\varphi(\mathrm{sim}(C_I))) \geq \min\{\mathrm{rk}(\mathrm{sim}(C_I)), R_\delta(k,s)\}$. Then $C = 0$ iff $\varphi(C) = 0$.*

5.2 Preserving the Simple Part (Towards Theorem 2)

The following lemma shows that Ψ meets the first condition of Lemma 17. This is also the heart of PIT when $k = 2$. The actual hitting set, though, we provide in the next subsection.

Lemma 18 (Ψ preserves the simple part). *Let C be a $\Sigma\Pi\Sigma\Pi_\delta(k,s,n)$ circuit. Let $D_1 \geq 2\delta^2+1$, let $D_1 \geq D_2 \geq \delta+1$ and let $D = (D_1,D_2)$. Then there exists a prime $p \leq (2ksn\delta^2)^{8\delta^2+2}(\log_2 D_1)^2+1$ such that any subset $S \subset \overline{K}$ of size $2\delta^4k^2s^2p$ contains c satisfying $\Psi_{D,p,c}(\mathrm{sim}(C)) = \mathrm{sim}(\Psi_{D,p,c}(C))$.*

5.3 A Hitting Set (Proving Theorems 2 and 3)

Armed with Lemmas 17 and 18 we could now complete the construction of the hitting set for $\Sigma\Pi\Sigma\Pi_\delta(k,s,n)$ circuits using the faithful homomorphism Ψ with the right parameters.

Let $n,\delta,k,s \geq 1$ and let $r = R_\delta(k,s)$. We introduce the following parameters. They are blown up so that they support 2^k applications (one for each $I \subseteq [k]$) of Lemmas 14 and 18. Define $D = (D_1,D_2)$ by $D_1 := (2\delta n)^{2r}$ and $D_2 := \delta+1$, and $p_{\max} := 2^{2(k+1)} \cdot (2krsn\delta^2)^{8\delta^2+4\delta r}\lceil\log_2 D_1\rceil^2+1$. Pick arbitrary $H_1, H_2 \subset \overline{K}$ of sizes $2^{k+2}k^2rs^2\delta^4p_{\max}$ resp. $\delta s+1$. Finally, denote $\Psi^{(i)}_{D,p,c} := \Psi_{D,p,c}(x_i) \in \overline{K}[\boldsymbol{z}]$ for $i = 1,\dots,n$ and define the subset

$$\mathcal{H}_{\delta,k,s} = \left\{ \left(\Psi^{(1)}_{D,p,c}(\boldsymbol{a}),\dots,\Psi^{(n)}_{D,p,c}(\boldsymbol{a})\right) \mid p \in [p_{\max}],\, c \in H_1,\, \boldsymbol{a} \in H_2^{r+1} \right\} \subset \overline{K}^n \ .$$

The following theorem shows that, over large or zero characteristic, this is a hitting set for $\Sigma\Pi\Sigma\Pi_\delta(k,s,n)$ circuits.

Theorem 19. *Assume that $\mathrm{ch}(K) = 0$ or $\mathrm{ch}(K) > \delta^r$. Then $\mathcal{H}_{\delta,k,s}$ is a hitting set for $\Sigma\Pi\Sigma\Pi_\delta(k,s,n)$ circuits. It can be constructed in $\mathrm{poly}(\delta rsn)^{\delta^2kr}$ time.*

Since trivially $R_\delta(2,s) = 1$, we obtain an explicit hitting set for the top fanin 2 case. Moreover, in this case we can also eliminate the dependence on the characteristic (because Lemma 18 is field independent).

Corollary 20. *Let K be of arbitrary characteristic. Then $\mathcal{H}_{\delta,2,s}$ is a hitting set for $\Sigma\Pi\Sigma\Pi_\delta(2,s,n)$ circuits. It can be constructed in $\mathrm{poly}(\delta sn)^{\delta^2}$ time.*

6 Conclusion

The notion of rank has been quite useful in depth-3 PIT. In this work we give the first generalization of it to depth-4 circuits. We used trdeg and developed fundamental maps – the faithful homomorphisms – that preserve trdeg of sparse polynomials in a blackbox and efficient way (assuming a small trdeg). Crucially, we showed that faithful homomorphisms preserve the nonzeroness of circuits.

Our work raises several open questions. The faithful homomorphism construction over a small characteristic has restricted efficiency, in particular, it is interesting only when the sparse polynomials have very low degree. Could Lemma 13 be improved to handle larger δ? In general, the classical methods stop short of dealing with small characteristic because the "geometric" Jacobian criterion is not there. We have given some new tools to tackle that, for eg., Corollary 5 and Lemmas 12 and 13. But more tools are needed, for eg. a homomorphism like that of Lemma 14 for arbitrary fields.

Currently, we do not know a better upper bound for $R_\delta(k,s)$ other than ks. For $\delta = 1$, it is just the rank of depth-3 identities, which is known to be $O(k^2 \log s)$ ($O(k^2)$ over $\mathbb{R}$) [25]. Even for $\delta = 2$ we leave the rank question open. We conjecture $R_2(k,s) = O_k(\log s)$ (generally, Conjecture 16). Our hope is that understanding these small δ identities should give us more potent tools to attack depth-4 PIT in generality.

References

1. Adleman, L.M., Lenstra, H.W.: Finding irreducible polynomials over finite fields. In: Proceedings of the 18th Annual ACM Symposium on Theory of Computing (STOC), pp. 350–355 (1986)
2. Agrawal, M.: Proving lower bounds via pseudo-random generators. In: Sarukkai, S., Sen, S. (eds.) FSTTCS 2005. LNCS, vol. 3821, pp. 92–105. Springer, Heidelberg (2005)
3. Agrawal, M.: Determinant versus permanent. In: Proceedings of the 25th International Congress of Mathematicians (ICM), vol. 3, pp. 985–997 (2006)
4. Agrawal, M., Biswas, S.: Primality and identity testing via Chinese remaindering. Journal of the ACM 50(4), 429–443 (2003)
5. Agrawal, M., Vinay, V.: Arithmetic circuits: A chasm at depth four. In: Proceedings of the 49th Annual Symposium on Foundations of Computer Science (FOCS), pp. 67–75 (2008)
6. Anderson, M., van Melkebeek, D., Volkovich, I.: Derandomizing polynomial identity testing for multilinear constant-read formulae. In: Proceedings of the 26th Annual IEEE Conference on Computational Complexity, CCC (2011)
7. Beecken, M., Mittmann, J., Saxena, N.: Algebraic Independence and Blackbox Identity Testing. Tech. Rep. TR11-022, Electronic Colloquium on Computational Complexity, ECCC (2011)
8. Chen, Z., Kao, M.: Reducing randomness via irrational numbers. SIAM J. on Computing 29(4), 1247–1256 (2000)
9. DeMillo, R.A., Lipton, R.J.: A probabilistic remark on algebraic program testing. Information Processing Letters 7(4), 193–195 (1978)
10. Dvir, Z., Gabizon, A., Wigderson, A.: Extractors and rank extractors for polynomial sources. Computational Complexity 18(1), 1–58 (2009)

11. Dvir, Z., Gutfreund, D., Rothblum, G., Vadhan, S.: On approximating the entropy of polynomial mappings. In: Proceedings of the 2nd Symposium on Innovations in Computer Science, ICS (2011)
12. Eisenbud, D.: Commutative Algebra with a View Toward Algebraic Geometry. Springer, New York (1995)
13. Heintz, J., Schnorr, C.P.: Testing polynomials which are easy to compute (extended abstract). In: Proceedings of the Twelfth Annual ACM Symposium on Theory of Computing, New York, NY, USA, pp. 262–272 (1980)
14. Kabanets, V., Impagliazzo, R.: Derandomizing polynomial identity tests means proving circuit lower bounds. Computational Complexity 13(1), 1–46 (2004)
15. Kalorkoti, K.: A lower bound for the formula size of rational functions. SIAM J. Comp. 14(3), 678–687 (1985)
16. Karnin, Z., Shpilka, A.: Deterministic black box polynomial identity testing of depth-3 arithmetic circuits with bounded top fan-in. In: Proceedings of the 23rd Annual Conference on Computational Complexity (CCC), pp. 280–291 (2008)
17. Kayal, N.: The Complexity of the Annihilating Polynomial. In: Proceedings of the 24th Annual IEEE Conference on Computational Complexity (CCC), pp. 184–193 (2009)
18. Kemper, G.: A Course in Commutative Algebra. Springer, Berlin (2011)
19. Lewin, D., Vadhan, S.: Checking polynomial identities over any field: Towards a derandomization? In: Proceedings of the 30th Annual Symposium on the Theory of Computing (STOC), pp. 428–437 (1998)
20. Lovász, L.: On determinants, matchings and random algorithms. In: Fundamentals of Computation Theory (FCT), pp. 565–574 (1979)
21. Lovász, L.: Singular spaces of matrices and their applications in combinatorics. Bol. Soc. Braz. Mat. 20, 87–99 (1989)
22. Perron, O.: Algebra I (Die Grundlagen). Berlin (1927)
23. Płoski, A.: Algebraic Dependence of Polynomials After O. Perron and Some Applications. In: Cojocaru, S., Pfister, G., Ufnarovski, V. (eds.) Computational Commutative and Non-Commutative Algebraic Geometry, pp. 167–173. IOS Press, Amsterdam (2005)
24. Saraf, S., Volkovich, I.: Black-box identity testing of depth-4 multilinear circuits. In: Proceedings of the 43rd ACM Symposium on Theory of Computing, STOC (2011)
25. Saxena, N., Seshadhri, C.: From Sylvester-Gallai configurations to rank bounds: Improved black-box identity test for depth-3 circuits. In: Proceedings of the 51st Annual Symposium on Foundations of Computer Science (FOCS), pp. 21–29 (2010)
26. Saxena, N., Seshadhri, C.: An Almost Optimal Rank Bound for Depth-3 Identities. SIAM J. Comp. 40(1), 200–224 (2011)
27. Saxena, N., Seshadhri, C.: Blackbox identity testing for bounded top fanin depth-3 circuits: the field doesn't matter. In: Proceedings of the 43rd ACM Symposium on Theory of Computing, STOC (2011)
28. Schwartz, J.T.: Fast probabilistic algorithms for verification of polynomial identities. Journal of the ACM 27(4), 701–717 (1980)
29. Shpilka, A., Yehudayoff, A.: Arithmetic Circuits: A survey of recent results and open questions. Foundations and Trends in Theoretical Computer Science 5(3-4), 207–388 (2010)
30. Zippel, R.: Probabilistic algorithms for sparse polynomials. In: Ng, K.W. (ed.) EUROSAM 1979 and ISSAC 1979. LNCS, vol. 72, pp. 216–226. Springer, Heidelberg (1979)