Electronic Colloquium on Computational Complexity, Report No. 22 (2011)

Algebraic Independence and Blackbox Identity Testing

Malte Beecken Johannes Mittmann 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. Polynomials $\{f_1, \ldots, f_m\} \subset \mathbb{F}[x_1, \ldots, x_n]$ are called algebraically independent if there is no non-zero polynomial F such that $F(f_1, \ldots, f_m) = 0$. The transcendence degree, $\mathrm{trdeg}\{f_1, \ldots, f_m\}$, is the maximal number r of algebraically independent polynomials in the set. In this paper we design blackbox and efficient linear maps φ that reduce the number of variables from n to r but maintain $\mathrm{trdeg}\{\varphi(f_i)\}_i = r$, assuming f_i's sparse and small r. We apply these fundamental maps to solve several cases of blackbox identity testing:

1. Given a polynomial-degree circuit C and sparse polynomials $f_1, \ldots, f_m$ with trdeg r, we can test blackbox $D := C(f_1, \ldots, f_m)$ for zeroness in $\mathrm{poly}(\mathrm{size}(D))^r$ 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 $\mathrm{poly}(\delta sn)^{\delta^2}$ 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 $\mathrm{poly}(\delta snR)^{Rk\delta^2}$ 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.

Keywords: Algebraic independence, transcendence degree, arithmetic circuits, polynomial identity testing, blackbox algorithms, depth-4 circuits.

ISSN 1433-8092

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 [DL78, Sch80, Zip79, CK00, LV98, AB03] 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 [Lov79] and matrix completion [Lov89], and connections to sought-after super-polynomial lower bounds [HS80, KI04]. 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 [Agr05, Agr06]. 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 [AV08] 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 [DS06, KS07, KS08, SS, KS09, SS10, SS11]. 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 [KMSV10, SV11]. The latter is somewhat subsumed by the PIT algorithms for constant-read multilinear formulas [AvMV10]. To save space we would not go into the rich history of PIT and instead refer to the surveys [Sax09, SY10].

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 the *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 [Mor96]. The notion of trdeg has appeared in complexity theory in several contexts. Kalorkoti [Kal85] used trdeg to prove an $\Omega(n^3)$ formula size lower bound for $n \times n$ determinant. In the works [DGW09, DGRV11] 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. It also appears implicitly in [Dvi09] while constructing *extractors* for varieties. Finally, the complexity of the annihilating polynomial is studied in [Kay09]. 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. By $\Sigma\Pi\Sigma\Pi_\delta(k, s, n)$ we 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* $\mathrm{poly}(\delta sn)^{\delta^2}$ *time test to check $C = 0$.*

Simple, minimal and rank 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 $\{T_i \mid i \in [k]\}$ 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 $\mathrm{poly}(\delta rsn)^{rk\delta^2}$ 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 [Per27] 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. 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 $C(f_1,\ldots,f_m)$ (Corollary 13). We prove this by an elegant application of Krull's *principal ideal theorem*.

Once the fundamental machinery is set up, we prove Theorem 1 by designing a hitting set. The zero or large characteristic case is handled in Sect. 4.1. The arbitrary characteristic case is in Sect. 4.2.

Finally, we apply the faithful homomorphisms to depth-4 circuits. The proof of Theorem 2 is provided in Sect. 5.2. The rank-based hitting set is constructed in Sect. 5.3 proving Theorem 3. The full proofs tend to be extremely technical and have been moved to the appendix.

2 Preliminaries: Perron, Jacobi & 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 $0 \le r \le n$, $\binom{[n]}{r}$ denotes the set of r-subsets of $[n]$.

2.1 Perron's criterion (arbitrary field)

Let $f_1, \ldots, f_m \in K[\boldsymbol{x}]$ be polynomials. When we want to emphasize the base field with the transcendence degree, we would use the notation $\operatorname{trdeg}_K\{f_1, \ldots, f_m\}$. It is interesting to note that transcendence degree is invariant to *algebraic* field extensions, i.e. $\operatorname{trdeg}_K\{f_1, \ldots, f_m\}$ is the same as $\operatorname{trdeg}_{\overline{K}}\{f_1, \ldots, f_m\}$ (Lemma 27). The name transcendence degree stems from field theory. The transcendence degree of a field extension L/K, denoted by $\operatorname{trdeg}(L/K)$, is the cardinality of any transcendence basis for L/K (for more information on transcendental extensions, see [Mor96, Chap. 19]). For $L = K(f_1, \ldots, f_m)$, we have $\operatorname{trdeg}_K\{f_1, \ldots, f_m\} = \operatorname{trdeg}(L/K)$ (cf. [Mor96, Theorem 19.14]). Since $\operatorname{trdeg}(K(\boldsymbol{x})/K) = n$, we obtain $0 \le \operatorname{trdeg}_K\{f_1, \ldots, f_m\} \le n$.

Algebraic independence over K strongly resembles K-linear independence. In fact, algebraic independence makes a finite subset $\{f_1, \ldots, f_m\} \subset K[\boldsymbol{x}]$ into a *matroid* (a generalization of vector space, cf. [Oxl06, Sect. 6.7]).

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)**.** [Pło05, Theorem 1.1] *Let $f_i \in K[\boldsymbol{x}]$ be a polynomial of degree $\delta_i \ge 1$, 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 $\deg(F) \le (\prod_i \delta_i)/\min_i\{\delta_i\}$.*

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 [Kay09, Theorem 11] and generalize it to arbitrary characteristic. The proof uses a result from Sect. 3 and is given in Appendix A.1.

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

Proof sketch. In Lemma 14 we construct a homomorphism (by first principles) that reduces the number of variables to r and preserves the trdeg. We can then invoke Perron's theorem on $r+1$ of the polynomials. □

Remark. The bound in Corollary 5 is tight. To see this, let $n \ge 2$, let $\delta \ge 1$ and define the polynomials, $f_1 := x_1$, $f_2 := x_2 - x_1^\delta$, $\ldots$, $f_n := x_n - x_{n-1}^\delta$, $f_{n+1} := x_n^\delta$ in $K[\boldsymbol{x}]$. Then $\operatorname{trdeg}\{f_1, \ldots, f_{n+1}\} = n$ and every annihilating polynomial of $f_1, \ldots, f_{n+1}$ has degree at least δ^n.

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.

For $i \in [n]$, we denote the i-th formal partial derivative of a polynomial $f \in K[\boldsymbol{x}]$ by $\partial_{x_i} f$. Now let $f_1, \ldots, f_m \in K[\boldsymbol{x}]$. Then

$$J_{\boldsymbol{x}}(f_1, \ldots, f_m) := \big(\partial_{x_j} f_i\big)_{i,j} = \begin{pmatrix} \partial_{x_1} f_1 & \cdots & \partial_{x_n} f_1 \\ \vdots & & \vdots \\ \partial_{x_1} f_m & \cdots & \partial_{x_n} f_m \end{pmatrix} \in K[\boldsymbol{x}]^{m \times n}$$

is called the *Jacobian matrix* of $f_1, \ldots, f_m$. Its matrix-rank over the function field is of great interest.

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* $\mathrm{rk}_L\, J_{\boldsymbol{x}}(f_1, \ldots, f_m) = \mathrm{trdeg}_K\{f_1, \ldots, f_m\}$*, where $L = K(\boldsymbol{x})$.*

A proof of the Jacobian criterion in characteristic 0 appears, for example, in [ER93] and the case of large prime characteristic was dealt with in [DGW09]. By virtue of Theorem 4 our proof could tolerate a slightly smaller characteristic. For the reader's convenience, a full proof is given in Appendix A.2. We isolate the following special case of Theorem 6, because it holds in arbitrary characteristic.

Lemma 7. *Let $f_1, \ldots, f_m \in K[\boldsymbol{x}]$. Then* $\mathrm{trdeg}_K\{f_1, \ldots, f_m\} \geq \mathrm{rk}_L\, J_{\boldsymbol{x}}(f_1, \ldots, f_m)$*, 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 (whose elements may not be the usual polynomials any more). Let $a_1, \ldots, a_m \in A$ and consider the K-algebra homomorphism

$$\rho : K[\boldsymbol{y}] \to A, \qquad F \mapsto F(a_1, \ldots, a_m),$$

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 the transcendence degree of S over K by an obvious supremum:

$$\mathrm{trdeg}_K(S) := \sup\big\{|T| \mid T \subseteq S \text{ is finite and algebraically independent}\big\}.$$

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 8 (Dimension and trdeg)**.** *Let $A = K[a_1, \ldots, a_m]$ be an affine K-algebra. Then* $\dim(A) = \operatorname{trdeg}_K(A) = \operatorname{trdeg}_K\{a_1, \ldots, a_m\}$.

Proof. Cf. [Kem11, Theorem 5.9 and Proposition 5.10]. Also, the integral domain case is in the standard text [Mat89, Theorem 5.6]. □

The following corollary is a simple consequence of Theorem 8. It shows that homomorphisms cannot increase the dimension of affine algebras. The proof is given in Appendix A.3.

Corollary 9. *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* $\dim(\varphi(A)) = \dim(A)$.

In the next section we will need the following version of Krull's principal ideal theorem.

Theorem 10 (Krull's Hauptidealsatz)**.** *Let A be an affine K-domain and let $a \in A \setminus (A^* \cup \{0\})$. Then* $\dim(A/\langle a \rangle) = \dim(A) - 1$.

Proof. Cf. [Eis95, Corollary 13.11] or [Mat89, Theorem 13.5]. □

3 Faithful homomorphisms: Reducing the variables

Let $f_1, \ldots, f_m \in K[\boldsymbol{x}]$ be polynomials and let $r := \operatorname{trdeg}\{f_1, \ldots, f_m\}$. 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 $1 \leq r \leq n$. 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 11. 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 faithful homomorphisms are useful for us.

Theorem 12 (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 (iff $A \cong K[\varphi(f_1), \ldots, \varphi(f_m)]$).*

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 8 and Corollary 9. 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 element-wise, and hence $f \notin A^*$. Since A is an affine domain, Theorem 10 implies $\dim(A/\langle f\rangle) = r - 1$. Since $f \in \ker(\varphi_A)$, the K-algebra homomorphism

$$\overline{\varphi}_A : A/\langle f\rangle \to K[\boldsymbol{z}], \qquad a + \langle f\rangle \mapsto \varphi_A(a)$$

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 9 implies

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

a contradiction. It follows that φ_A is injective.

When φ_A is injective, clearly we have $A \cong \varphi_A(A) = K[\varphi(f_1), \ldots, \varphi(f_m)]$. ☐

Corollary 13. *Let C be an m-variate circuit over K. Let φ be faithful to $\{f_1, \ldots, f_m\} \subset K[\boldsymbol{x}]$. Then, $C(f_1, \ldots, f_m) = 0$ iff $C(\varphi(f_1), \ldots, \varphi(f_m)) = 0$.*

Proof. Note that $C(f_1, \ldots, f_m)$ resp. $C(\varphi(f_1), \ldots, \varphi(f_m))$ are elements in the algebras $K[f_1, \ldots, f_m]$ resp. $K[\varphi(f_1), \ldots, \varphi(f_m)]$. Since φ is an isomorphism between these two algebras, the corollary is evident. ☐

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 [AL86]). It is a generalization of [Kay09, Claim 11.1] to arbitrary characteristic. The proof is given in Appendix B.1.

Lemma 14 (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 $\{f_1, \ldots, f_m\}$.*

Proof sketch. We prove this by first principles. The proof is by identifying r variables from $\{x_1, \ldots, x_n\}$ that we leave *free* and the rest $n-r$ variables we fix to generic elements from K. Using annihilating polynomials we could show that this map preserves the trdeg. ☐

Below we want to make this lemma effective. This will again 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 single constant will be substituted for t.

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

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

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

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

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

$$\Phi_{I,D,p,c} : \overline{K}[\boldsymbol{x}] \to \overline{K}[\boldsymbol{z}], \qquad f \mapsto \big(\Phi_{I,D,p}(f)\big)(c, \boldsymbol{z}).$$

The following lemma bounds the number of bad choices for the parameters p and c. It is proven in Appendix B.1.

Lemma 15 (Φ is faithful)**.** *Let $f_1, \ldots, f_m \in K[\boldsymbol{x}]$ 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 $\{f_1, \ldots, f_m\}$.*

Proof sketch. We identify a maximal $I \subseteq [n]$ such that for the field $L := K(x_i \mid i \notin I)$, $\operatorname{trdeg}_L\{f_1, \ldots, f_m\} = \operatorname{trdeg}_K\{f_1, \ldots, f_m\}$. Now x_i, for $i \in I$, is algebraic over the field $L(f_1, \ldots, f_m)$. This gives us annihilating polynomials whose degrees we could bound by Corollary 5, and hence their sparsities. By sparse PIT tricks we get a bound on the 'good' p and c. ∎

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 $x_1, \ldots, x_n$. In this section we will devise a construction, that treats the variables $x_1, \ldots, x_n$ 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 $K[\boldsymbol{z}] = K[z_0, \ldots, z_r]$, where $1 \le r \le n$. Let $D_1, D_2 \ge 2$ 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 $i = 1, \ldots, n$. This map (linear in the z's) should be thought of as a variable reduction from n to $r+1$. The coefficients of $z_1, \ldots, z_r$ 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 $p \ge 1$ 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

$$\Psi_{D,p,c} : \overline{K}[\boldsymbol{x}] \to \overline{K}[\boldsymbol{z}], \qquad f \mapsto \big(\Psi_{D,p}(f)\big)(c, \boldsymbol{z}).$$

The following lemma bounds the number of bad choices for the parameters p and c. The proof, which is given in Appendix B.2, uses the Jacobian criterion, therefore the lemma has a restriction on $\mathrm{ch}(K)$.

Lemma 16 (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 $D_1 \ge \max\{\delta r + 1, (n+1)^{r+1}\}$ and $D_2 \ge 2$. Then there exists a prime $p \le (2nr\ell)^{2(r+1)}(\log_2 D_1)^2 + 1$ such that any subset of $\overline{K}$ of size $\delta r p$ contains c such that $\Psi_{D,p,c}$ is faithful to $\{f_1, \ldots, f_m\}$.*

Proof sketch. We study the action of Ψ_D on the Jacobian determinant. Because of the chain rule of partial derivatives, this leads us to a product of two determinants, which we expand using the Cauchy-Binet formula and estimate its sparsity. By sparse PIT tricks we get a bound on the 'good' p and c. ∎

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 a faithful homomorphism to transform $C(f_1, \ldots, f_m)$ into an r-variate circuit. Then, a hitting set for r-variate degree-d polynomials is used, given by the following version of the Schwartz-Zippel lemma.

Lemma 17 (Schwartz-Zippel)**.** *Let $H \subset \overline{K}$ be a subset of size $d + 1$. Then $\mathcal{H} = H^r$ is a hitting set for $\{f \in K[z_1, \ldots, z_r] \mid \deg(f) \leq d\}$.*

Proof. Cf. [Alo99, Lemma 2.1]. $\square$

4.1 A hitting set (large or zero characteristic)

We use the map Ψ from Sect. 3.2. This 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.

1. Define $D = (D_1, D_2)$ by $D_1 := (2\delta n)^{r+1}$ and $D_2 := 2$.
2. Define $p_{\max} := (2nr\ell)^{2(r+1)} \lceil \log_2 D_1 \rceil^2 + 1$.
3. Pick arbitrary $H_1, H_2 \subset \overline{K}$ of sizes $\delta r p_{\max}$ resp. $d + 1$.

Denote $\Psi^{(i)}_{D,p,c} := \Psi_{D,p,c}(x_i) \in \overline{K}[\boldsymbol{z}]$ for $i = 1, \ldots, n$ and define the subset

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

The following theorem shows that, over a large or zero characteristic, this is a hitting set for the class of circuits under consideration. A proof is given in Appendix C.1.

Theorem 18. *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.*

4.2 A hitting set (arbitrary characteristic)

We use the map Φ from Sect. 3.1. This hitting set construction is efficient for δ, r constants and d polynomial in the input size.

Let $n, d, r, \delta \geq 1$ and let $K[\boldsymbol{z}] = K[z_1, \ldots, z_r]$. We introduce the following parameters.

1. Define $D := \delta^{r+1} + 1$.
2. Define $p_{\max} := (n + \delta^r)^{8\delta^{r+1}} \lceil \log_2 D \rceil^2 + 1$.
3. Pick arbitrary $H_1, H_2 \subset \overline{K}$ of sizes $\delta^r r p_{\max}$ resp. $d + 1$.

Denote $\Phi^{(i)}_{I,D,p,c} := \Phi_{I,D,p,c}(x_i) \in \overline{K}[\boldsymbol{z}]$ for $i = 1, \ldots, n$ and define the subset

$$\mathcal{H}_{d,r,\delta} = \left\{ \left(\Phi^{(1)}_{I,D,p,c}(\boldsymbol{a}), \ldots, \Phi^{(n)}_{I,D,p,c}(\boldsymbol{a})\right) \,\middle|\, I \in \tbinom{[n]}{r},\, p \in [p_{\max}],\, c \in H_1,\, \boldsymbol{a} \in H_2^r \right\} \subset \overline{K}^n.$$

The following theorem shows that this is a hitting set for the class of circuits under consideration. A proof is given in Appendix C.2.

Theorem 19. *The set $\mathcal{H}_{d,r,\delta}$ is a hitting set for the class of degree-d circuits with inputs being degree-δ subcircuits of transcendence degree at most r. It can be constructed in* $\operatorname{poly}(dr\delta n)^{r\delta^{r+1}}$ *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, $\deg(C) \leq \delta s$. We define an $\mathcal{S}(\cdot)$ operator as:

$$\mathcal{S}(C) := \left\{ f_{i,j} \mid i \in [k] \text{ and } j \in [s] \right\} \subset K[\boldsymbol{x}].$$

It gives 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 $\operatorname{sim}(C) := C/\gcd(C) \in \Sigma\Pi\Sigma\Pi_\delta(k, s, n)$. 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 $C_I \neq 0$ 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 $|\mathcal{S}(C)| \leq ks$ (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 [SS], 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 20. *We conjecture*

$$R_\delta(k,s) = \begin{cases} \mathrm{poly}(\delta k), & \text{if } \mathrm{ch}(K) = 0, \\ \mathrm{poly}(\delta k \log s), & \text{otherwise.} \end{cases}$$

The following lemma is a vast generalization of [KS08, 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 21 (Rank is useful)**.** *Let C be a $\Sigma\Pi\Sigma\Pi_\delta(k,s,n)$ circuit, let $r := R_\delta(k,s)$ and let $\varphi : K[\boldsymbol{x}] \to K[\boldsymbol{z}] = K[z_0, z_1, \ldots, z_r]$ be a linear K-algebra homomorphism that, for all $I \subseteq [k]$, satisfies:*

1. *$\varphi(\mathrm{sim}(C_I)) = \mathrm{sim}(\varphi(C_I))$, and*
2. *$\mathrm{rk}(\varphi(\mathrm{sim}(C_I))) \geq \min\{\mathrm{rk}(\mathrm{sim}(C_I)), R_\delta(k,s)\}$.*

Then $C = 0$ if and only if $\varphi(C) = 0$.

Proof. If $C = 0$, then clearly $\varphi(C) = 0$. Conversely, let $\varphi(C) = 0$. Let $I \subseteq [k]$ be a non-empty subset such that $\varphi(C_I)$ is a minimal circuit computing the zero polynomial. Then, by assumption (1.), $\varphi(\mathrm{sim}(C_I)) = \mathrm{sim}(\varphi(C_I)) \in \Sigma\Pi\Sigma\Pi_\delta(k,s,n)$ is a minimal and simple circuit computing the zero polynomial. Hence, $\mathrm{rk}(\varphi(\mathrm{sim}(C_I))) < R_\delta(k,s)$. By assumption (2.), this implies $\mathrm{rk}(\varphi(\mathrm{sim}(C_I))) = \mathrm{rk}(\mathrm{sim}(C_I))$, thus φ is faithful to $\mathcal{S}(\mathrm{sim}(C_I))$. Theorem 12 yields $\mathrm{sim}(C_I) = 0$, hence $C_I = 0$. Since $\varphi(C)$ is the sum of zero and minimal circuits $\varphi(C_I)$ for some $I \subseteq [k]$, we obtain $C = 0$ as required. $\square$

5.2 Preserving the simple part (towards Theorem 2)

The following lemma shows that Ψ meets condition (1.) of Lemma 21. The proof is given in Appendix D.1. This is also the heart of PIT when $k = 2$. The actual hitting set, though, we provide in the next subsection.

Lemma 22 (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 $2\delta^4 k^2 s^2 p$ contains c satisfying $\Psi_{D,p,c}(\mathrm{sim}(C)) = \mathrm{sim}(\Psi_{D,p,c}(C))$.*

Proof sketch. For any coprime $f_i, f_j \in \mathcal{S}(C)$ we look at their images under Ψ. We view $\Psi(f_i)$ and $\Psi(f_j)$ as univariates wrt z_0 and fix $z_1 = \cdots = z_r = 0$. If we could keep these two univariates monic (before the fixing) and their resultants nonzero (after the fixing), then the coprimality of $\Psi(f_i)$ and $\Psi(f_j)$ would be ensured. Both those requirements are fulfilled by estimating the sparsity and using sparse PIT tricks. $\square$

5.3 A hitting set (proving Theorems 2 & 3)

Armed with Lemmas 21 and 22 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 $I \subset [k]$) of Lemmas 16 and 22.

1. Define $D = (D_1, D_2)$ by $D_1 := (2\delta n)^{2r}$ and $D_2 := \delta + 1$.
2. Define $p_{\max} := 2^{2(k+1)} \cdot (2krsn\delta^2)^{8\delta^2+4\delta r}\lceil \log_2 D_1 \rceil^2 + 1$.
3. Pick arbitrary $H_1, H_2 \subset \overline{K}$ of sizes $2^{k+2}k^2rs^2\delta^4 p_{\max}$ resp. $\delta s+1$.

Denote $\Psi^{(i)}_{D,p,c} := \Psi_{D,p,c}(x_i) \in \overline{K}[\boldsymbol{z}]$ for $i=1,\ldots,n$ and define the subset

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

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

Theorem 23. *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 $\mathrm{poly}(\delta rsn)^{\delta^2 kr}$ 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 22 is field independent).

Corollary 24. *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.*

A proof of the theorem and the corollary can be found in Appendix D.2.

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 15 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 14 and 15. But more tools are needed, for eg. a homomorphism like that of Lemma 16 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 $\mathbb{R}$) [SS10]. Even for $\delta = 2$ we leave the rank question open. We conjecture $R_2(k,s) = O_k(\log s)$ (generally, Conjecture 20). Our hope is that understanding these small δ identities should give us more potent tools to attack depth-4 PIT in generality.

Acknowledgements We are grateful to the Hausdorff Center for Mathematics, Bonn, for its kind support. The first two authors would also like to thank the Bonn International Graduate School in Mathematics for research funding.

References

[AB03] M. Agrawal and S. Biswas. Primality and identity testing via Chinese remaindering. *Journal of the ACM*, 50(4):429–443, 2003. (Conference version in FOCS 1999).

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

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

[AL86] L. M. Adleman and H. W. Lenstra. Finding irreducible polynomials over finite fields. In *Proceedings of the 18th Annual ACM Symposium on Theory of Computing (STOC)*, pages 350–355, 1986.

[Alo99] N. Alon. Combinatorial Nullstellensatz. *Combinatorics, Probability and Computing*, 8:7–29, 1999.

[AV08] M. Agrawal and V. Vinay. Arithmetic circuits: A chasm at depth four. In *Proceedings of the 49th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 67–75, 2008.

[AvMV10] M. Anderson, D. van Melkebeek, and I. Volkovich. Derandomizing polynomial identity testing for multilinear constant-read formulae. Technical Report TR10-135, ECCC, 2010.

[BHLV09] M. Bläser, M. Hardt, R. J. Lipton, and N. K. Vishnoi. Deterministically testing sparse polynomial identities of unbounded degree. *Information Processing Letters*, 109(3):187–192, 2009.

[CK00] Z. Chen and M. Kao. Reducing randomness via irrational numbers. *SIAM J. on Computing*, 29(4):1247–1256, 2000. (Conference version in STOC 1997).

[CLO97] D. Cox, J. Little, and D. O'Shea. *Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra*. Springer-Verlag, New York, second edition, 1997.

[DGRV11] Z. Dvir, D. Gutfreund, G. Rothblum, and S. Vadhan. On approximating the entropy of polynomial mappings. In *Proceedings of the 2nd Symposium on Innovations in Computer Science (ICS)*, 2011.

[DGW09] Z. Dvir, A. Gabizon, and A. Wigderson. Extractors and rank extractors for polynomial sources. *Computational Complexity*, 18(1):1–58, 2009. (Conference version in FOCS 2007).

[DL78] Richard A. DeMillo and Richard J. Lipton. A probabilistic remark on algebraic program testing. *Information Processing Letters*, 7(4):193–195, 1978.

[DS06] Z. Dvir and A. Shpilka. Locally decodable codes with 2 queries and polynomial identity testing for depth 3 circuits. *SIAM J. on Computing*, 36(5):1404–1434, 2006. (Conference version in STOC 2005).

[Dvi09] Z. Dvir. Extractors for varieties. In *Proceedings of the 24th Annual IEEE Conference on Computational Complexity (CCC)*, pages 102–113, 2009.

[Eis95] D. Eisenbud. *Commutative Algebra with a View Toward Algebraic Geometry*. Springer-Verlag, New York, 1995.

[ER93] R. Ehrenborg and G. Rota. Apolarity and Canonical Forms for Homogeneous Polynomials. *Europ. J. Combinatorics*, 14:157–181, 1993.

[HS80] J. Heintz and C. P. Schnorr. Testing polynomials which are easy to compute (extended abstract). In *Proceedings of the twelfth annual ACM Symposium on Theory of Computing*, pages 262–272, New York, NY, USA, 1980.

[Kal85] K. Kalorkoti. A lower bound for the formula size of rational functions. *SIAM J. Comp.*, 14(3):678–687, 1985. (Conference version in ICALP 1982).

[Kay09] N. Kayal. The Complexity of the Annihilating Polynomial. In *Proceedings of the 24th Annual IEEE Conference on Computational Complexity (CCC)*, pages 184–193, 2009.

[Kem11] G. Kemper. *A Course in Commutative Algebra*. Springer-Verlag, Berlin, 2011.

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

[KMSV10] Z. Karnin, P. Mukhopadhyay, A. Shpilka, and I. Volkovich. Deterministic identity testing of depth-4 multilinear circuits with bounded top fan-in. In *Proceedings of the 42nd ACM Symposium on Theory of Computing (STOC)*, pages 649–658, 2010.

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

[KS08] Z. Karnin and A. Shpilka. Deterministic black box polynomial identity testing of depth-3 arithmetic circuits with bounded top fan-in. In *Proceedings of the 23rd Annual Conference on Computational Complexity (CCC)*, pages 280–291, 2008.

[KS09] N. Kayal and S. Saraf. Blackbox polynomial identity testing for depth 3 circuits. In *Proceedings of the 50th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 198–207, 2009.

[Lan02] S. Lang. *Algebra*. Springer-Verlag, New York, third edition, 2002.

[Lov79] L. Lovász. On determinants, matchings and random algorithms. In *Fundamentals of Computation Theory (FCT)*, pages 565–574, 1979.

[Lov89] L. Lovász. Singular spaces of matrices and their applications in combinatorics. *Bol. Soc. Braz. Mat*, 20:87–99, 1989.

[LV98] D. Lewin and S. Vadhan. Checking polynomial identities over any field: Towards a derandomization? In *Proceedings of the 30th Annual Symposium on the Theory of Computing (STOC)*, pages 428–437, 1998.

[Mat89] H. Matsumura. *Commutative Ring Theory*. Cambridge Studies in Advanced Mathematics, Cambridge, UK, second edition, 1989.

[Mor96] P. Morandi. *Field and Galois Theory*. Springer-Verlag, New York, 1996.

[Oxl06] James Oxley. *Matroid Theory*. Oxford University Press, 2006.

[Pap95] C. H. Papadimitriou. *Computational complexity*. Addison-Wesley, Reading, Massachusetts, 1995.

[Per27] O. Perron. *Algebra I (Die Grundlagen)*. Berlin, 1927.

[Pło05] A. Płoski. Algebraic Dependence of Polynomials After O. Perron and Some Applications. In Svetlana Cojocaru, Gerhard Pfister, and Victor Ufnarovski, editors, *Computational Commutative and Non-Commutative Algebraic Geometry*, pages 167–173. IOS Press, 2005.

[Sax09] N. Saxena. Progress on polynomial identity testing. *Bulletin of the European Association for Theoretical Computer Science (EATCS)- Computational Complexity Column*, (99):49–79, 2009.

[Sch80] J. T. Schwartz. Fast probabilistic algorithms for verification of polynomial identities. *Journal of the ACM*, 27(4):701–717, 1980.

[SS] N. Saxena and C. Seshadhri. An Almost Optimal Rank Bound for Depth-3 Identities. *SIAM J. Comp. (to appear)*. (Conference version in CCC 2009).

[SS10] N. Saxena and C. Seshadhri. From Sylvester-Gallai configurations to rank bounds: Improved black-box identity test for depth-3 circuits. In *Proceedings of the 51st Annual Symposium on Foundations of Computer Science (FOCS)*, pages 21–29, 2010.

[SS11] N. Saxena and C. Seshadhri. 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.

[SV11] S. Saraf and I. Volkovich. Black-box identity testing of depth-4 multilinear circuits. In *Proceedings of the 43rd ACM Symposium on Theory of Computing (STOC)*, 2011.

[SY10] A. Shpilka and A. Yehudayoff. Arithmetic Circuits: A survey of recent results and open questions. *Foundations and Trends in Theoretical Computer Science*, 5(3–4):207–388, 2010.

[vdE00] A. van den Essen. *Polynomial Automorphisms and the Jacobian Conjecture*. Birkhäuser Verlag, Basel, 2000.

[Zen93] J. Zeng. A Bijective Proof of Muir's Identity and the Cauchy-Binet Formula. *Linear Algebra and its Applications*, 184:79–82, 1993.

[Zip79] R. Zippel. Probabilistic algorithms for sparse polynomials. In *Proceedings of the International Symposium on Symbolic and Algebraic Manipulation (EUROSAM)*, pages 216–226, 1979.

A Proofs for Sect. 2: Preliminaries

A.1 Proofs for Sect. 2.1: Perron's criterion

For the proof of Corollary 5 we will need three well-known lemmas. The first one is about resultants. For more information about resultants, see [CLO97].

Lemma 25 (Resultant)**.** *Let $f, g \in K[\boldsymbol{x}]$ such that $\deg_{x_i}(f) > 0$ and $\deg_{x_i}(g) > 0$ for some $i \in [n]$. Then $\mathrm{res}_{x_i}(f, g) = 0$ if and only if f and g have a common factor $h \in K[\boldsymbol{x}]$ with $\deg_{x_i}(h) > 0$.*

Proof. Cf. [CLO97, Chap. 3, §6, Proposition 1]. □

The following lemma identifies a situation where annihilating polynomials are unique up to a factor in K^*.

Lemma 26 (Unique annihilating polynomials)**.** *Let $f_1, \ldots, f_m \in K[\boldsymbol{x}]$ contain precisely $m-1$ algebraically independent polynomials and let $I \subseteq K[y_1, \ldots, y_m]$ be the ideal of algebraic relations among $f_1, \ldots, f_m$. Then I is principal.*

Proof. We follow the instructions of [vdE00, Exercise 3.2.7]. Assume that $f_1, \ldots, f_{m-1}$ are algebraically independent and let $F_1, F_2 \in K[y_1, \ldots, y_m]$ be non-zero irreducible polynomials satisfying $F_i(f_1, \ldots, f_m) = 0$ for $i = 1, 2$. It suffices to show that $F_1 = cF_2$ for some $c \in K^*$.

For this, view F_1, F_2 as elements of $R[y_m]$, where $R = K[y_1, \ldots, y_{m-1}]$, and consider the y_m-resultant $g := \mathrm{res}_{y_m}(F_1, F_2) \in R$. By [CLO97, Chap. 3, §5, Proposition 9], there exist $g_1, g_2 \in R[y_m]$ such that $g = g_1F_1 + g_2F_2$. We have

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

Since $f_1, \ldots, f_{m-1}$ are algebraically independent, it follows that $g = 0$. By Lemma 25, F_1, F_2 have a non-trivial common factor in $R[y_m]$. Since F_1, F_2 are irreducible, we obtain $F_1 = cF_2$ for some $c \in K^*$, as required. □

The following lemma contains a useful fact about annihilating polynomials and algebraic field extensions (cf. [Kay09, Claim 7.2] for a similar statement).

Lemma 27 (Going to a field extension)**.** *Let $f_1, \ldots, f_m \in K[\boldsymbol{x}]$ and let L/K be an algebraic field extension. If there exists a non-zero polynomial $F \in L[\boldsymbol{y}] = L[y_1, \ldots, y_m]$ such that $F(f_1, \ldots, f_m) = 0$, then there exists a non-zero polynomial $G \in K[\boldsymbol{y}]$ such that $G(f_1, \ldots, f_m) = 0$ and $\deg(G) \leq \deg(F)$. In particular, $f_1, \ldots, f_m$ are algebraically independent over K if and only if they are algebraically independent over L.*

Proof. Let $F \in L[\boldsymbol{y}]$ be a non-zero polynomial such that $F(f_1, \ldots, f_m) = 0$. Denote by $c_1, \ldots, c_\ell \in L$ the non-zero coefficients of F. Replacing L by $K(c_1, \ldots, c_\ell)$, we may assume that L/K is algebraic and finitely generated (as a field) over K. By [Lan02, Chapter V, §1, Proposition 1.6], this implies that $[L : K] =: d < \infty$. Let $b_1, \ldots, b_d \in L$ be a K-basis of L. Then we can write F as

$$F = F_1 \cdot b_1 + \cdots + F_d \cdot b_d$$

for some $F_1, \ldots, F_d \in K[\boldsymbol{y}]$, not all zero, such that $\deg(F_i) \leq \deg(F)$ for all $i = 1, \ldots, d$. Substituting $f_1, \ldots, f_m$, we obtain

$$0 = F(f_1, \ldots, f_m) = F_1(f_1, \ldots, f_m) \cdot b_1 + \cdots + F_d(f_1, \ldots, f_m) \cdot b_d.$$

The K-linear independence of $b_1, \ldots, b_d$ implies that all coefficients of

$$F_i(f_1, \ldots, f_m) \in K[\boldsymbol{x}]$$

are zero for $i = 1, \ldots, d$. (Here we use that the indeterminates $x_1, \ldots, x_n$ are L-linearly independent, because L/K is algebraic.) Therefore, some non-zero F_i yields a $G \in K[\boldsymbol{y}]$ with the desired properties. $\square$

Corollary 5. 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 $F(f_1, \ldots, f_m) = 0$.

Proof of Corollary 5. By Lemma 27, we may assume wlog that K is infinite. Furthermore, we may assume that $m = r + 1$ and $f_1, \ldots, f_r$ are algebraically independent. Let $F \in K[\boldsymbol{y}] = K[y_1, \ldots, y_{r+1}]$ be a non-zero *irreducible* polynomial such that $F(f_1, \ldots, f_{r+1}) = 0$. By Lemma 14, there exists a linear K-algebra homomorphism

$$\varphi : K[\boldsymbol{x}] \to K[\boldsymbol{z}] = K[z_1, \ldots, z_r]$$

which is faithful to $\{f_1, \ldots, f_{r+1}\}$. Set $g_i := \varphi(f_i) \in K[\boldsymbol{z}]$ for $i = 1, \ldots, r + 1$. Then $g_1, \ldots, g_{r+1}$ are of degree at most δ and by Theorem 4 there exists a non-zero polynomial $G \in K[\boldsymbol{y}]$ such that $G(g_1, \ldots, g_{r+1}) = 0$ and $\deg(G) \leq \delta^r$. But since

$$F(g_1, \ldots, g_{r+1}) = F(\varphi(f_1), \ldots, \varphi(f_{r+1})) = \varphi(F(f_1, \ldots, f_{r+1})) = 0,$$

Lemma 26 implies that F divides G. Hence, $\deg(F) \leq \deg(G) \leq \delta^r$. $\square$

A.2 Proofs for Sect. 2.2: Jacobi's criterion

In the proof of the Jacobian criterion we will make use of the following facts about partial derivatives. Let $f \in K[\boldsymbol{x}]$. First assume that $\mathrm{ch}(K) = 0$. Then, for $i \in [n]$, we have

$$\partial_{x_i} f = 0 \qquad \text{if and only if} \qquad f \in K[x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n].$$

Therefore, we have $\partial_{x_i}(f) = 0$ for all $i = 1, \dots, n$ if and only if $f = 0$. Now assume $\mathrm{ch}(K) = p > 0$. Then, for $i \in [n]$, we have

$$\partial_{x_i} f = 0 \qquad \text{if and only if} \qquad f \in K[x_1, \dots, x_{i-1}, x_i^p, x_{i+1}, \dots, x_n].$$

Hence, $\partial_{x_i} f = 0$ for all $i = 1, \dots, n$ if and only if $f \in K[x_1^p, \dots, x_n^p]$. If, in addition, K is a perfect field (in characteristic p this means that every element of K is a p-th power), then we have $\partial_{x_i} f = 0$ for all $i = 1, \dots, n$ if and only if $f = g^p$ for some $g \in K[\boldsymbol{x}]$. An example of a perfect field is the algebraic closure $\overline{K}$ of K.

Now let K be an arbitrary field, let $f_1, \dots, f_m \in K[\boldsymbol{x}]$ and let $F_1, \dots, F_s \in K[\boldsymbol{y}]$. Then, by the *chain rule*, we have

$$\begin{aligned} &J_{\boldsymbol{x}}(F_1(f_1, \dots, f_m), \dots, F_s(f_1, \dots, f_m)) \\ &\qquad\qquad = \big(J_{\boldsymbol{y}}(F_1, \dots, F_s)\big)(f_1, \dots, f_m) \cdot J_{\boldsymbol{x}}(f_1, \dots, f_m). \end{aligned}$$

Now we are prepared to proceed with the proofs.

Lemma 7. Let $f_1, \dots, f_m \in K[\boldsymbol{x}]$. Then $\mathrm{trdeg}_K\{f_1, \dots, f_m\} \geq \mathrm{rk}_L\, J_{\boldsymbol{x}}(f_1, \dots, f_m)$, where $L = K(\boldsymbol{x})$.

Proof of Lemma 7. Let $r = \mathrm{rk}_L\, J_{\boldsymbol{x}}(f_1, \dots, f_m)$. We may assume that the first r rows of $J(f_1, \dots, f_m)$ are L-linearly independent. Assume, for the sake of contradiction, that $f_1, \dots, f_r$ are algebraically dependent. Choose a non-zero polynomial $F \in K[\boldsymbol{y}] = K[y_1, \dots, y_r]$ of minimal degree such that $F(f_1, \dots, f_r) = 0$. Differentiating with respect to $x_1, \dots, x_n$ using the chain rule yields the vector-matrix equation

$$\big((\partial_{y_1} F)(f_1, \dots, f_r), \quad \dots, \quad (\partial_{y_r} F)(f_1, \dots, f_r)\big) \cdot \begin{pmatrix} \partial_{x_1} f_1 & \cdots & \partial_{x_n} f_1 \\ \vdots & & \vdots \\ \partial_{x_1} f_r & \cdots & \partial_{x_n} f_r \end{pmatrix} = 0.$$

Since this matrix has rank r over L, it follows that $(\partial_{y_i} F)(f_1, \dots, f_r) = 0$ for all $i = 1, \dots, r$. Since the degree of F was chosen to be minimal, it follows that $\partial_{y_i} F = 0$ for all $i = 1, \dots, r$. If $\mathrm{ch}(K) = 0$, this implies $F = 0$, a contradiction. If $\mathrm{ch}(K) = p > 0$, this implies $F \in K[y_1^p, \dots, y_r^p]$. Since $\overline{K}$ is perfect and $F \neq 0$, there is a non-zero $G \in \overline{K}[\boldsymbol{y}]$ such that $F = G^p$. From

$$0 = F(f_1, \dots, f_r) = G(f_1, \dots, f_r)^p$$

wee see that $G(f_1, \dots, f_r) = 0$. By Lemma 27, there exists a non-zero $G' \in K[\boldsymbol{y}]$ such that $G'(f_1, \dots, f_r) = 0$ and $\deg(G') \leq \deg(G) < \deg(F)$. This contradicts the choice of F. Therefore, $f_1, \dots, f_r$ are algebraically independent, hence $\mathrm{trdeg}(\{f_1, \dots, f_m\}) \geq r$. ☐

Theorem 6. Let $f_1, \dots, f_m \in K[\boldsymbol{x}]$ be polynomials of degree at most δ and trdeg r. Assume that $\mathrm{ch}(K) = 0$ or $\mathrm{ch}(K) > \delta^r$. Then $\mathrm{rk}_L\, J_{\boldsymbol{x}}(f_1, \dots, f_m) = \mathrm{trdeg}_K\{f_1, \dots, f_m\}$, where $L = K(\boldsymbol{x})$.

Proof of Theorem 6. Let $r = \operatorname{trdeg}\{f_1, \dots, f_m\}$. By Lemma 7, we have

$$r \geq \operatorname{rk}_L J(f_1, \dots, f_m),$$

so it remains to show the converse inequality.

After renumbering $f_1, \dots, f_m$ and $x_1, \dots, x_n$, we may assume that the polynomials $f_1, \dots, f_r, x_{r+1}, \dots, x_n$ are algebraically independent. Consequently, for $i = 1, \dots, n$, there exist non-zero polynomials $F_i \in K[y_0, \dots, y_n]$ of minimal degree such that $\deg_{y_0}(F_i) > 0$ and

$$F_i(x_i, f_1, \dots, f_r, x_{r+1}, \dots, x_n) = 0. \tag{2}$$

By Theorem 4 (with $(n-r+1)$ of the δ_i's being 1), we have $\deg(F_i) \leq \delta^r$. Hence, by the assumptions on $\operatorname{ch}(K)$, we have $\partial_{y_0} F_i \neq 0$. Since the degree of F_i was chosen to be minimal, we have

$$(\partial_{y_0} F_i)(x_i, f_1, \dots, f_r, x_{r+1}, \dots, x_n) \neq 0.$$

Denote

$$G_{i,j} := (\partial_{y_j} F_i)(x_i, f_1, \dots, f_r, x_{r+1}, \dots, x_n)$$

for $j = 0, \dots, n$. Differentiating equation (2) with respect to x_k using the chain rule yields

$$G_{i,0} \cdot \delta_{i,k} + \sum_{j=1}^{r} G_{i,j} \cdot \partial_{x_k} f_j + \sum_{j=r+1}^{n} G_{i,j} \cdot \delta_{j,k} = 0$$

for $k = 1, \dots, n$. Since $G_{i,0} \neq 0$, this can be rewritten as

$$\sum_{j=1}^{r} \frac{-G_{i,j}}{G_{i,0}} \cdot \partial_{x_k} f_j + \sum_{j=r+1}^{n} \frac{-G_{i,j}}{G_{i,0}} \cdot \delta_{j,k} = \delta_{i,k}.$$

This shows that the block diagonal matrix

$$\begin{pmatrix} \partial_{x_1} f_1 & \cdots & \partial_{x_r} f_1 & & & \\ \vdots & & \vdots & & & \\ \partial_{x_1} f_r & \cdots & \partial_{x_r} f_r & & & \\ & & & 1 & & \\ & & & & \ddots & \\ & & & & & 1 \end{pmatrix} \in L^{n \times n}$$

is invertible. Therefore, the first r rows of $J(f_1, \dots, f_m)$ are L-linearly independent and hence $r \leq \operatorname{rk}_L J(f_1, \dots, f_m)$. $\square$

A.3 Proofs for Sect. 2.3: Krull dimension

Corollary 9. 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 $\dim(\varphi(A)) = \dim(A)$.

Proof of Corollary 9. Since A is an affine algebra, there exist $a_1, \ldots, a_m \in A$ such that $A = K[a_1, \ldots, a_m]$. Then $\varphi(A) = K[\varphi(a_1), \ldots, \varphi(a_m)]$ is finitely generated as a K-algebra as well.

Now assume for the sake of contradiction that $d := \dim(\varphi(A)) > \dim(A)$. By Theorem 8, there exist $a_1, \ldots, a_d \in A$ such that $\varphi(a_1), \ldots, \varphi(a_d)$ are algebraically independent. Since $d > \dim(A)$, the elements $a_1, \ldots, a_d$ are algebraically dependent. Hence, there exists a non-zero polynomial $F \in K[y_1, \ldots, y_d]$ such that $F(a_1, \ldots, a_d) = 0$. It follows that

$$0 = \varphi(F(a_1, \ldots, a_d)) = F(\varphi(a_1), \ldots, \varphi(a_d))$$

and this implies that $\varphi(a_1), \ldots, \varphi(a_d)$ are algebraically dependent, a contradiction. Therefore, $\dim(\varphi(A)) \leq \dim(A)$.

Now let φ be injective, let $d := \dim(A)$ and let $a_1, \ldots, a_d \in A$ be algebraically independent. Assume for the sake of contradiction that $\varphi(a_1), \ldots, \varphi(a_d)$ are algebraically dependent. Then there exists a non-zero polynomial $F \in K[y_1, \ldots, y_d]$ such that $F(\varphi(a_1), \ldots, \varphi(a_d)) = 0$. From

$$0 = F(\varphi(a_1), \ldots, \varphi(a_d)) = \varphi(F(a_1, \ldots, a_d))$$

we see that $F(a_1, \ldots, a_d) = 0$, because φ is injective. But this means that $a_1, \ldots, a_d$ are algebraically dependent, a contradiction. Thus $\dim(\varphi(A)) \geq \dim(A)$. □

B Proofs for Sect. 3: Faithful homomorphisms

Let $\mathbb{P}$ denote the set of prime numbers and $\mathrm{sp}(f)$ denote the *sparsity* of a polynomial f.

In the proofs of Lemmas 15, 16 and 22 we will use the following well-known facts.

Lemma 28 (Sparse PIT)**.** *Let $\ell \geq 1$ and $d \geq 2$. Let R be a commutative ring and let $f \in R[t]$ be a non-zero polynomial of sparsity at most ℓ and degree at most d. Then there are at most $\ell \cdot \log_2(d) - 1$ prime numbers p such that $f = 0 \pmod{\langle t^p - 1\rangle_{R[t]}}$.*

Proof. Cf. [BHLV09, Lemma 13] and note that the given proof also works for polynomials over a ring (instead of a field). □

Lemma 29 (Primes)**.** *Let $r \in \mathbb{R}^{\geq 2}$. Then the interval $[1, r^2 + 1]$ contains at least $\lceil r \rceil$ prime numbers.*

Proof. Cf. [Pap95, Claim on p. 478]. □

B.1 Proofs for Sect. 3.1: A Kronecker-inspired map

Lemma 14. 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 $\{f_1, \ldots, f_m\}$.

Proof of Lemma 14. After renumbering $f_1, \ldots, f_m$ and $x_1, \ldots, x_n$, we may assume that $f_1, \ldots, f_r, x_{r+1}, \ldots, x_n$ are algebraically independent. Consequently, for $i = 1, \ldots, r$, there exists a non-zero polynomial $G_i \in K[y_0, y_1, \ldots, y_n]$ such that $\deg_{y_0}(G_i) > 0$ and

$$G_i(x_i, f_1, \ldots, f_r, x_{r+1}, \ldots, x_n) = 0.$$

Denote by $g_i \in K[y_1, \ldots, y_n]$ the (non-zero) leading coefficient of G_i as a polynomial in y_0 with coefficients in $K[y_1, \ldots, y_n]$. The algebraic independence of $f_1, \ldots, f_r$, $x_{r+1}, \ldots, x_n$ implies

$$g_i(f_1, \ldots, f_r, x_{r+1}, \ldots, x_n) \neq 0.$$

Since K is infinite, there exist $c_{r+1}, \ldots, c_n \in K$ such that

$$(g_i(f_1, \ldots, f_r, x_{r+1}, \ldots, x_n))(x_1, \ldots, x_r, c_{r+1}, \ldots, c_n) \neq 0$$

for all $i = 1, \ldots, r$. Now define the K-algebra homomorphism

$$\varphi : K[\boldsymbol{x}] \to K[\boldsymbol{z}], \qquad x_i \mapsto \begin{cases} z_i, & \text{if } 1 \leq i \leq r, \\ c_i, & \text{otherwise.} \end{cases}$$

Then, by the choice of $c_{r+1}, \ldots, c_n$, we have

$$G_i(y_0, \varphi(f_1), \ldots, \varphi(f_r), c_{r+1}, \ldots, c_n) \neq 0$$

and

$$G_i(z_i, \varphi(f_1), \ldots, \varphi(f_r), c_{r+1}, \ldots, c_n) = 0$$

for $i = 1, \ldots, r$. This shows that z_i is algebraically dependent on $\varphi(f_1), \ldots, \varphi(f_r)$ for $i = 1, \ldots, r$. It follows that

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

hence φ is faithful to $\{f_1, \ldots, f_m\}$. $\square$

Lemma 15. Let $f_1, \ldots, f_m \in K[\boldsymbol{x}]$ 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 $\{f_1, \ldots, f_m\}$.

Proof of Lemma 15. We may assume wlog that $\operatorname{trdeg}\{f_1, \ldots, f_m\} = r$ and, after renumbering $f_1, \ldots, f_m$, that

$$f_1, \ldots, f_r, x_{j_{r+1}}, \ldots, x_{j_n}$$

are algebraically independent for some $j_{r+1}, \ldots, j_n \in [n]$ with $j_{r+1} < \cdots < j_n$. Denote the complement $[n] \setminus \{j_{r+1}, \ldots, j_n\}$ by $I = \{j_1, \ldots, j_r\}$, where $j_1 < \cdots < j_r$. By Corollary 5, there exists a non-zero polynomial $G_i \in K[y_0, y_1, \ldots, y_n]$ such that $\deg(G_i) \leq \delta^r$, $\deg_{y_0}(G_i) > 0$ and

$$G_i(x_{j_i}, f_1, \ldots, f_r, x_{j_{r+1}}, \ldots, x_{j_n}) = 0$$

for $i = 1, \ldots, r$. Denote by $g_i \in K[y_1, \ldots, y_n]$ the (non-zero) leading coefficient of G_i as a polynomial y_0 with coefficients in $K[y_1, \ldots, y_n]$. The algebraic independence of $f_1, \ldots, f_r$, $x_{j_{r+1}}, \ldots, x_{j_n}$ implies

$$g_i(f_1, \ldots, f_r, x_{j_{r+1}}, \ldots, x_{j_n}) \neq 0.$$

We have

$$\deg\big(g_i(f_1, \ldots, f_r, x_{j_{r+1}}, \ldots, x_{j_n})\big) \leq \delta^{r+1} < D.$$

Therefore, the polynomial

$$h_i := g_i(\Phi_{I,D}(f_1), \ldots, \Phi_{I,D}(f_r), \Phi_{I,D}(x_{j_{r+1}}), \ldots, \Phi_{I,D}(x_{j_n})) \in K[t, \boldsymbol{z}]$$

is non-zero (this is the classical Kronecker substitution: D is so large that the monomials remain separated). We have

$$\deg_t(h_i) \leq \delta^{r+1} \cdot (D + D^2 + \cdots + D^{n-r}) \leq D^{n+1}.$$

Also, the sparsity of h_i (short, sp) can be bounded as:

$$\begin{aligned} \operatorname{sp}(h_i) &= \operatorname{sp}\big(g_i(f_1, \ldots, f_r, x_{j_{r+1}}, \ldots, x_{j_n})\big) \\ &\leq \operatorname{sp}(g_i) \cdot \max\{\operatorname{sp}(f_1), \ldots, \operatorname{sp}(f_r)\}^{\deg(g_i)} \\ &\leq \binom{n+\delta^r}{\delta^r} \cdot \binom{n+\delta}{\delta}^{\delta^r} \\ &\leq (n+\delta^r)^{\delta^r} \cdot (n+\delta)^{\delta^{r+1}}. \end{aligned}$$

Let $B_i \subseteq \mathbb{P}$ be the set of all primes p satisfying $h_i = 0 \pmod{\langle t^p - 1\rangle_{K[t,\boldsymbol{z}]}}$. Then $|B_i| < (n+1)(n+\delta^r)^{\delta^r}(n+\delta)^{\delta^{r+1}} \log_2 D$ by Lemma 28. Finally set $B := B_1 \cup \cdots \cup B_r$. Then

$$|B| < r(n+1)(n+\delta^r)^{\delta^r}(n+\delta)^{\delta^{r+1}} \log_2 D \leq (n+\delta^r)^{4\delta^{r+1}} \log_2 D.$$

Now pick a suitable prime $p \in \mathbb{P} \setminus B$ (by Lemma 29). Let $i \in [r]$. Then $h_i \neq 0 \pmod{\langle t^p - 1\rangle_{K[t,\boldsymbol{z}]}}$. Define

$$h_i^{(p)} := g_i(\Phi_{I,D,p}(f_1), \ldots, \Phi_{I,D,p}(f_r), \Phi_{I,D,p}(x_{j_{r+1}}), \ldots, \Phi_{I,D,p}(x_{j_n})) \in K[t, \boldsymbol{z}].$$

Since $h_i^{(p)} = h_i \neq 0 \pmod{\langle t^p - 1\rangle_{K[t,\boldsymbol{z}]}}$, we have $h_i^{(p)} \neq 0$. Let $S_i \subset \overline{K}$ be the set of all $c \in \overline{K}$ such that $h_i^{(p)}(c, \boldsymbol{z}) = 0$. Then $|S_i| \leq \deg_t(h_i^{(p)}) < \delta^r p$. Finally set $S := S_1 \cup \cdots \cup S_r$. Then $|S| < r\delta^r p$.

Now let $i \in [r]$ and $c \in \overline{K} \setminus S$. Then

$$G_i\big(y_0, \Phi_{I,D,p,c}(f_1), \ldots, \Phi_{I,D,p,c}(f_r), c^{\lfloor D^1 \rfloor_p}, \ldots, c^{\lfloor D^{n-r} \rfloor_p}\big) \neq 0,$$

because $h_i^{(p)}(c, \boldsymbol{z}) \neq 0$, and

$$G_i\big(z_i, \Phi_{I,D,p,c}(f_1), \ldots, \Phi_{I,D,p,c}(f_r), c^{\lfloor D^1 \rfloor_p}, \ldots, c^{\lfloor D^{n-r} \rfloor_p}\big) = 0.$$

This shows that z_i is algebraically dependent on $\Phi_{I,D,p,c}(f_1), \ldots, \Phi_{I,D,p,c}(f_r)$ for $i = 1, \ldots, r$. It follows that

$$\operatorname{trdeg}\{\Phi_{I,D,p,c}(f_1), \ldots, \Phi_{I,D,p,c}(f_m)\} = r = \operatorname{trdeg}\{f_1, \ldots, f_m\}$$

for all $c \in \overline{K} \setminus S$. □

B.2 Proofs for Section 3.2: A Vandermonde-inspired map

Lemma 16. 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 $\operatorname{ch}(K) = 0$ or $\operatorname{ch}(K) > \delta^r$. 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 $\{f_1, \ldots, f_m\}$.

Proof of Lemma 16. Let $s := \operatorname{trdeg}\{f_1, \ldots, f_m\} \leq r$ and let $i_1, \ldots, i_s \in [m]$ such that $f_{i_1}, \ldots, f_{i_s}$ are algebraically independent. By the chain rule, we have

$$\begin{aligned} &J_{z_1,\ldots,z_s}(\Psi_D(f_{i_1}), \ldots, \Psi_D(f_{i_s})) \\ &\quad = \big(J_{\boldsymbol{x}}(f_{i_1}, \ldots, f_{i_s})\big)(\Psi_D(x_1), \ldots, \Psi_D(x_n)) \cdot J_{z_1,\ldots,z_s}(\Psi_D(x_1), \ldots, \Psi_D(x_n)). \end{aligned} \tag{3}$$

We introduce some notation. Define the polynomial

$$f' := \det J_{z_1,\ldots,z_s}(\Psi_D(f_{i_1}), \ldots, \Psi_D(f_{i_s})) \in K[t, \boldsymbol{z}]$$

and set $f := f'(t, 0, \ldots, 0) \in K[t]$. For an index set $I = \{j_1, \ldots, j_s\} \in \binom{[n]}{s}$ with $j_1 < \cdots < j_s$, denote

$$g'_I := \big(\det J_{x_{j_1},\ldots,x_{j_s}}(f_{i_1}, \ldots, f_{i_s})\big)(\Psi_D(x_1), \ldots, \Psi_D(x_n)) \in K[t, \boldsymbol{z}]$$

and

$$h'_I := \det J_{z_1,\ldots,z_s}(\Psi_D(x_{j_1}), \ldots, \Psi_D(x_{j_s})) \in K[t, \boldsymbol{z}],$$

and set $g_I := g'_I(t, 0 \ldots, 0) \in K[t]$ and $h_I := h'_I(t, 0, \ldots, 0) \in K[t]$. Applying the Cauchy-Binet formula (cf. [Zen93]) to (3) and substituting $(t, 0, \ldots, 0)$ for $(t, z_0, \ldots, z_r)$, we obtain

$$f = \sum_{I \in \mathcal{I}} g_I \cdot h_I, \tag{4}$$

where $\mathcal{I} := \{I \in \binom{[n]}{s} \mid g_I \neq 0\}$. We want to prove that $f \neq 0$. It suffices to show that there is a unique $I \in \mathcal{I}$ for which $\deg(g_I \cdot h_I)$ is maximal.

First we show that $\mathcal{I} \neq \varnothing$. Since $f_{i_1}, \ldots, f_{i_s}$ are algebraically independent, there exists $I = \{j_1, \ldots, j_s\} \in \binom{[n]}{s}$ with $j_1 < \cdots < j_s$ such that

$$\det J_{x_{j_1}, \ldots, x_{j_s}}(f_{i_1}, \ldots, f_{i_s}) \neq 0$$

by Theorem 6. We have

$$\deg\bigl(\det J_{x_{j_1}, \ldots, x_{j_s}}(f_{i_1}, \ldots, f_{i_s})\bigr) \leq \delta s \leq \delta r.$$

Since $D \geq \delta r + 1$, it follows that $g_I \neq 0$ (this is the classical Kronecker substitution: D is so large that the monomials remain separated), hence $I \in \mathcal{I}$.

Next we want to show that $h_I \neq 0$ and $\deg(h_I) < D$ for all $I \in \binom{[n]}{s}$, and we want to show that $\deg(h_I) \neq \deg(h_{I'})$ for all $I, I' \in \binom{[n]}{s}$ with $I \neq I'$. To this end, let $I = \{j_1, \ldots, j_s\} \in \binom{[n]}{s}$ with $j_1 < \cdots < j_s$. Then

$$h_I = \det \begin{pmatrix} t^{j_1(n+1)^1} & \ldots & t^{j_1(n+1)^s} \\ \vdots & & \vdots \\ t^{j_s(n+1)^1} & \ldots & t^{j_s(n+1)^s} \end{pmatrix} = \sum_{\sigma \in \mathfrak{S}_s} \operatorname{sgn}(\sigma) \cdot t^{d_\sigma},$$

where $\mathfrak{S}_s$ denotes the symmetric group on $\{1, \ldots, s\}$ and

$$d_\sigma := j_1(n+1)^{\sigma(1)} + \cdots + j_s(n+1)^{\sigma(s)} \in \mathbb{N}.$$

It is not hard to show that $d_{\mathrm{id}} > d_\sigma$ for all $\sigma \in \mathfrak{S}_s \setminus \{\mathrm{id}\}$. This implies $h_I \neq 0$ and

$$\deg(h_I) = j_1(n+1)^1 + \cdots + j_s(n+1)^s < (n+1)^{s+1} \leq (n+1)^{r+1} \leq D.$$

From the degree formula it is not hard to deduce that $\deg(h_I) \neq \deg(h_{I'})$ for all $I, I' \in \binom{[n]}{s}$ with $I \neq I'$.

Now denote by $\mathcal{I}_{\max} \subseteq \mathcal{I}$ the set of all $I \in \mathcal{I}$ such that $\deg(g_I)$ is maximal. Let $I \in \mathcal{I}_{\max}$ and let $I' \in \mathcal{I} \setminus \mathcal{I}_{\max}$. Observe that, by construction, we have $\deg(g_I) - \deg(g_{I'}) \geq D$. Since $\deg(h_{I'}) < D$, it follows that

$$\deg(g_I \cdot h_I) \geq \deg(g_I) \geq \deg(g_{I'}) + D > \deg(g_{I'}) + \deg(h_{I'}) = \deg(g_{I'} \cdot h_{I'}).$$

Therefore, the summands in (4) of maximal degree have an index set in $\mathcal{I}_{\max}$.

Finally, let $I \in \mathcal{I}_{\max}$ be the unique index set such that $\deg(h_I)$ is maximal. Then $g_I \cdot h_I$ is the unique summand in (4) of maximal degree. This implies $f \neq 0$, as required.

By (4), we have

$$\operatorname{sp}(f) \leq \binom{n}{s} \cdot (s! \cdot \ell^s) \cdot s! \leq (ns\ell)^s \leq (nr\ell)^r$$

and

$$\deg(f) \leq r\delta \cdot (D_1 + D_1^2 + \cdots + D_1^n) + (n+1)^{r+1} \leq D_1^{n+1} + D_1 \leq D_1^{n+2}.$$

Let $B \subseteq \mathbb{P}$ be the set of all primes p satisfying $f = 0 \pmod{\langle t^p - 1\rangle_{K[t]}}$. Then

$$|B| < (n+2)(nr\ell)^r \log_2 D_1 \leq (2nr\ell)^{r+1} \log_2 D_1$$

by Lemma 28.

Now pick a suitable prime $p \in \mathbb{P} \setminus B$ (by Lemma 29). Then $f \neq 0 \pmod{\langle t^p - 1\rangle_{K[t]}}$. This implies $f' \neq 0 \pmod{\langle t^p - 1\rangle_{K[t,\boldsymbol{z}]}}$. Define

$$f^{(p)} := \det J_{z_1,\ldots,z_s}(\Psi_{D,p}(f_{i_1}), \ldots, \Psi_{D,p}(f_{i_s})) \in K[t, \boldsymbol{z}].$$

Since $f^{(p)} = f' \neq 0 \pmod{\langle t^p - 1\rangle_{K[t,\boldsymbol{z}]}}$, we have $f^{(p)} \neq 0$. Let $S \subset \overline{K}$ be the set of all $c \in \overline{K}$ such that $f^{(p)}(c, \boldsymbol{z}) = 0$. Then $|S| \leq \deg_t(f^{(p)}) < \delta s p \leq \delta r p$. Now let $c \in \overline{K} \setminus S$. Then

$$\det J_{z_1,\ldots,z_s}(\Psi_{D,p,c}(f_{i_1}), \ldots, \Psi_{D,p,c}(f_{i_s})) = f^{(p)}(c, \boldsymbol{z}) \neq 0.$$

By Theorem 6, this means that $\Psi_{D,p,c}(f_{i_1}), \ldots, \Psi_{D,p,c}(f_{i_s})$ are algebraically independent, hence

$$\operatorname{trdeg}\{\Psi_{D,p,c}(f_1), \ldots, \Psi_{D,p,c}(f_m)\} = s = \operatorname{trdeg}\{f_1, \ldots, f_m\}$$

for all $c \in \overline{K} \setminus S$. □

C Proofs for Sect. 4: Proving Theorem 1

C.1 Proofs for Sect. 4.1: A hitting set

Theorem 18. Assume that $\operatorname{ch}(K) = 0$ or $\operatorname{ch}(K) > \delta^r$. 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 $\operatorname{poly}(dr\delta\ell n)^r$ time.

Proof of Theorem 18. Let $C(f_1, \ldots, f_m)$ be a non-zero circuit of degree at most d with subcircuits $f_1, \ldots, f_m$ of sparsity at most ℓ, degree at most δ and trdeg at most r. By the choice of parameters, Lemma 16 implies that there exist a prime $p \in [p_{\max}]$ and an element $c \in H_1$ such that $\Psi_{D,p,c}$ is faithful to $\{f_1, \ldots, f_m\}$. Hence, by Theorem 12,

$$\Psi_{D,p,c}(C(f_1, \ldots, f_m)) = C(\Psi_{D,p,c}(f_1), \ldots, \Psi_{D,p,c}(f_m))$$

is a non-zero circuit with at most $r+1$ variables and of degree at most d. Now the first assertion follows from Lemma 17. The second assertion is obvious from the construction. □

C.2 Proofs for Sect. 4.2: Arbitrary characteristic

Theorem 19. The set $\mathcal{H}_{d,r,\delta}$ is a hitting set for the class of degree-d circuits with inputs being degree-δ subcircuits of transcendence degree at most r. It can be constructed in $\mathrm{poly}(dr\delta n)^{r\delta^{r+1}}$ time.

Proof of Theorem 19. Let $C(f_1, \ldots, f_m)$ be a non-zero circuit of degree at most d with subcircuits $f_1, \ldots, f_m$ of degree at most δ and trdeg at most r. By the choice of parameters, Lemma 15 implies that there exist an index set $I \in \binom{[n]}{r}$, a prime $p \in [p_{\max}]$ and an element $c \in H_1$ such that $\Phi_{I,D,p,c}$ is faithful to $\{f_1, \ldots, f_m\}$. Hence, by Theorem 12,

$$\Phi_{I,D,p,c}(C(f_1, \ldots, f_m)) = C(\Phi_{I,D,p,c}(f_1), \ldots, \Phi_{I,D,p,c}(f_m))$$

is a non-zero circuit with at most r variables and of degree at most d. Now the first assertion follows from Lemma 17. The second assertion is obvious from the construction. $\square$

D Proofs for Sect. 5: Depth-4 circuits

D.1 Proofs for Sect. 5.2: Preserving the simple part

Lemma 22. 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 $2\delta^4 k^2 s^2 p$ contains c satisfying $\Psi_{D,p,c}(\mathrm{sim}(C)) = \mathrm{sim}(\Psi_{D,p,c}(C))$.

Proof of Lemma 22. Let $f_1, \ldots, f_m \in K[\boldsymbol{x}]$ be the non-constant *irreducible* factors of the polynomials in $\mathcal{S}(C)$. Then $m \leq ks\delta$ and we have

$$\deg(f_i) \leq \delta \qquad \text{and} \qquad \mathrm{sp}(f_i) \leq \binom{n+\delta}{\delta} \leq (n+\delta)^\delta$$

for all $i = 1, \ldots, m$.

First we make the following observation. If $\varphi : K[\boldsymbol{x}] \to K[\boldsymbol{z}]$ is a K-algebra homomorphism such that

1. $\varphi(f_i)$ is non-constant, for all $i = 1, \ldots, m$, and
2. $\gcd(f_i, f_j) = 1$ implies $\gcd(\varphi(f_i), \varphi(f_j)) = 1$, for all $1 \leq i < j \leq m$,

then $\varphi(\mathrm{sim}(C)) = \mathrm{sim}(\varphi(C))$. To satisfy the first condition we will ensure that the images of $f_1, \ldots, f_m$ under Ψ are monic in z_0. This will also facilitate our task of meeting the second condition. Here we will use resultants with respect to z_0 to preserve coprimality.

So let $i \in [m]$ and define

$$g_i := f_i\big(t^{D_2^1}, \ldots, t^{D_2^n}\big) \in K[t].$$

Since $\deg(f_i) < D_2$, we have $g_i \neq 0$ (Kronecker substitution). We have

$$\deg(g_i) \leq \delta \cdot (D_2 + D_2^2 + \cdots + D_2^n) \leq D_2^{n+1}$$

and $\mathrm{sp}(g_i) = \mathrm{sp}(f_i) \leq (n+\delta)^\delta$. Let $B_{1,i} \subseteq \mathbb{P}$ be the set of all primes p satisfying $g_i = 0 \pmod{\langle t^p - 1\rangle_{K[t]}}$. Then $|B_{1,i}| < (n+1)(n+\delta)^\delta \log_2 D_2$ by Lemma 28. Finally, set $B_1 := B_{1,1} \cup \cdots \cup B_{1,m}$. Then

$$|B_1| \leq m(n+1)(n+\delta)^\delta \log_2 D_2 \leq ks\delta(n+1)(n+\delta)^\delta \log_2 D_2.$$

Now let $i \in [m]$ and define

$$h_i := f_i\big(x_1 + t^{D_2^1} z_0, \ldots, x_n + t^{D_2^n} z_0\big) \in K[t, z_0, \boldsymbol{x}].$$

Then the leading term of h_i as a polynomial in z_0 is g_i. In particular, $h_i \neq 0$. We have

$$\mathrm{sp}(h_i) \leq 2^\delta \cdot \mathrm{sp}(f_i) \leq 2^\delta (n+\delta)^\delta.$$

Now let $i, j \in [m]$ with $i < j$ such that $\gcd(f_i, f_j) = 1$. Then $\gcd(h_i, h_j) = 1$, because the map:

$$K(t, z_0)[\boldsymbol{x}] \to K(t, z_0)[\boldsymbol{x}], \qquad x_i \mapsto x_i + t^{D_2^i} z_0 \quad (i = 1, \ldots, n)$$

is a $K(t, z_0)$-algebra automorphism. This implies $\mathrm{res}_{z_0}(h_i, h_j) \neq 0$. We have

$$\deg_{\boldsymbol{x}}\big(\mathrm{res}_{z_0}(h_i, h_j)\big) \leq 2\delta^2 < D_1,$$

therefore the polynomial

$$h_{i,j} := \mathrm{res}_{z_0}\big((\Psi_D(f_i))(t, z_0, 0, \ldots, 0), (\Psi_D(f_i))(t, z_0, 0, \ldots, 0)\big) \in K[t, z_0]$$

is non-zero (Kronecker substitution). We have

$$\deg_t(h_{i,j}) \leq 2\delta^2 \cdot (D_1 + D_1^2 + \cdots + D_1^n) \leq D_1^{n+1}$$

(using $D_1 \geq D_2$) and

$$\mathrm{sp}(h_{i,j}) \leq \max\{\mathrm{sp}(h_i), \mathrm{sp}(h_j)\}^{2\delta} \leq 2^{2\delta^2}(n+\delta)^{2\delta^2}.$$

Let $B_{2,i,j} \subseteq \mathbb{P}$ be the set of all primes p satisfying $h_{i,j} \neq 0 \pmod{\langle t^p - 1\rangle_{K[t,z_0]}}$. Then $|B_{2,i,j}| < (n+1)2^{2\delta^2}(n+\delta)^{2\delta^2} \log_2 D_1$ by Lemma 28. Finally, set $B_2 := \bigcup_{i,j} B_{2,i,j}$, where the union is over all $i, j \in [m]$ with $i < j$ such that $\gcd(f_i, f_j) = 1$. Then

$$\begin{aligned} |B_2| &< \tfrac{1}{2} m^2 (n+1) 2^{2\delta^2} (n+\delta)^{2\delta^2} \log_2 D_1 \\ &\leq \tfrac{1}{2}(ks\delta)^2 (n+1) 2^{2\delta^2} (n+\delta)^{2\delta^2} \log_2 D_1. \end{aligned}$$

Ultimately, set $B := B_1 \cup B_2$. Then

$$\begin{aligned} |B| &\le 2\,|B_2| < (ks\delta)^2(n+1)2^{2\delta^2}(n+\delta)^{2\delta^2}\log_2 D_1 \\ &\le (2ksn\delta^2)^{4\delta^2+1}\log_2 D_1. \end{aligned}$$

Now pick a suitable prime $p \in \mathbb{P} \setminus B$ (by Lemma 29). First, let $i \in [m]$. Since $p \notin B_1$, we have $g_i \neq 0 \pmod{\langle t^p - 1\rangle_{K[t]}}$. Define

$$g_i^{(p)} := f_i\big(t^{\lfloor D_2^1 \rfloor_p}, \ldots, t^{\lfloor D_2^n \rfloor_p}\big) \in K[t].$$

Since $g_i^{(p)} = g_i \neq 0 \pmod{\langle t^p - 1\rangle_{K[t]}}$, we have $g_i^{(p)} \neq 0$. Let $S_{1,i} \subset \overline{K}$ be the set of all $c \in \overline{K}$ such that $g_i^{(p)}(c) = 0$. Then $|S_{1,i}| \le \deg(g_i^{(p)}) < \delta p$. Finally, set $S_1 := S_{1,1} \cup \cdots \cup S_{1,m}$. Then $|S_1| < m\delta p \le ks\delta^2 p$. Now let $i, j \in [m]$ with $i < j$ such that $\gcd(f_i, f_j) = 1$. Since $p \notin B_2$, we have $h_{i,j} \neq 0 \pmod{\langle t^p - 1\rangle_{K[t,z_0]}}$. Define

$$h_{i,j}^{(p)} := \mathrm{res}_{z_0}\big((\Psi_{D,p}(f_i))(t, z_0, 0, \ldots, 0), (\Psi_{D,p}(f_i))(t, z_0, 0, \ldots, 0)\big) \in K[t, z_0].$$

Since $h_{i,j}^{(p)} = h_{i,j} \neq 0 \pmod{\langle t^p - 1\rangle_{K[t,z_0]}}$, we have $h_{i,j}^{(p)} \neq 0$. Let $S_{2,i,j} \subset \overline{K}$ be the set of all $c \in \overline{K}$ such that $h_{i,j}^{(p)}(c, z_0) = 0$. Then $|S_{2,i,j}| \le \deg_t(h_{i,j}^{(p)}) < 2\delta^2 p$. Finally set $S_2 := \bigcup_{i,j} S_{2,i,j}$, where the union is over all $i, j \in [m]$ with $i < j$ such that $\gcd(f_i, f_j) = 1$. Then $|S_2| < \frac{1}{2}m^2 \cdot 2\delta^2 p \le \delta^4 k^2 s^2 p$. Ultimately, set $S := S_1 \cup S_2$. Then $|S| < 2\delta^4 k^2 s^2 p$.

Let $i \in [m]$. Then $\Psi_{D,p,c}(f_i)$ is monic in z_0 for all $c \in \overline{K} \setminus S$. Now let $i, j \in [m]$ with $i < j$ such that $\gcd(f_i, f_j) = 1$. Then

$$\begin{aligned} &\big(\mathrm{res}_{z_0}(\Psi_{D,p,c}(f_i), \Psi_{D,p,c}(f_j))\big)(z_0, 0, \ldots, 0) \\ &\qquad = \mathrm{res}_{z_0}\big((\Psi_{D,p,c}(f_i))(z_0, 0, \ldots, 0), (\Psi_{D,p,c}(f_i))(z_0, 0, \ldots, 0)\big) \\ &\qquad = h_{i,j}^{(p)}(c, z_0) \neq 0 \end{aligned}$$

for all $c \in \overline{K} \setminus S$. Thus, $\mathrm{res}_{z_0}(\Psi_{D,p,c}(f_i), \Psi_{D,p,c}(f_j)) \neq 0$ and by Lemma 25 it follows that $\gcd(\Psi_{D,p,c}(f_i), \Psi_{D,p,c}(f_j)) = 1$ for all $c \in \overline{K} \setminus S$. □

D.2 Proofs for Sect. 5.3: A hitting set

Theorem 23. 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 $\mathrm{poly}(\delta rsn)^{\delta^2 kr}$ time.

Proof of Theorem 23. Let $C \in \Sigma\Pi\Sigma\Pi_\delta(k, s, n)$ be a non-zero circuit. First, let us show by a loose estimation that our parameters afford 2^k applications of Lemmas 16 and 22 (one for each $\mathcal{S}(C_I)$ resp. C_I, for all $I \subseteq [k]$). The number of 'bad' primes by the proofs of these lemmas are at most:

$$\begin{aligned} &2^k \cdot (2nr(n+\delta)^\delta)^{r+1}\log_2 D_1 + 2^k \cdot (2ksn\delta^2)^{4\delta^2+1}\log_2 D_1 \\ &\quad < 2^k \cdot (2nr \cdot 2n\delta)^{\delta(r+1)}\log_2 D_1 + 2^k \cdot (2ksn\delta^2)^{4\delta^2+1}\log_2 D_1 \\ &\quad < 2^k \cdot (2nr\delta)^{2\delta(r+1)}\log_2 D_1 + 2^k \cdot (2ksn\delta^2)^{4\delta^2+1}\log_2 D_1 \\ &\quad < 2^{k+1} \cdot (2krsn\delta^2)^{4\delta^2+2\delta r}\log_2 D_1. \end{aligned}$$

Thus, the set $[p_{\max}]$ would have a 'good' prime p (by Lemma 29). Next comes the estimate on the number of 'bad' c:

$$2^k \delta r p + 2^k \cdot (2\delta^4 k^2 s^2 p) < 2^{k+2} k^2 r s^2 \delta^4 p.$$

Thus, Lemma 16 and Lemma 22 imply that there exist a prime $p \in [p_{\max}]$ and an element $c \in H_1$ such that, for all $I \subseteq [k]$, we have

1. $\Psi_{D,p,c}(\mathrm{sim}(C_I)) = \mathrm{sim}(\Psi_{D,p,c}(C_I))$, and
2. $\Psi_{D,p,c}$ is faithful to some subset $\{f_1, \ldots, f_m\} \subseteq \mathcal{S}(\mathrm{sim}(C_I))$ of transcendence degree $\min\{\mathrm{rk}(\mathrm{sim}(C_I)), r\}$.

Hence, by Lemma 21, $\Psi_{D,p,c}(C)$ is a non-zero circuit with at most $r+1$ variables and of degree at most δs. Now the first assertion follows from Lemma 17. The second assertion is obvious from the construction. □

Corollary 24. 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 $\mathrm{poly}(\delta s n)^{\delta^2}$ time.

Proof of Corollary 24. First observe $R_\delta(2, s) = 1$. Since Ψ sends non-constant sparse polynomials of a circuit to non-constant polynomials (see the proof of Lemma 22), it is faithful to sets of transcendence degree 1. Hence we do not need to invoke Lemma 16 (where the dependence on the characteristic came from). □

ECCC ISSN 1433-8092

http://eccc.hpi-web.de