Information and Computation 222 (2013) 2–19

Contents lists available at SciVerse ScienceDirect

Information and Computation

www.elsevier.com/locate/yinco

Algebraic independence and blackbox identity testing ☆

M. Beecken, J. Mittmann *, N. Saxena

Hausdorff Center for Mathematics, Endenicher Allee 62, D-53115 Bonn, Germany

ARTICLE INFO

Article history:
Available online 26 October 2012

Keywords:
Algebraic independence
Transcendence degree
Arithmetic circuits
Polynomial identity testing
Blackbox algorithms
Depth-4 circuits

ABSTRACT

Algebraic independence is a fundamental notion in commutative algebra that generalizes independence of linear polynomials. Polynomials $\{f_1, \ldots, f_m\} \subset K[x_1, \ldots, x_n]$ (over a field K) are called algebraically independent if there is no non-zero polynomial F such that $F(f_1, \ldots, f_m) = 0$. The transcendence degree, $\operatorname{trdeg}\{f_1, \ldots, f_m\}$, 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 $\operatorname{trdeg}\{\varphi(f_i)\}_i = r$, assuming sparse f_i and small r. We apply these fundamental maps to solve two cases of blackbox identity testing (assuming a large or zero characteristic):

1. Given a polynomial-degree circuit C and sparse polynomials $f_1, \ldots, f_m$ of transcendence degree r, we can test blackbox $D := C(f_1, \ldots, f_m)$ for zeroness in $\operatorname{poly}(\operatorname{size}(D))^r$ time.
2. Define a $\Sigma\Pi\Sigma\Pi_\delta(k, s, n)$ circuit 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 this class of depth-4 circuits 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 $\operatorname{poly}(\delta s n R)^{Rk\delta^2}$ 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 transcendence degree 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 $K[x_1, \ldots, x_n]$ (over a field K). 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 [1–6] that solve PIT. In a nutshell, the basic Schwartz–Zippel–DeMillo–Lipton test works as follows: Given a circuit $C(x_1, \ldots, x_n)$, check $C(\boldsymbol{a}) = 0$ for a random $\boldsymbol{a} \in S$, where $S \subset \overline{K}^n$ is a sufficiently large finite subset. 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, e.g. bipartite matching [7] and matrix completion [8,9], and connections to sought-after super-polynomial lower bounds [10,11]. Especially, *blackbox* PIT (i.e. the circuit C is given as a blackbox and we are only allowed to make oracle

☆ A preliminary version of this paper appeared in ICALP 2011.

* Corresponding author.
E-mail addresses: malte.beecken@hcm.uni-bonn.de (M. Beecken), johannes.mittmann@hcm.uni-bonn.de (J. Mittmann), nitin.saxena@hcm.uni-bonn.de (N. Saxena).

0890-5401/$ – see front matter
http://dx.doi.org/10.1016/j.ic.2012.10.004

queries) has direct connections to lower bounds [12,13]. By a blackbox PIT test for a family of circuits $\mathcal{F}$ we mean efficiently designing a *hitting set* $\mathcal{H} \subset \overline{K}^n$ such that: Given a non-zero $C \in \mathcal{F}$, there exists an $\boldsymbol{a} \in \mathcal{H}$ that *hits* C, i.e. $C(\boldsymbol{a}) \neq 0$.

The attempts to solve blackbox PIT have focused on restricted circuit families. A natural restriction is *constant depth*. Agrawal and Vinay [14] showed that a blackbox PIT algorithm for depth-4 circuits would (almost) solve PIT for low-degree circuits (and prove exponential circuit lower bounds). 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 [15–21]. 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 [22]. The latter is somewhat subsumed by the PIT algorithms for constant-read multilinear formulas [23]. To save space we would not go into the rich history of PIT and instead refer to the surveys [24,25].

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 $K[x_1,\ldots,x_n]$, 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 K^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*, 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 $f_1,\ldots,f_m \in K[x_1,\ldots,x_n]$. They are called *algebraically dependent* (over K) if there is a non-zero polynomial $F \in K[y_1,\ldots,y_m]$ such that $F(f_1,\ldots,f_m) = 0$. In this case, F is called an *annihilating polynomial* of $f_1,\ldots,f_m$. If such an annihilating polynomial does not exist, then $f_1,\ldots,f_m$ are called *algebraically independent* (over K). The *transcendence degree*, $\mathrm{trdeg}_K\{f_1,\ldots,f_m\}$, is the maximal number r of algebraically independent polynomials in the set $\{f_1,\ldots,f_m\}$. Though intuitive, it is non-trivial to prove that r is at most n.

The notion of transcendence degree has appeared in complexity theory in several contexts. Kalorkoti [26] used it to prove an $\Omega(n^3)$ formula size lower bound for the $n \times n$ determinant. In the works [27,28] studying the *entropy* of polynomial mappings $(f_1,\ldots,f_m) : K^n \to K^m$, transcendence degree is a natural measure of entropy when the field has large or zero characteristic. Finally, the complexity of the annihilating polynomial is studied in [29]. However, our work is the first to study transcendence degree in the context of PIT.

1.1. Our main results

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

Theorem 1. *Let C be an m-variate circuit. Let $f_1,\ldots,f_m$ be ℓ-sparse, degree-δ, n-variate polynomials of transcendence degree r. Suppose we have oracle access to the n-variate degree-d 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 that K has characteristic zero or larger than δ^r).*

We also give an algorithm that works for all fields, but has a worse time complexity. Note that the above theorem seems non-trivial even for a constant m, say $C' = C(f_1,f_2,f_3)$, as the output of C' may not be sparse and the f_i 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: $r \leqslant 3$.)

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

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

where $f_{i,j}$ 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 some progress.

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* by $\mathrm{rk}(C) := \mathrm{trdeg}_K\{f_{i,j} \mid i \in [k],\ \ j \in [s]\}$. 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 non-empty $I \subsetneq [k]$ such that $\sum_{i\in I} T_i = 0$. Define $R_\delta(k,s)$ to be the smallest $r \geqslant 1$ such that: Any $\Sigma\Pi\Sigma\Pi_\delta(k,s,n)$ circuit C that is simple, minimal and zero satisfies $\mathrm{rk}(C) < r$. If $\delta = 1$, these notions agree with the corresponding concepts for $\Sigma\Pi\Sigma$ circuits.

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

Again, we also give an algorithm that works for all fields, but has a worse time complexity. 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). In this sense, we generalize the state of

the art from depth-3 to depth-4 case. This theorem includes the known PIT vs. rank connection for depth-3 circuits. Furthermore, it is done in a seamless way by considering the notion of algebraic independence instead of linear independence. Our new techniques hold the promise of dealing with more complicated cases where δ is higher.

For the top fanin 2 case we obtain the following result that does not require a rank bound.

Corollary 3. *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 $C=0$.*

1.2. Organization and our approach

A priori it is not clear whether the problem of deciding algebraic independence of given polynomials $\{f_1,\ldots,f_m\}\subset K[x_1,\ldots,x_n]$ over a field K is even computable. Perron [30] proved that, for $m=n+1$, the annihilating polynomial has degree only exponential in n. We generalize this to any m in Section 2.1. This implies that deciding algebraic independence is a computable problem over any field (alternatively, Gröbner bases can be used). When the characteristic of K is zero or large enough, there is a more efficient criterion due to Jacobi [31] (Section 2.2). For using transcendence degree in PIT we also have to relate it to the *Krull dimension* of algebras (Section 2.3).

The central concept that we develop is that of a *faithful homomorphism*. An algebra homomorphism $\varphi: K[x_1,\ldots,x_n]\to K[z_1,\ldots,z_r]$ is faithful to polynomials $f_1,\ldots,f_m$ of transcendence degree $r\leqslant n$ if the images $\varphi(f_1),\ldots,\varphi(f_m)$ are of transcendence degree r, too. Additionally, to be useful, φ should be constructible in an efficient and blackbox way. We give such a construction in Section 3.2, establishing the following theorem.

Theorem 4. *For all $n,\delta,r\geqslant 1$ there exist an $N\geqslant 1$ and effective homomorphisms $\varphi_1,\ldots,\varphi_N: K[x_1,\ldots,x_n]\to K[z_1,\ldots,z_r]$ with the following property: For all polynomials $f_1,\ldots,f_m$ of degree at most δ and transcendence degree at most r there is an $i\in[N]$ such that φ_i is faithful to $f_1,\ldots,f_m$.*

Theorem 4 is proven as Lemma 22 (with an effective bound for N). If $f_1,\ldots,f_m$ are sparse and the characteristic of K is zero or large enough, a better bound for N can be given (see Lemma 23). The proofs use Perron's theorem and the Jacobian criterion, but require new techniques as well. The reason why faithful homomorphisms are useful in PIT is because they preserves the non-zeroness of a circuit $C(f_1,\ldots,f_m)$ (Theorem 14). We prove this by an application of *Krull's principal ideal theorem*.

Once the fundamental machinery is set up, we give two applications of faithful homomorphisms in Sections 4 and 5. In both applications, faithful homomorphisms are used to reduce the number of variables. Then the non-vanishing version of the *Combinatorial Nullstellensatz* (which is a consequence of the basic Schwartz–Zippel–DeMillo–Lipton Lemma) is used to design a hitting set. The proof of Theorem 1 is provided in Section 4.2, and the proofs of Theorem 2 and Corollary 3 are given in Section 5.4. In the time complexity estimates we prefer to give a 'clean' expression which in some cases might even be suboptimal.

2. Preliminaries – Perron, Jacobi and Krull

Let $n\geqslant 1$ and let K be a field of characteristic $\mathrm{char}(K)$. Throughout this paper, $K[\boldsymbol{x}]=K[x_1,\ldots,x_n]$ is a polynomial ring in n variables over K. The sparsity $\mathrm{sp}(f)$ of a polynomial $f\in K[\boldsymbol{x}]$ is the number of non-zero monomial terms. The algebraic closure of the field will be written as $\overline{K}$. We denote the multiplicative group of units of a ring R by R^*. For $0\leqslant r\leqslant n$, we use the notation $[r,n]:=\{r,\ldots,n\}$ and $[n]:=[1,n]$. By $\binom{[n]}{r}$ we denote the set of r-subsets of $[n]$. The symmetric group on $[n]$ will be written as $\mathfrak{S}_n$. The set of prime numbers will be denoted by $\mathbb{P}$.

2.1. Perron's theorem – arbitrary K

Let $f_1,\ldots,f_m\in K[\boldsymbol{x}]$ be polynomials. It is interesting to note that transcendence degree is invariant to *algebraic* field extensions, i.e. $\mathrm{trdeg}_K\{f_1,\ldots,f_m\}$ is the same as $\mathrm{trdeg}_{\overline{K}}\{f_1,\ldots,f_m\}$ (Lemma A.2). The name transcendence degree stems from field theory. The transcendence degree of a field extension L/K, denoted by $\mathrm{trdeg}(L/K)$, is the cardinality of any transcendence basis for L/K (for more information on transcendental extensions, see [32, Chap. 19]). For $L=K(f_1,\ldots,f_m)$, we have $\mathrm{trdeg}_K\{f_1,\ldots,f_m\}=\mathrm{trdeg}(L/K)$ (cf. [32, Theorem 19.14]). Since $\mathrm{trdeg}(K(\boldsymbol{x})/K)=n$, we obtain $0\leqslant\mathrm{trdeg}_K\{f_1,\ldots,f_m\}\leqslant n$.

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. [33, 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 5 *(Perron's theorem on algebraic independence). (See [34, Theorem 1.1].) Let $f_1,\ldots,f_{n+1}\in K[\boldsymbol{x}]$ be non-constant polynomials and let $\delta_i=\deg(f_i)$ 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*

$$\deg(F)\leqslant\frac{\delta_1\cdots\delta_{n+1}}{\min\{\delta_1,\ldots,\delta_{n+1}\}}\leqslant\big(\max\{\delta_1,\ldots,\delta_{n+1}\}\big)^n.$$

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 transcendence degree of the polynomials instead of the number of variables. We hereby improve [29, Theorem 11] and generalize it to arbitrary characteristic. The proof uses a result from Section 3 and is given in Appendix A.

Corollary 6 *(Degree bound for annihilating polynomials). Let $f_1, \ldots, f_m \in K[\boldsymbol{x}]$ be algebraically dependent polynomials of maximal degree $\delta \geqslant 1$. Then there exists a non-zero polynomial $F \in K[y_1, \ldots, y_m]$ such that $F(f_1, \ldots, f_m) = 0$ and*

$$\deg(F) \leqslant \delta^r,$$

where $r = \operatorname{trdeg}_K\{f_1, \ldots, f_m\}$.

Remark 7. The bound in Corollary 6 is tight. To see this, let $n \geqslant 2$, let $\delta \geqslant 1$ 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. The Jacobian criterion – large or zero char(K)

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

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

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

Theorem 8 *(Jacobian criterion). Let $f_1, \ldots, f_m \in K[\boldsymbol{x}]$ be polynomials of degree at most $\delta \geqslant 1$. Assume that $\operatorname{char}(K) = 0$ or $\operatorname{char}(K) > \delta^r$, where $r = \operatorname{trdeg}_K\{f_1, \ldots, f_m\}$. Then*

$$\operatorname{trdeg}_K\{f_1, \ldots, f_m\} = \operatorname{rk}_L J_{\boldsymbol{x}}(f_1, \ldots, f_m),$$

where $L = K(\boldsymbol{x})$.

In particular, if $f_1, \ldots, f_m$ are linear forms (i.e. homogeneous degree-1 polynomials), then their K-linear rank agrees with their transcendence degree.

A proof of the Jacobian criterion in characteristic 0 appears, for example, in [35] and the case of large prime characteristic was dealt with in [27]. By virtue of Theorem 5 our proof could tolerate a slightly smaller characteristic. For the reader's convenience, a full proof is given in Appendix B. We isolate the following special case of Theorem 8, because it holds in arbitrary characteristic.

Lemma 9. *Let $f_1, \ldots, f_m \in K[\boldsymbol{x}]$. Then*

$$\operatorname{trdeg}_K\{f_1, \ldots, f_m\} \geqslant \operatorname{rk}_L J_{\boldsymbol{x}}(f_1, \ldots, f_m),$$

where $L = K(\boldsymbol{x})$.

We conclude this section by stating the *chain rule* for partial derivatives. Let $f_1, \ldots, f_m \in K[\boldsymbol{x}]$ and let $F_1, \ldots, F_s \in K[\boldsymbol{y}] = K[y_1, \ldots, y_m]$. Then we have

$$J_{\boldsymbol{x}}\big(F_1(f_1, \ldots, f_m), \ldots, F_s(f_1, \ldots, f_m)\big) = \big(J_{\boldsymbol{y}}(F_1, \ldots, F_s)\big)(f_1, \ldots, f_m) \cdot J_{\boldsymbol{x}}(f_1, \ldots, f_m).$$

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 anymore). 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 the supremum

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

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 $r \geqslant 0$ 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 10 *(Dimension and transcendence degree). (See [36, Proposition 5.10].) Let $A = K[a_1, \ldots, a_m]$ be an affine K-algebra. Then* $\dim(A) = \operatorname{trdeg}_K(A) = \operatorname{trdeg}_K\{a_1, \ldots, a_m\}$.

The following corollary is a simple consequence of Theorem 10. It shows that homomorphisms cannot increase the dimension of affine algebras.

Corollary 11. *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* $\dim(\varphi(A)) \leqslant \dim(A)$. *If, in addition, φ is injective, then* $\dim(\varphi(A)) = \dim(A)$.

Proof. 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 10, 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, $\dim(\varphi(A)) \leqslant \dim(A)$.

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 $\dim(\varphi(A)) \geqslant \dim(A)$. □

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

Theorem 12 *(Krull's Hauptidealsatz). (See [37, Corollary 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 – or how to reduce the number of 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 $1 \leqslant r \leqslant n$. 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 13. 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, because it preserves the non-zeroness of a circuit $C(f_1, \ldots, f_m)$.

Theorem 14 *(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 10 and Corollary 11. 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 $f \notin A^* \cup \{0\}$. Since A is an affine domain, Theorem 12 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 11 implies

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

a contradiction. It follows that φ_A is injective. □

Corollary 15. *Let C be an m-variate circuit over K. Let φ be faithful to $\{f_1, \ldots, f_m\} \subset K[\boldsymbol{x}]$. Then, $C(f_1, \ldots, f_m) = 0$ if and only if $C(\varphi(f_1), \ldots, \varphi(f_m)) = 0$.*

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, by the theorem, φ is an isomorphism between these two algebras, the corollary is evident. □

3.1. Existence

The following lemma shows that even *linear* (i.e. the images of the variables are of degree at most 1) faithful homomorphisms exist for all subsets of polynomials, provided that K is large enough. It is a generalization of [29, Claim 11.1] to arbitrary characteristic.

Lemma 16 *(Existence). Let K be an infinite field and let $f_1, \ldots, f_m \in K[\boldsymbol{x}]$ be polynomials of transcendence degree 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. 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 $i \in [r]$, 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 viewed 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

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

for all $i \in [r]$. Now define the K-algebra homomorphism

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

Then we have $G_i(z_i, \varphi(f_1), \ldots, \varphi(f_r), c_{r+1}, \ldots, c_n) = 0$ and, by the choice of $c_{r+1}, \ldots, c_n$,

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

for all $i \in [r]$. This shows that z_i is algebraically dependent on $\varphi(f_1), \ldots, \varphi(f_r)$ for all $i \in [r]$. 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 $\{f_1, \ldots, f_m\}$. □

3.2. An explicit faithful homomorphism – stochastic matrix inspired

We will now give an explicit construction of a faithful homomorphism by mimicking the proof of Lemma 16. Let $1 \leqslant r \leqslant n$, let $K[z_0, \boldsymbol{z}] = K[z_0, z_1, \ldots, z_r]$ and let $\boldsymbol{t} = \{t_1, t_2, t_3\}$ be new indeterminates (*tag variables*).

Remark 17. As in Lemma 16, the field K will sometimes be required to be large enough. In those cases we will move to the algebraic closure $\overline{K}$. For algorithmic purposes, a large enough algebraic field extension can be constructed [38].

We construct a homomorphism in three steps. The final map (in Lemmas 22 and 23) will be a composition $\Psi \circ \Xi \circ \Lambda$ of three maps, some of which also depend on a few parameters. In the next two subsections we describe these maps and their properties. There are four maps – Ψ (it zeroes out some variables), Ξ (it relabels the variables depending on its parameter), Λ (it shifts each of the variables) and Γ (it is a homogenized version of Λ). They form the backbone of all our subsequent proofs. In particular, they are used with different parameters to design faithful maps in Lemma 22 (arbitrary characteristic) and Lemma 23 (characteristic zero or large). The latter, expectedly, is more efficient than the former.

We start with the map that is applied last. Define the $\overline{K}$-algebra homomorphism

$$\Psi : \overline{K}[\boldsymbol{x}, \boldsymbol{t}] \to \overline{K}[\boldsymbol{z}, \boldsymbol{t}], \qquad x_i \mapsto \begin{cases} z_i, & \text{if } i \in [r], \\ 0, & \text{if } i \in [r+1, n]. \end{cases}$$

Here we agree that, whenever we do not specify the image of a variable, this variable is mapped to itself (here $t_i \mapsto t_i$ for $i \in [3]$). It turns out that, after *shifting* the variables (homomorphism Λ in Section 3.2.2) and *mixing* them (homomorphism Ξ in Section 3.2.1), this projection is faithful to any set of transcendence degree at most r.

3.2.1. Mixing the variables – map Ξ

Now we will define a homomorphism that imitates the renumbering of variables that took place in the first step of the proof of Lemma 16. To this end, we will construct a matrix of univariate polynomials that interpolates the permutation matrices given by the renumberings.

Let $c : \binom{[n]}{r} \to \overline{K}$ be an injection that assigns a constant $c_I := c(I)$ to each r-subset $I \subseteq [n]$. It simply numbers r-subsets by field elements. Now let $I = \{i_1 < \cdots < i_r\} \in \binom{[n]}{r}$ and let $[n] \setminus I = \{i_{r+1} < \cdots < i_n\}$. Define the permutation $\pi_I : [n] \to [n]$, $i_j \mapsto j$ for $j \in [n]$. This assignment yields an injection $\binom{[n]}{r} \to \mathfrak{S}_n$, $I \mapsto \pi_I$ with the property $\pi_I(I) = [r]$.

For $i, j \in [n]$, let $a_{i,j} \in \overline{K}[t_1]$ be the unique polynomial of degree $\binom{n}{r} - 1$ satisfying

$$a_{i,j}(c_I) = \delta_{\pi_I(i),j} \quad \text{for all } I \in \binom{[n]}{r}.$$

That means, $(a_{i,j}(c_I))$ is the permutation matrix given by π_I. In particular, we have $\det(a_{i,j}(c_I)) = \operatorname{sgn}(\pi_I) \in \{-1, 1\}$, hence $\det(a_{i,j}) \neq 0$. The matrix $(a_{i,j})$ can be easily constructed by interpolation.

Remark 18. Another curious feature of the matrix $(a_{i,j})$ is the property $\sum_{j=1}^{n} a_{i,j} = 1$ for all $i \in [n]$, and $\sum_{i=1}^{n} a_{i,j} = 1$ for all $j \in [n]$. This follows from the fact that those polynomials are of degree at most $\binom{n}{r} - 1$ and evaluate to 1 for all $\binom{n}{r}$ points c_I. We say that $(a_{i,j})$ is a *generalized doubly stochastic* matrix.

Now we define the $\overline{K}$-algebra homomorphism

$$\Xi : \overline{K}[\boldsymbol{x}, \boldsymbol{t}] \to \overline{K}[\boldsymbol{x}, \boldsymbol{t}], \qquad x_i \mapsto \sum_{j=1}^{n} a_{i,j} x_j$$

for $i \in [n]$. For $i \in [n]$, we have $\deg(\Xi(x_i)) = \binom{n}{r}$, $\deg_{\boldsymbol{x}}(\Xi(x_i)) = 1$ and $\deg_{t_1}(\Xi(x_i)) = \binom{n}{r} - 1$. Finally, for $c \in \overline{K}$, define the substitution homomorphism

$$\Xi_c : \overline{K}[\boldsymbol{x}] \to \overline{K}[\boldsymbol{x}], \qquad f \mapsto \big(\Xi(f)\big)(\boldsymbol{x}, c).$$

By definition, Ξ_{c_I} is an automorphism sending the variables $\{x_i \mid i \in I\}$ to $\{x_i \mid i \in [r]\}$ and sending the variables $\{x_i \mid i \in [n] \setminus I\}$ to $\{x_i \mid i \in [r+1, n]\}$ (preserving the order of indices).

The map Ξ_c is an automorphism of $\overline{K}[\boldsymbol{x}]$ for almost all $c \in \overline{K}$. The following lemma bounds the number of bad choices for the parameter c (in the tag variable t_1).

Lemma 19. *There exists a subset $B_{t_1} \subset \overline{K}$ with $|B_{t_1}| < n\binom{n}{r}$ such that $\Xi_c : \overline{K}[\boldsymbol{x}] \to \overline{K}[\boldsymbol{x}]$ is an automorphism for all $c \in \overline{K} \setminus B_{t_1}$.*

Proof. Let $f := \det(a_{i,j}) \in \overline{K}[t_1]$. Since $f(c_{[r]}) = \det(a_{i,j}(c_{[r]})) = \det(\delta_{i,j}) = 1$, we have $f \neq 0$. Let $B_{t_1} \subset \overline{K}$ be the set of zeros of f. Then $|B_{t_1}| \leqslant \deg(f) < n\binom{n}{r}$. Thus, for $c \in \overline{K} \setminus B_{t_1}$, we have $f(c) \neq 0$, hence Ξ_c is an automorphism. □

3.2.2. Shifting the variables – maps Λ and Γ

Finally, we define a homomorphism Λ that efficiently transforms a non-zero sparse polynomial $f \in K[\boldsymbol{x}]$ in such a way that it does not vanish at the point $\mathbf{0} = \mathbf{0}_n = (0, \ldots, 0) \in K^n$. For this we use standard techniques from sparse PIT [39].

Let $D \geqslant 2$ and define the $\overline{K}$-algebra automorphism

$$\Lambda_D : \overline{K}[\boldsymbol{x}, \boldsymbol{t}] \to \overline{K}[\boldsymbol{x}, \boldsymbol{t}], \qquad x_i \mapsto x_i + t_2^{D^{i-1}}$$

for $i \in [n]$. Now let $p \geqslant 1$. For an integer $a \in \mathbb{Z}$, we denote by $\lfloor a \rfloor_p$ the integer $b \in \mathbb{Z}$ satisfying $0 \leqslant b < p$ and $a = b \pmod p$. We define the $\overline{K}$-algebra automorphism

$$\Lambda_{D,p} : \overline{K}[\boldsymbol{x}, \boldsymbol{t}] \to \overline{K}[\boldsymbol{x}, \boldsymbol{t}], \qquad x_i \mapsto x_i + t_2^{\lfloor D^{i-1} \rfloor_p}$$

for $i \in [n]$. Note that, for $f \in K[\boldsymbol{x}]$, $\Lambda_{D,p}(f)$ is a representative of the residue class $\Lambda_D(f) \pmod{\langle t_2^p - 1 \rangle_{\overline{K}[\boldsymbol{x}, t_2]}}$. Finally, for $c \in \overline{K}$, define the $\overline{K}$-algebra automorphism

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

For almost all $D \geqslant 2$, $p \in \mathbb{P}$ and $c \in \overline{K}$, this homomorphism shifts the variables of a non-zero polynomial $f \in K[\boldsymbol{x}]$ in such a way that it does not vanish at $\mathbf{0}$. The following lemma bounds the number of bad choices for the parameters p and c.

Lemma 20. *Let $f \in K[\boldsymbol{x}]$ be a non-zero polynomial of sparsity at most $\ell \geqslant 1$ and degree at most $\delta \geqslant 1$. Let $D \geqslant \delta + 1$.*

Then there exists a subset $B \subset \mathbb{P}$ of prime numbers with $|B| < n\ell \log_2 D$ satisfying the following property: For all $p \in \mathbb{P} \setminus B$ there exists a subset $B_{t_2} \subset \overline{K}$ with $|B_{t_2}| < \delta p$ such that

$$\big(\Lambda_{D,p,c}(f)\big)(\mathbf{0}) \neq 0$$

for all $c \in \overline{K} \setminus B_{t_2}$.

Proof. Let $g := (\Lambda_D(f))(\mathbf{0}) \in K[t_2]$. We have $g = f(t_2, t_2^D, \ldots, t_2^{D^{n-1}}) \neq 0$, because the map

$$[0,\delta]^n \to \mathbb{N}, \qquad (d_1, \ldots, d_n) \mapsto d_1 D^0 + d_2 D^1 + \cdots + d_n D^{n-1}$$

is injective and so all the monomials of f remain separated in g. This method is often referred to as a *Kronecker substitution* (in f). We have $\operatorname{sp}(g) = \operatorname{sp}(f) \leqslant \ell$ and $\deg(g) \leqslant \delta D^{n-1} < D^n$. Let $B \subset \mathbb{P}$ be the set of all primes p satisfying $g = 0 \pmod{\langle t_2^p - 1\rangle_{K[t_2]}}$. Then $|B| < n\ell \log_2 D$ by [39, Lemma 13].

Now let $p \in \mathbb{P} \setminus B$ and let $g_p := (\Lambda_{D,p}(f))(\mathbf{0}) \in K[t_2]$. We have $g_p = g \neq 0 \pmod{\langle t_2^p - 1\rangle_{K[t_2]}}$, thus $g_p \neq 0$. Let $B_{t_2} \subset \overline{K}$ be the set of all $c \in \overline{K}$ such that $g_p(c) = 0$. Then $|B_{t_2}| \leqslant \deg(g_p) < \delta p$. For $c \in \overline{K} \setminus B_{t_2}$ we have $(\Lambda_{D,p,c}(f))(\mathbf{0}) = g_p(c) \neq 0$, as desired. □

Now we will define a homogeneous version of Λ. It will be needed in Section 5.2. For $D \geqslant 2$ and $p \geqslant 1$, define the $\overline{K}$-algebra automorphisms

$$\Gamma_D : \overline{K}[z_0, \boldsymbol{x}, t_3] \to \overline{K}[z_0, \boldsymbol{x}, t_3], \qquad x_i \mapsto x_i + t_3^{D^{i-1}} z_0,$$
$$\Gamma_{D,p} : \overline{K}[z_0, \boldsymbol{x}, t_3] \to \overline{K}[z_0, \boldsymbol{x}, t_3], \qquad x_i \mapsto x_i + t_3^{\lfloor D^{i-1} \rfloor_p} z_0,$$

for $i \in [n]$. For $c \in \overline{K}$, define the $\overline{K}$-algebra automorphism

$$\Gamma_{D,p,c} : \overline{K}[z_0, \boldsymbol{x}] \to \overline{K}[z_0, \boldsymbol{x}], \qquad f \mapsto \big(\Gamma_{D,p}(f)\big)(z_0, \boldsymbol{x}, c).$$

Lemma 21. *Let $f \in K[\boldsymbol{x}]$ be a non-zero polynomial of sparsity at most $\ell \geqslant 1$ and degree at most $\delta \geqslant 1$. Let $D \geqslant \delta + 1$.*

Then there exists a subset $B \subset \mathbb{P}$ of prime numbers with $|B| < n\ell \log_2 D$ satisfying the following property: For all $p \in \mathbb{P} \setminus B$ there exists a subset $B_{t_3} \subset \overline{K}$ with $|B_{t_3}| < \delta p$ such that

$$\deg_{z_0}\big(\big(\Gamma_{D,p,c}(f)\big)(z_0, \mathbf{0})\big) = \deg_{z_0}\big(\Gamma_{D,p,c}(f)\big) = \deg\big(\Gamma_{D,p,c}(f)\big) = \deg(f)$$

for all $c \in \overline{K} \setminus B_{t_3}$.

Proof. Observe that the coefficient of the term $z_0^{\deg(f)}$ in $\Gamma_D(f)$ is $g(t_3, t_3^D, \ldots, t_3^{D^{n-1}})$, where $g \in K[\boldsymbol{x}] \setminus \{0\}$ is the homogeneous degree-$\deg(f)$ part of f. Now the assertion follows from Lemma 20. □

3.2.3. Proof of faithfulness

Now we are well equipped for showing the faithfulness of the composition $\Psi \circ \Xi \circ \Lambda$. Given polynomials $f_1, \ldots, f_m \in K[\boldsymbol{x}]$, the homomorphism $\Psi \circ \Xi_{c_1} \circ \Lambda_{D,p,c_2}$ is faithful to $\{f_1, \ldots, f_m\}$ for almost all $D \geqslant 2$, $p \in \mathbb{P}$ and $c_1, c_2 \in \overline{K}$. In arbitrary characteristic, the following lemma bounds the number of bad choices for the parameters p and c_1, c_2. This also proves Theorem 4.

Lemma 22. *Let $f_1, \ldots, f_m \in K[\boldsymbol{x}]$ be polynomials of degree at most $\delta \geqslant 1$ and transcendence degree at most r. Let $D \geqslant \delta^{r+1} + 1$.*

Then there exists a set $B \subset \mathbb{P}$ of prime numbers with $|B| < rn\binom{n+\delta^{r+1}}{\delta^{r+1}} \log_2 D$ satisfying the following property: For all $p \in \mathbb{P} \setminus B$ there exist subsets $B_{t_1}, B_{t_2} \subset \overline{K}$ with $|B_{t_1}| < r\delta^{r+1}\binom{n}{r}^{r+1}$ and $|B_{t_2}| < r\delta^{r+1} p$ such that

$$\Psi \circ \Xi_{c_1} \circ \Lambda_{D,p,c_2} \text{ is faithful to } \{f_1, \ldots, f_m\}$$

for all $c_1 \in \overline{K} \setminus B_{t_1}$ and $c_2 \in \overline{K} \setminus B_{t_2}$.

Proof. We may assume that $f_1, \ldots, f_r$ are algebraically independent (if the transcendence degree is smaller than r, we can add algebraically independent variables). Let $I = \{i_1 < \cdots < i_r\} \in \binom{[n]}{r}$ be an index set with complement $[n] \setminus I = \{i_{r+1} < \cdots < i_n\}$ such that $f_1, \ldots, f_r, x_{i_{r+1}}, \ldots, x_{i_n}$ are algebraically independent. Then, for $j \in [r]$, there exists a non-zero polynomial $G_j \in K[y_0, \boldsymbol{y}] = K[y_0, y_1, \ldots, y_n]$ such that $\deg_{y_0}(G_j) > 0$, $\deg(G_j) \leqslant \delta^r$ (by Theorem 5) and

$$G_j(x_{i_j}, f_1, \ldots, f_r, x_{i_{r+1}}, \ldots, x_{i_n}) = 0. \tag{2}$$

Denote by $g_j \in K[\boldsymbol{y}]$ the (non-zero) leading coefficient of G_j viewed as a polynomial in y_0 with coefficients in $K[\boldsymbol{y}]$. Since $f_1, \ldots, f_r, x_{i_{r+1}}, \ldots, x_{i_n}$ are algebraically independent, the polynomial

$$g'_j := g_j(f_1, \ldots, f_r, x_{i_{r+1}}, \ldots, x_{i_n}) \in K[\boldsymbol{x}]$$

is non-zero. We have $\deg(g'_j) \leqslant \delta^{r+1}$ and hence we can bound the sparsity of g'_j in a trivial way by $\operatorname{sp}(g'_j) \leqslant \binom{n+\delta^{r+1}}{\delta^{r+1}}$. Applying Lemma 20 to g'_j provides a set $B_j \subset \mathbb{P}$ of prime numbers with $|B_j| < n\binom{n+\delta^{r+1}}{\delta^{r+1}} \log_2 D$. Set $B := B_1 \cup \cdots \cup B_r$ and let $p \in \mathbb{P} \setminus B$. For $j \in [r]$, let $B_{t_2,j} \subset \overline{K}$ be the subset with $|B_{t_2,j}| < \delta^{r+1} p$ provided by Lemma 20 applied to g'_j. Set $B_{t_2} := B_{t_2,1} \cup \cdots \cup B_{t_2,r}$ and let $c_2 \in \overline{K} \setminus B_{t_2}$. Then $(\Lambda_{D,p,c_2}(g'_j))(\mathbf{0}) \neq 0$ for all $j \in [r]$.

We want to show that $\Psi \circ \Xi \circ \Lambda_{D,p,c_2}$ is faithful to $\{f_1, \ldots, f_r\}$. Denote $\boldsymbol{f} = (f_1, \ldots, f_r)$ and let $j \in [r]$. Applying $\Psi \circ \Xi_{c_I} \circ \Lambda_{D,p,c_2}$ to (2) yields

$$\begin{aligned} 0 &= \Psi\big(G_j\big(x_j + c_2^{\lfloor D^{i_j-1} \rfloor_p}, (\Xi_{c_I} \circ \Lambda_{D,p,c_2})(\boldsymbol{f}), x_{r+1} + c_2^{\lfloor D^{i_{r+1}-1} \rfloor_p}, \ldots, x_n + c_2^{\lfloor D^{i_n-1} \rfloor_p}\big)\big) \\ &= G_j\big(z_j + c_2^{\lfloor D^{i_j-1} \rfloor_p}, (\Psi \circ \Xi_{c_I} \circ \Lambda_{D,p,c_2})(\boldsymbol{f}), c_2^{\lfloor D^{i_{r+1}-1} \rfloor_p}, \ldots, c_2^{\lfloor D^{i_n-1} \rfloor_p}\big). \end{aligned} \tag{3}$$

On the other hand, we have

$$G_j\big(y_0, (\Psi \circ \Xi_{c_I} \circ \Lambda_{D,p,c_2})(\boldsymbol{f}), c_2^{\lfloor D^{i_{r+1}-1} \rfloor_p}, \ldots, c_2^{\lfloor D^{i_n-1} \rfloor_p}\big) \neq 0, \tag{4}$$

because $(\Psi \circ \Xi_{c_I} \circ \Lambda_{D,p,c_2})(g'_j) \neq 0$. The latter follows from $(\Lambda_{D,p,c_2}(g'_j))(\mathbf{0}) \neq 0$, because $((\Psi \circ \Xi_{c_I})(x_i))(\mathbf{0}) = 0$ for all $i \in [n]$. Eqs. (3) and (4) show that z_j is algebraically dependent on $(\Psi \circ \Xi_{c_I} \circ \Lambda_{D,p,c_2})(f_1), \ldots, (\Psi \circ \Xi_{c_I} \circ \Lambda_{D,p,c_2})(f_r)$ for all $j \in [r]$. Hence $\Psi \circ \Xi_{c_I} \circ \Lambda_{D,p,c_2}$ is faithful to $\{f_1, \ldots, f_r\}$ and this implies that $\Psi \circ \Xi \circ \Lambda_{D,p,c_2}$ is faithful to $\{f_1, \ldots, f_r\}$ (otherwise the substitution $t_1 \mapsto c_I$ would increment the transcendence degree, which is impossible by Corollary 11).

It remains to show that $\Psi \circ \Xi_c \circ \Lambda_{D,p,c_2}$ is faithful to $\{f_1, \ldots, f_r\}$ for almost all $c \in \overline{K}$. Denote $f'_i := (\Psi \circ \Xi \circ \Lambda_{D,p,c_2})(f_i) \in \overline{K}[\boldsymbol{z}, t_1]$ for $i \in [r]$. We first show that $f'_1, \ldots, f'_r, t_1$ are algebraically independent. To this end, assume that t_1 is algebraically dependent on $f'_1, \ldots, f'_r$. Then there exists a non-zero polynomial $H \in \overline{K}[y_0, \boldsymbol{y}] = \overline{K}[y_0, y_1, \ldots, y_r]$ such that $\deg_{y_0}(H) > 0$ and $H(t_1, f'_1, \ldots, f'_r) = 0$. Since $y_0 - c_I$ is transcendental, we may assume that $y_0 - c_I$ does not divide H. Therefore, the polynomial $H' := H(c_I, \boldsymbol{y}) \in \overline{K}[\boldsymbol{y}]$ is non-zero. Above we showed that $f'_1(\boldsymbol{z}, c_I), \ldots, f'_r(\boldsymbol{z}, c_I)$ are algebraically independent. We arrived at the contradiction

$$H'\big(f'_1(\boldsymbol{z}, c_I), \ldots, f'_r(\boldsymbol{z}, c_I)\big) = \big(H\big(t_1, f'_1, \ldots, f'_r\big)\big)(\boldsymbol{z}, c_I) = 0,$$

hence $f'_1, \ldots, f'_r, t_1$ are algebraically independent. Now we can proceed as above. For $i \in [r]$, there exist non-zero polynomials $H_i \in \overline{K}[y_0, \boldsymbol{y}] = \overline{K}[y_0, y_1, \ldots, y_{r+1}]$ such that $\deg_{y_0}(H_i) > 0$, $\deg(H_i) \leqslant \delta^r \binom{n}{r}^r$ (by Theorem 5) and $H_i(z_i, f'_1, \ldots, f'_r, t_1) = 0$. Denote by $h_i \in \overline{K}[\boldsymbol{y}]$ the (non-zero) leading coefficient of H_i as a polynomial in z_0 with coefficients in $\overline{K}[\boldsymbol{y}]$. Since $f'_1, \ldots, f'_r, t_1$ are algebraically independent, the polynomial $h'_i := h_i(f'_1, \ldots, f'_r, t_1) \in \overline{K}[\boldsymbol{z}, t_1]$ is non-zero. Let $B_{t_1,i} \subset \overline{K}$ be the subset of all $c \in \overline{K}$ such that $h'_i(\boldsymbol{z}, c) = 0$. Then $|B_{t_1,i}| \leqslant \deg_{t_1}(h'_i) < \delta^{r+1}\binom{n}{r}^{r+1}$. Set $B_{t_1} := B_{t_1,1} \cup \cdots \cup B_{t_1,r}$ and let $c_1 \in \overline{K} \setminus B_{t_1}$. It follows that z_i is algebraically dependent on $f'_1(\boldsymbol{z}, c_1), \ldots, f'_r(\boldsymbol{z}, c_1)$ for all $i \in [r]$. This means that $\Psi \circ \Xi_{c_1} \circ \Lambda_{D,p,c_2}$ is faithful to $\{f_1, \ldots, f_r\}$. □

In characteristic zero and large prime characteristic, a more efficient version of Lemma 22 can be given. The reason is that we can work with the Jacobian criterion instead of the degree bound for annihilating polynomials.

Lemma 23. *Let $f_1, \ldots, f_m \in K[\boldsymbol{x}]$ be polynomials of sparsity at most $\ell \geqslant 1$, degree at most $\delta \geqslant 1$ and transcendence degree at most r. Assume that $\operatorname{char}(K) = 0$ or $\operatorname{char}(K) > \delta^r$. Let $D \geqslant \delta r + 1$.*

Then there exists a set $B \subset \mathbb{P}$ of prime numbers with $|B| < r!n\ell^r \log_2 D$ satisfying the following property. For all $p \in \mathbb{P} \setminus B$ there exist subsets $B_{t_1}, B_{t_2} \subset \overline{K}$ with $|B_{t_1}| < r\binom{n}{r}$ and $|B_{t_2}| < r\delta p$ such that

$$\Psi \circ \Xi_{c_1} \circ \Lambda_{D,p,c_2} \text{ is faithful to } \{f_1, \ldots, f_m\}$$

for all $c_1 \in \overline{K} \setminus B_{t_1}$ and $c_2 \in \overline{K} \setminus B_{t_2}$.

Proof. We may assume that $f_1, \ldots, f_r$ are algebraically independent (if the transcendence degree is smaller than r, we can add algebraically independent variables). Let $I = \{i_1 < \cdots < i_r\} \in \binom{[n]}{r}$ be an index set with complement $[n] \setminus I = \{i_{r+1} < \cdots < i_n\}$ such that $f_1, \ldots, f_r, x_{i_{r+1}}, \ldots, x_{i_n}$ are algebraically independent.

We denote $\boldsymbol{f} = (f_1, \ldots, f_r)$. By the Jacobian criterion, the polynomial $g := \det J_{x_{i_1}, \ldots, x_{i_r}}(\boldsymbol{f}) \in K[\boldsymbol{x}]$ is non-zero. We have $\deg(g) \leqslant r\delta$ and $\operatorname{sp}(g) \leqslant r!\ell^r$. Applying Lemma 20 to g provides a set $B \subset \mathbb{P}$ of prime numbers with $|B| < r!n\ell^r \log_2 D$. Let $p \in \mathbb{P} \setminus B$ and let $B_{t_2} \subset \overline{K}$ with $|B_{t_2}| < r\delta p$ be the subset provided by Lemma 20. Let $c_2 \in \overline{K} \setminus B_{t_2}$. Then $(\Lambda_{D,p,c_2}(g))(\mathbf{0}) \neq 0$.

By the chain rule, we have

$$J_{\boldsymbol{z}}\big((\Psi\circ\Xi\circ\Lambda_{D,p,c_2})(\boldsymbol{f})\big)=\Psi\big(J_{\boldsymbol{x}}\big((\Xi\circ\Lambda_{D,p,c_2})(\boldsymbol{f})\big)\big)\cdot\begin{pmatrix}I_r\\ \mathbf{0}_{(n-r)\times r}\end{pmatrix}$$
$$=\Psi\big(J_{x_1,\ldots,x_r}\big((\Xi\circ\Lambda_{D,p,c_2})(\boldsymbol{f})\big)\big).$$

Denote $h:=\det J_{x_1,\ldots,x_r}((\Xi\circ\Lambda_{D,p,c_2})(\boldsymbol{f}))\in K[\boldsymbol{x},t_1]$. Again, by the chain rule, we have

$$J_{x_1,\ldots,x_r}\big((\Xi\circ\Lambda_{D,p,c_2})(\boldsymbol{f})\big)=(\Xi\circ\Lambda_{D,p,c_2})\big(J_{\boldsymbol{x}}(\boldsymbol{f})\big)\cdot(a_{j,k})_{1\leqslant j\leqslant n,\ 1\leqslant k\leqslant r}.$$

Using the Cauchy–Binet formula (cf. [40]), we obtain

$$h=\sum_{1\leqslant j_1<\cdots<j_r\leqslant n}\big((\Xi\circ\Lambda_{D,p,c_2})\big(\det J_{x_{j_1},\ldots,x_{j_r}}(\boldsymbol{f})\big)\big)\cdot\det(a_{j_q,k})_{1\leqslant q,k\leqslant r}.$$

By the definition of $a_{j,k}\in\overline{K}[t_1]$, we have $\det(a_{j_q,k}(c_I))_{1\leqslant q,\ k\leqslant r}\neq 0$ if and only if $i_q=j_q$ for all $q\in[r]$ (because, in the k-th column, 1 appears only at row $\pi_I^{-1}(k)=i_k$, and we assumed $i_1<\cdots<i_r$ and $j_1<\cdots<j_r$). Therefore,

$$h(\boldsymbol{x},c_I)=(\Xi_{c_I}\circ\Lambda_{D,p,c_2})\big(\det J_{x_{i_1},\ldots,x_{i_r}}(\boldsymbol{f})\big)\cdot\operatorname{sgn}(\pi_I)$$
$$=(\Xi_{c_I}\circ\Lambda_{D,p,c_2})(g)\cdot\operatorname{sgn}(\pi_I)$$
$$\neq 0.$$

Since $(\Xi_{c_I}(x_i))(\mathbf{0})=0$ for all $i\in[n]$, we also have $h(\mathbf{0},c_I)\neq 0$. Thus $h(\mathbf{0},t_1)\neq 0$. Let $B_{t_1}\subset\overline{K}$ be the set of all $c\in\overline{K}$ such that $h(\mathbf{0},c)=0$. Then $|B_{t_1}|\leqslant\deg_{t_1}(h(\mathbf{0},t_1))\leqslant\deg(\det(a_{j_q,k})_{1\leqslant q,\ k\leqslant r})<r\binom{n}{r}$. Now let $c_1\in\overline{K}\setminus B_{t_1}$. Then

$$\det J_{\boldsymbol{z}}\big((\Psi\circ\Xi_{c_1}\circ\Lambda_{D,p,c_2})(\boldsymbol{f})\big)=\Psi\big(\det J_{x_1,\ldots,x_r}\big((\Xi_{c_1}\circ\Lambda_{D,p,c_2})(\boldsymbol{f})\big)\big)$$
$$=\Psi\big(h(\boldsymbol{x},c_1)\big)$$
$$=h(\boldsymbol{z},\mathbf{0}_{n-r},c_1)\neq 0.$$

The assertion, that $\Psi\circ\Xi_{c_1}\circ\Lambda_{D,p,c_2}$ is faithful to $\boldsymbol{f}$, now follows from the Jacobian criterion. □

4. Circuits with sparse inputs of small transcendence degree

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. We denote the class of those circuits by $\mathcal{F}_{d,r,\delta,\ell}$.

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, provided by the non-vanishing version of the Combinatorial Nullstellensatz (a consequence of the Schwartz–Zippel–DeMillo–Lipton Lemma).

Lemma 24 *(Combinatorial Nullstellensatz). (See [41, Lemma 2.1].) Let $H\subset\overline{K}$ be a subset of size $d+1$. Then $\mathcal{H}=H^r$ is a hitting set for $\{f\in K[z_1,\ldots,z_r]\mid\deg(f)\leqslant d\}$.*

We will also require a bound for the number of primes in an interval.

Lemma 25. *Let $k\geqslant 2$. Then the set $[k^2]$ contains at least k prime numbers.*

Proof. For $k=2,3,4$ this can be verified directly. So let $k\geqslant 5$. Then, by [42, Corollary 1, (3.5)], the set $[k^2]$ contains at least $k^2/\log_e(k^2)\geqslant k$ prime numbers. □

4.1. A hitting set (arbitrary characteristic)

Let $n,d,r,\delta\geqslant 1$ and let $K[\boldsymbol{z}]=K[z_1,\ldots,z_r]$. To use the map $\Psi\circ\Xi\circ\Lambda$ defined in Section 3.2 we introduce the following parameters.

(1) Define $D:=\delta^{r+1}+1$.
(2) Define $p_{\max}:=(rn(n+\delta^{r+1})^{\delta^{r+1}}\lceil\log_2 D\rceil+1)^2$.
(3) Pick arbitrary $H_1,H_2,H_3\subset\overline{K}$ of sizes $(\delta n)^{r^2+r}$, $r\delta^{r+1}p_{\max}$ and $d+1$, respectively.

Denote $\Phi_{p,c_1,c_2} := \Psi \circ \Xi_{c_1} \circ \Lambda_{D,p,c_2}$ and $\Phi^{(i)}_{p,c_1,c_2} := (\Phi_{p,c_1,c_2})(x_i) \in \overline{K}[\boldsymbol{z}]$ for $i \in [n]$. Define the subset

$$\mathcal{H}_{d,r,\delta} = \left\{ \left(\Phi^{(1)}_{p,c_1,c_2}(\boldsymbol{a}), \ldots, \Phi^{(n)}_{p,c_1,c_2}(\boldsymbol{a}) \right) \mid p \in [p_{\max}],\ (c_1,c_2) \in H_1 \times H_2,\ \boldsymbol{a} \in H_3^r \right\} \subset \overline{K}^n.$$

The following theorem shows that this is a hitting set for $\mathcal{F}_{d,r,\delta,\ell}$. This construction is efficient for δ, r constant and d polynomial in the input size. In this case ℓ is also polynomial in the input size and thus does not appear.

Theorem 26. *The set $\mathcal{H}_{d,r,\delta}$ is a hitting set for $\mathcal{F}_{d,r,\delta,\ell}$. It can be constructed in* $\mathrm{poly}(dr\delta n)^{r^2\delta^{r+1}}$ *time.*

Proof. Let $C(f_1,\ldots,f_m) \in \mathcal{F}_{d,r,\delta,\ell}$ be a non-zero circuit. By Lemma 25, the set $[p_{\max}]$ contains at least $rn(n+\delta^{r+1})^{\delta^{r+1}} \log_2 D + 1$ primes. By Lemma 22, there exist $p \in [p_{\max}]$ and $(c_1,c_2) \in H_1 \times H_2$ such that Φ_{p,c_1,c_2} is faithful to $\{f_1,\ldots,f_m\}$. Hence, by Theorem 14,

$$\Phi_{p,c_1,c_2}\big(C(f_1,\ldots,f_m)\big) = C\big(\Phi_{p,c_1,c_2}(f_1),\ldots,\Phi_{p,c_1,c_2}(f_m)\big)$$

is a non-zero circuit with at most r variables and of degree at most d. Now the first assertion follows from Lemma 24. The second assertion is obvious from the construction. □

4.2. A hitting set (zero or large characteristic)

If $\mathrm{char}(K)$ is zero or large enough, we can give a more efficient hitting set construction. Let $n,d,r,\delta,\ell \geqslant 1$ and let $K[\boldsymbol{z}] = K[z_1,\ldots,z_r]$. Again, we use the map $\Psi \circ \Xi \circ \Lambda$ defined in Section 3.2. We introduce the following parameters.

(1) Define $D := \delta r + 1$.
(2) Define $p_{\max} := (n(r\ell)^r \lceil \log_2 D \rceil + 1)^2$.
(3) Pick arbitrary $H_1, H_2, H_3 \subset \overline{K}$ of sizes n^r, $r\delta p_{\max}$ and $d+1$, respectively.

Denote $\Phi_{p,c_1,c_2} := \Psi \circ \Xi_{c_1} \circ \Lambda_{D,p,c_2}$ and $\Phi^{(i)}_{p,c_1,c_2} := (\Phi_{p,c_1,c_2})(x_i) \in \overline{K}[\boldsymbol{z}]$ for $i \in [n]$. Define the subset

$$\mathcal{H}_{d,r,\delta,\ell} = \left\{ \left(\Phi^{(1)}_{p,c_1,c_2}(\boldsymbol{a}), \ldots, \Phi^{(n)}_{p,c_1,c_2}(\boldsymbol{a}) \right) \mid p \in [p_{\max}],\ (c_1,c_2) \in H_1 \times H_2,\ \boldsymbol{a} \in H_3^r \right\} \subset \overline{K}^n.$$

The following theorem shows that, over a large or zero characteristic, this is a hitting set for $\mathcal{F}_{d,r,\delta,\ell}$. This proves Theorem 1. This construction is efficient for r constant and ℓ, d polynomial in the input size.

Theorem 27. *Assume that* $\mathrm{char}(K) = 0$ *or* $\mathrm{char}(K) > \delta^r$. *Then $\mathcal{H}_{d,r,\delta,\ell}$ is a hitting set for $\mathcal{F}_{d,r,\delta,\ell}$. It can be constructed in* $\mathrm{poly}(dr\delta\ell n)^r$ *time.*

Proof. Let $C(f_1,\ldots,f_m) \in \mathcal{F}_{d,r,\delta,\ell}$ be a non-zero circuit. By Lemma 25, the set $[p_{\max}]$ contains at least $n(r\ell)^r \lceil \log_2 D \rceil + 1$ primes. By Lemma 23, there exist $p \in [p_{\max}]$ and $(c_1,c_2) \in H_1 \times H_2$ such that Φ_{p,c_1,c_2} is faithful to $\{f_1,\ldots,f_m\}$. Hence, by Theorem 14,

$$\Phi_{p,c_1,c_2}\big(C(f_1,\ldots,f_m)\big) = C\big(\Phi_{p,c_1,c_2}(f_1),\ldots,\Phi_{p,c_1,c_2}(f_m)\big)$$

is a non-zero circuit with at most r variables and of degree at most d. Now the first assertion follows from Lemma 24. The second assertion is obvious from the construction. □

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 Section 1.1. Note that the parameters bound the circuit degree, $\deg(C) \leqslant \delta s$. 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 non-zero). 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 $C_I \neq 0$ 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,

$R_\delta(k,s) \leqslant ks$, because $|\mathcal{S}(C)| \leqslant ks$ for all $C \in \Sigma\Pi\Sigma\Pi_\delta(k,s,n)$ and $\mathcal{S}(C)$ cannot be algebraically independent if $C = 0$. Since the K-linear rank of linear forms agrees with their transcendence degree, better upper bounds for $R_1(k,s)$ can be obtained from the rank bounds for $\Sigma\Pi\Sigma$ circuits. By [20], we have $R_1(k,s) = O(k^2 \log s)$ for arbitrary fields K, and $R_1(k,s) = O(k^2)$ for $K = \mathbb{R}$.

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 [18], we obtain the lower bound $R_1(k,s) = \Omega(k)$ if $\operatorname{char}(K) = 0$, and $R_1(k,s) = \Omega(k \log_p s)$ if $\operatorname{char}(K) = p > 0$. 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 $\operatorname{char}(K) = 0$, and $R_\delta(k,s) = \Omega(\delta k \log_p s)$ if $\operatorname{char}(K) = p > 0$. This leads us to the following natural conjecture.

Conjecture 28. *We have*

$$R_\delta(k,s) = \begin{cases} \operatorname{poly}(\delta k), & \text{if } \operatorname{char}(K) = 0, \\ \operatorname{poly}(\delta k \log_p s), & \text{if } \operatorname{char}(K) = p > 0. \end{cases}$$

Note that we expect $R_\delta(k,s)$ to be independent of s in characteristic 0. This is in accordance with the experience from depth-3 circuits.

The following lemma is a vast generalization of [17, 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 homomorphism that reduces the number of variables from n to $R_\delta(k,s)+1$.

Lemma 29. *Let C be a $\Sigma\Pi\Sigma\Pi_\delta(k,s,n)$ circuit, let $r := R_\delta(k,s)$ and let $\varphi : K[\boldsymbol{x}] \to K[z_0,\boldsymbol{z}] = K[z_0,z_1,\ldots,z_r]$ be a linear K-algebra homomorphism that, for all $I \subseteq [k]$, satisfies*

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

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), $\varphi(\operatorname{sim}(C_I)) = \operatorname{sim}(\varphi(C_I))$ is a minimal and simple circuit computing the zero polynomial. Note that $\varphi(\operatorname{sim}(C_I)) \in \Sigma\Pi\Sigma\Pi_\delta(k,s,n)$, because φ is a linear homomorphism. Hence, $\operatorname{rk}(\varphi(\operatorname{sim}(C_I))) < R_\delta(k,s)$. By assumption (2), this implies $\operatorname{rk}(\varphi(\operatorname{sim}(C_I))) = \operatorname{rk}(\operatorname{sim}(C_I))$, thus φ is faithful to $\mathcal{S}(\operatorname{sim}(C_I))$. Theorem 14 yields $\operatorname{sim}(C_I) = 0$, 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. □

5.2. Preserving the simple part – using the map Γ

The following lemma shows that $\Psi \circ \Xi_{c_1} \circ \Lambda_{D_2,p_2,c_2} \circ \Gamma_{D_3,p_3,c_3}$ meets condition (1) of Lemma 29 for almost all $D_2, D_3 \geqslant 2$, $p_2, p_3 \in \mathbb{P}$ and $c_1, c_2, c_3 \in \overline{K}$. It is also the key for the top fanin 2 case (Corollary 33). The proof is via *resultants*. For more information about resultants, see [43].

Lemma 30. *Let C be a $\Sigma\Pi\Sigma\Pi_\delta(k,s,n)$ circuit. Let $D_2 \geqslant 2\delta^2+1$ and let $D_3 \geqslant \delta+1$. Let $\Phi : \overline{K}[z_0,\boldsymbol{x}] \to \overline{K}[z_0,\boldsymbol{z}]$ be a $\overline{K}$-algebra homomorphism such that $\Phi(z_0) = z_0$ and for all $i \in [n]$ we have $\Phi(x_i) \in \overline{K}[\boldsymbol{z}]$ and $(\Phi(x_i))(\mathbf{0}) = 0$.*

Then there exists $B_3 \subset \mathbb{P}$ with $|B_3| < ks\delta n\binom{n+\delta}{\delta} \log_2 D_3$ such that, for all $p_3 \in \mathbb{P} \setminus B_3$ there exists $B_{t_3} \subset \overline{K}$ with $|B_{t_3}| < ks\delta^2 p_3$, such that, for all $c_3 \in \overline{K} \setminus B_{t_3}$ there exists $B_2 \subset \mathbb{P}$ with $|B_2| < \binom{ks\delta}{2} n\binom{n+2\delta^2}{2\delta^2} \log_2 D_2$ satisfying the following property: For all $p_2 \in \mathbb{P} \setminus B_2$ there exists $B_{t_2} \subset \overline{K}$ with $|B_{t_2}| < \binom{ks\delta}{2} 2\delta^2 p_2$ such that

$$(\Phi \circ \Lambda_{D_2,p_2,c_2} \circ \Gamma_{D_3,p_3,c_3})\big(\operatorname{sim}(C)\big) = \operatorname{sim}\big((\Phi \circ \Lambda_{D_2,p_2,c_2} \circ \Gamma_{D_3,p_3,c_3})(C)\big)$$

for all $c_2 \in \overline{K} \setminus B_{t_2}$.

Proof. Let $f_1,\ldots,f_m \in \overline{K}[\boldsymbol{x}]$ be the non-constant *absolutely irreducible* factors of the polynomials in $\mathcal{S}(C)$. Then $m \leqslant ks\delta$ and we have, for all $i \in [m]$, $\deg(f_i) \leqslant \delta$ and $\operatorname{sp}(f_i) \leqslant \binom{n+\delta}{\delta}$.

First we make the following observation. If $\varphi : \overline{K}[\boldsymbol{x}] \to \overline{K}[z_0,\boldsymbol{z}]$ is a $\overline{K}$-algebra homomorphism such that

(1) $\varphi(f_i)$ is non-constant for all $i \in [m]$, and
(2) $\gcd(f_i,f_j) = 1$ implies $\gcd(\varphi(f_i),\varphi(f_j)) = 1$ for all $i,j \in [m]$ with $i < j$,

then $\varphi(\mathrm{sim}(C)) = \mathrm{sim}(\varphi(C))$. To achieve the first condition, we will apply Lemma 21 to $f_1, \ldots, f_m$. To preserve the gcd of a pair f_i, f_j, we will apply Lemma 20 on the mutual resultants of $(\Gamma_{D_3,p_3,c_3})(f_i)$'s with respect to z_0.

For $i \in [m]$, applying Lemma 21 to f_i provides a set $B_{3,i} \subset \mathbb{P}$ of prime numbers with $|B_{3,i}| < n\binom{n+\delta}{\delta}\log_2 D_3$. Set $B_3 := B_{3,1} \cup \cdots \cup B_{3,m}$ and let $p_3 \in \mathbb{P} \setminus B_3$. For $i \in [m]$, let $B_{t_3,i} \subset \overline{K}$ be the subset with $|B_{t_3,i}| < \delta p_3$ provided by Lemma 21 applied to f_i. Set $B_{t_3} := B_{t_3,1} \cup \cdots \cup B_{t_3,m}$ and let $c_3 \in \overline{K} \setminus B_{t_3}$. For $i \in [m]$, let $g_i := (\Gamma_{D_3,p_3,c_3})(f_i) \in \overline{K}[z_0, \boldsymbol{x}]$. Then $\deg_{z_0}(g_i) = \deg(g_i) = \deg(f_i)$.

Now let $i, j \in [m]$ with $i < j$ such that $\gcd(f_i, f_j) = 1$ in $\overline{K}[\boldsymbol{x}]$. Since Γ_{D_3,p_3,c_3} is an automorphism of $\overline{K}[z_0, \boldsymbol{x}]$, we also have $\gcd(g_i, g_j) = 1$. By [43, Chap. 3, §6, Proposition 1], the polynomial $g_{i,j} := \mathrm{res}_{z_0}(g_i, g_j) \in \overline{K}[\boldsymbol{x}]$ is non-zero. We have $\deg(g_{i,j}) \leqslant 2\delta^2$ and thus $\mathrm{sp}(g_{i,j}) \leqslant \binom{n+2\delta^2}{2\delta^2}$. Applying Lemma 20 to $g_{i,j}$ provides a set $B_{2,i,j} \subset \mathbb{P}$ of prime numbers with $|B_{2,i,j}| < n\binom{n+2\delta^2}{2\delta^2}\log_2 D_2$. Set $B_2 := \bigcup_{i,j} B_{2,i,j}$, where the union is over all $i, j \in [m]$ as above, and let $p_2 \in \mathbb{P} \setminus B_2$. For $i, j \in [m]$ as above, let $B_{t_2,i,j} \subset \overline{K}$ be the subset with $|B_{t_2,i,j}| < 2\delta^2 p_2$ provided by Lemma 20 applied to $g_{i,j}$. Set $B_{t_2} := \bigcup_{i,j} B_{t_2,i,j}$, where the union is over all $i, j \in [m]$ as above, and let $c_2 \in \overline{K} \setminus B_{t_2}$. Then, for $i, j \in [m]$ as above, we have $(\Lambda_{D_2,p_2,c_2}(g_{i,j}))(\boldsymbol{0}) \neq 0$.

To finish the proof, we have to verify that $\Phi \circ \Lambda_{D_2,p_2,c_2} \circ \Gamma_{D_3,p_3,c_3}$ satisfies conditions (1) and (2). For $i \in [m]$, $(\Phi \circ \Lambda_{D_2,p_2,c_2} \circ \Gamma_{D_3,p_3,c_3})(f_i)$ is non-constant, because

$$\deg_{z_0}\big((\Phi \circ \Lambda_{D_2,p_2,c_2} \circ \Gamma_{D_3,p_3,c_3})(f_i)\big) = \deg_{z_0}\big((\Gamma_{D_3,p_3,c_3})(f_i)\big) = \deg(f_i) > 0.$$

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

$$\begin{aligned}&\mathrm{res}_{z_0}\big((\Phi \circ \Lambda_{D_2,p_2,c_2} \circ \Gamma_{D_3,p_3,c_3})(f_i), (\Phi \circ \Lambda_{D_2,p_2,c_2} \circ \Gamma_{D_3,p_3,c_3})(f_j)\big)\\ &\quad = (\Phi \circ \Lambda_{D_2,p_2,c_2})\big(\mathrm{res}_{z_0}(g_i, g_j)\big) = (\Phi \circ \Lambda_{D_2,p_2,c_2})(g_{i,j}) \neq 0,\end{aligned}$$

where the first equality follows from the fact that $\Phi \circ \Lambda_{D_2,p_2,c_2}$ does not change the leading term of g_i and g_j as polynomials in z_0, and the inequality holds because $(\Phi \circ \Lambda_{D_2,p_2,c_2})(g_{i,j})(\boldsymbol{0}) = (\Lambda_{D_2,p_2,c_2}(g_{i,j}))(\boldsymbol{0}) \neq 0$. Therefore, by [43, Chap. 3, §6, Proposition 1], $(\Phi \circ \Lambda_{D_2,p_2,c_2} \circ \Gamma_{D_3,p_3,c_3})(f_i)$ and $(\Phi \circ \Lambda_{D_2,p_2,c_2} \circ \Gamma_{D_3,p_3,c_3})(f_j)$ are coprime. □

5.3. A hitting set (arbitrary characteristic)

Armed with Lemmas 29 and 30 we can now complete the construction of the hitting set for $\Sigma\Pi\Sigma\Pi_\delta(k, s, n)$ circuits using the faithful homomorphism $\Psi \circ \Xi \circ \Lambda \circ \Gamma$ with the right parameters. Let $n, \delta, k, s \geqslant 1$ and let $r = R_\delta(k, s)$. We introduce the following parameters.

(1) Define $D_2 := 2\delta^{r+1} + 1$ and $D_3 := \delta + 1$.
(2) Define $p_{\max,2} := (2^k n(ks)^2 r(n + 2\delta^{r+1})^{2\delta^{r+1}}\lceil\log_2 D_2\rceil + 1)^2$ and $p_{\max,3} := (2^k nks(n+\delta)^\delta\lceil\log_2 D_3\rceil + 1)^2$.
(3) Pick arbitrary $H_1, \ldots, H_4 \subset \overline{K}$ of sizes $2^k\delta^{r+1}n^{r^2+r}$, $2^{k+1}r(ks)^2\delta^{r+3}p_{\max,2}$, $2^k ks\delta^2 p_{\max,3}$ and $\delta s + 1$, respectively.

Set $\boldsymbol{p} := (p_2, p_3)$ and $\boldsymbol{c} := (c_1, c_2, c_3)$. Denote $\Phi_{\boldsymbol{p},\boldsymbol{c}} := \Psi \circ \Xi_{c_1} \circ \Lambda_{D_2,p_2,c_2} \circ \Gamma_{D_3,p_3,c_3}$ and $\Phi^{(i)}_{\boldsymbol{p},\boldsymbol{c}} := \Phi_{\boldsymbol{p},\boldsymbol{c}}(x_i) \in \overline{K}[z_0, \boldsymbol{z}]$ for $i \in [n]$ and define the subset

$$\mathcal{H}_{\delta,k,s} = \Big\{\big(\Phi^{(1)}_{\boldsymbol{p},\boldsymbol{c}}(\boldsymbol{a}), \ldots, \Phi^{(n)}_{\boldsymbol{p},\boldsymbol{c}}(\boldsymbol{a})\big) \;\Big|\; \boldsymbol{p} \in [p_{\max,2}] \times [p_{\max,3}],\ \boldsymbol{c} \in H_1 \times H_2 \times H_3,\ \boldsymbol{a} \in H_4^{r+1}\Big\} \subset \overline{K}^n.$$

The following theorem shows that this is a hitting set for $\Sigma\Pi\Sigma\Pi_\delta(k, s, n)$ circuits. If Conjecture 28 holds true, the construction is not only non-trivial (i.e. better than the brute force PIT) in characteristic zero but even for $\mathrm{char}(K) = \Omega(1)$ (recall: δ, k are bounded constants in this section).

Theorem 31. *The set $\mathcal{H}_{\delta,k,s}$ is a hitting set for $\Sigma\Pi\Sigma\Pi_\delta(k, s, n)$. It can be constructed in $\mathrm{poly}(\delta rsn)^{kr^2\delta^{r+1}}$ time.*

Proof. Let $C \in \Sigma\Pi\Sigma\Pi_\delta(k, s, n)$ be a non-zero circuit. Note that the sparsity of elements in $\mathcal{S}(C)$ is bounded by $\binom{n+\delta}{\delta}$. The parameters above are blown up very generously so that they support 2^k applications of Lemma 22 (one for each $\mathcal{S}(C_I)$ for all $I \subseteq [k]$) and Lemma 30 (one for each C_I for all $I \subseteq [k]$). For example, by Lemma 25, the set $[p_{\max,2}]$ contains at least

$$2^k n(ks)^2 r\big(n + 2\delta^{r+1}\big)^{2\delta^{r+1}}\lceil\log_2 D_2\rceil + 1 \geqslant 2^k rn\binom{n+\delta^{r+1}}{\delta^{r+1}}\log_2 D_2 + 2^k\binom{ks\delta}{2}n\binom{n+2\delta^2}{2\delta^2}\log_2 D_2 + 1$$

primes. Thus, Lemma 30 resp. Lemma 22 imply that there exist $\boldsymbol{p} \in [p_{\max,2}] \times [p_{\max,3}]$ and $\boldsymbol{c} \in H_1 \times H_2 \times H_3$ such that, for all $I \subseteq [k]$, we have

(1) $\Phi_{\boldsymbol{p},\boldsymbol{c}}(\mathrm{sim}(C_I)) = \mathrm{sim}(\Phi_{\boldsymbol{p},\boldsymbol{c}}(C_I))$, and
(2) $\Phi_{\boldsymbol{p},\boldsymbol{c}}$ 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 29, $\Phi_{\boldsymbol{p},\boldsymbol{c}}(C)$ is a non-zero circuit with at most $r+1$ variables and of degree at most δs. Now the first assertion follows from Lemma 24. The second assertion is obvious from the construction. □

5.4. A hitting set (zero or large characteristic)

If $\operatorname{char}(K)$ is zero or large enough, we can give a more efficient hitting set construction. Let $n, \delta, k, s \geqslant 1$ and let $r = R_\delta(k,s)$. We introduce the following parameters.

(1) Define $D_2 := 2\delta^2 r + 1$ and $D_3 := \delta + 1$.
(2) Define $p_{\max,2} := (2^k n(ks)^2 r^r (n+2\delta^2)^{2\delta^2 r} \lceil \log_2 D_2 \rceil + 1)^2$ and $p_{\max,3} := (2^k nks(n+\delta)^\delta \lceil \log_2 D_3 \rceil + 1)^2$.
(3) Pick arbitrary $H_1, \ldots, H_4 \subset \overline{K}$ of sizes $2^k n^r$, $2^{k+1} r(ks\delta^2)^2 p_{\max,2}$, $2^k ks\delta^2 p_{\max,3}$ and $\delta s + 1$, respectively.

Set $\boldsymbol{p} := (p_2, p_3)$ and $\boldsymbol{c} := (c_1, c_2, c_3)$. Denote $\Phi_{\boldsymbol{p},\boldsymbol{c}} := \Psi \circ \Xi_{c_1} \circ \Lambda_{D_2,p_2,c_2} \circ \Gamma_{D_3,p_3,c_3}$ and $\Phi^{(i)}_{\boldsymbol{p},\boldsymbol{c}} := \Phi_{\boldsymbol{p},\boldsymbol{c}}(x_i) \in \overline{K}[z_0, \boldsymbol{z}]$ for $i \in [n]$ and define the subset

$$\mathcal{H}_{\delta,k,s} = \left\{ \left(\Phi^{(1)}_{\boldsymbol{p},\boldsymbol{c}}(\boldsymbol{a}), \ldots, \Phi^{(n)}_{\boldsymbol{p},\boldsymbol{c}}(\boldsymbol{a}) \right) \;\middle|\; \boldsymbol{p} \in [p_{\max,2}] \times [p_{\max,3}],\ \boldsymbol{c} \in H_1 \times H_2 \times H_3,\ \boldsymbol{a} \in H_4^{r+1} \right\} \subset \overline{K}^n.$$

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. This proves Theorem 2.

Theorem 32. *Assume that* $\operatorname{char}(K) = 0$ *or* $\operatorname{char}(K) > \delta^r$. *Then* $\mathcal{H}_{\delta,k,s}$ *is a hitting set for* $\Sigma\Pi\Sigma\Pi_\delta(k,s,n)$. *It can be constructed in* $\operatorname{poly}(\delta rsn)^{\delta^2 kr}$ *time.*

Proof. Let $C \in \Sigma\Pi\Sigma\Pi_\delta(k,s,n)$ be a non-zero circuit. Note that the sparsity of elements in $\mathcal{S}(C)$ is bounded by $\binom{n+\delta}{\delta}$. The parameters above are blown up very generously so that they support 2^k applications of Lemma 23 (one for each $\mathcal{S}(C_I)$ for all $I \subseteq [k]$) and Lemma 30 (one for each C_I for all $I \subseteq [k]$). For example, by Lemma 25, the set $[p_{\max,2}]$ contains at least

$$2^k n(ks)^2 r^r \left(n+2\delta^2\right)^{2\delta^2 r} \lceil \log_2 D_2 \rceil + 1 \geqslant 2^k nr! \binom{n+\delta}{\delta}^r \log_2 D_2 + 2^k \binom{ks\delta}{2} n \binom{n+2\delta^2}{2\delta^2} \log_2 D_2 + 1$$

primes. Thus, Lemma 30 resp. Lemma 23 imply that there exist $\boldsymbol{p} \in [p_{\max,2}] \times [p_{\max,3}]$ and $\boldsymbol{c} \in H_1 \times H_2 \times H_3$ such that, for all $I \subseteq [k]$, we have

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

Hence, by Lemma 29, $\Phi_{\boldsymbol{p},\boldsymbol{c}}(C)$ is a non-zero circuit with at most $r+1$ variables and of degree at most δs. Now the first assertion follows from Lemma 24. The second assertion is obvious from the construction. □

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. This proves Corollary 3.

Corollary 33. *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* $\operatorname{poly}(\delta sn)^{\delta^2}$ *time.*

Proof. We have $R_\delta(2,s) = 1$. From the proof of Lemma 30 we see that there exist $\boldsymbol{p} \in [p_{\max,2}] \times [p_{\max,3}]$ and $\boldsymbol{c} \in H_1 \times H_2 \times H_3$ such that, for all $I \subseteq [k]$, we have

(1) $\Phi_{\boldsymbol{p},\boldsymbol{c}}(\operatorname{sim}(C_I)) = \operatorname{sim}(\Phi_{\boldsymbol{p},\boldsymbol{c}}(C_I))$, and
(2) $\Phi_{\boldsymbol{p},\boldsymbol{c}}$ sends non-constant polynomials in $\mathcal{S}(C_I)$ to non-constant polynomials, hence $\Phi_{\boldsymbol{p},\boldsymbol{c}}$ is faithful to sets of transcendence degree 1.

Hence we are done as in the proof of Theorem 32, but without invoking Lemma 23 (where the dependence on the characteristic came from). □

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 the notion of transcendence degree and developed fundamental maps – the faithful homomorphisms – that

preserve the transcendence degree of sparse polynomials in a blackbox and efficient way (assuming a small transcendence degree). Crucially, we showed that faithful homomorphisms preserve the non-zeroness of circuits.

Our work raises several open questions. The faithful homomorphism construction over a small prime characteristic has restricted efficiency, in particular, it is interesting only when the sparse polynomials have very low degree. Could Lemma 22 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, e.g. Corollary 6 and Lemmas 16 and 22.

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 $O(k^2 \log s)$ (and $O(k^2)$ over $\mathbb{R}$) [20]. Even for $\delta = 2$ we leave the rank question open. We conjecture $R_2(k,s) = O(k \log s)$ (generally, Conjecture 28). Our hope is that understanding these small δ identities should give us more potent tools to attack depth-4 PIT in generality.

Acknowledgments

We are grateful to the Hausdorff Center for Mathematics, Bonn, for its kind support. The first two authors would like to thank the Bonn International Graduate School in Mathematics for research funding. The second author thanks Peter Scheiblechner for interesting discussions. Finally, we thank the anonymous reviewers for their suggestions to improve the writeup.

Appendix A. Proof of the degree bound for annihilating polynomials

For the proof of Corollary 6 we will need two lemmas. The first one is well known and identifies a situation where annihilating polynomials are unique up to a factor in K^*. Due to the lack of a suitable reference, we give the proof here.

Lemma A.1. *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 [44, 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 $i \in [2]$. 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 $g := \operatorname{res}_{y_m}(F_1, F_2) \in R$. By [43, Chap. 3, §5, Proposition 9], there exist $g_1, g_2 \in R[y_m]$ such that $g = g_1 F_1 + g_2 F_2$. We have

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

Since $f_1, \ldots, f_{m-1}$ are algebraically independent, it follows that $g = 0$. By [43, Chap. 3, §6, Proposition 1], 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. [29, Claim 7.2] for a similar statement).

Lemma A.2. *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 $\deg(G) \leqslant \deg(F)$. In particular, $f_1, \ldots, f_m$ are algebraically independent over K if and only if they are algebraically independent over L.*

Proof. Let $F = \sum_{\alpha \in S} c_\alpha \boldsymbol{y}^\alpha \in L[\boldsymbol{y}]$ be a non-zero polynomial such that $F(f_1, \ldots, f_m) = 0$, where $S \subset \mathbb{N}^m$ is non-empty finite set and $c_\alpha \in L^*$ for all $\alpha \in S$. Set $\boldsymbol{c} = (c_\alpha)_{\alpha \in S}$ and introduce a new set $\boldsymbol{t} = \{t_\alpha \mid \alpha \in S\}$ of variables. Let $G' := \sum_{\alpha \in S} t_\alpha \boldsymbol{y}^\alpha \in K[\boldsymbol{t}, \boldsymbol{y}]$ be the polynomial obtained by replacing the coefficients of F by the corresponding variables. We can write $G'(\boldsymbol{t}, f_1, \ldots, f_m) = \sum_{\alpha \in S'} \ell_\beta \boldsymbol{x}^\beta$, where $S' \subset \mathbb{N}^n$ is a non-empty finite set and $\ell_\beta \in K[\boldsymbol{t}]$ is a linear form for all $\beta \in S'$. Since L/K is algebraic, the monomials $\boldsymbol{x}^\beta$ are L-linearly independent. Therefore

$$\sum_{\beta \in S'} \ell_\beta(\boldsymbol{c}) \boldsymbol{x}^\beta = G'(\boldsymbol{c}, f_1, \ldots, f_m) = F(f_1, \ldots, f_m) = 0$$

implies that the homogeneous linear system

$$\ell_\beta(\boldsymbol{t}) = 0, \quad \beta \in S',$$

with coefficients in K has a non-trivial solution over L (namely $\boldsymbol{c}$). Thus it has also a non-trivial solution $\boldsymbol{c}'$ over K. We obtain a non-zero polynomial $G := G'(\boldsymbol{c}', \boldsymbol{y}) \in K[\boldsymbol{y}]$ with the desired properties. □

Proof of Corollary 6. By Lemma A.2, 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 16, 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 $i \in [r+1]$. Then $g_1, \ldots, g_{r+1}$ are of degree at most δ and by Theorem 5 there exists a non-zero polynomial $G \in K[\boldsymbol{y}]$ such that $G(g_1, \ldots, g_{r+1}) = 0$ and $\deg(G) \leqslant \delta^r$. But since

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

Lemma A.1 implies that F divides G. Hence, $\deg(F) \leqslant \deg(G) \leqslant \delta^r$. □

Appendix B. Proof of the Jacobian 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 $\operatorname{char}(K) = 0$. Then, for $i \in [n]$, we have

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

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

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

Hence, $\partial_{x_i} f = 0$ for all $i \in [n]$ if and only if $f \in K[x_1^p, \ldots, x_n^p]$. 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 $i \in [n]$ 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 we are prepared to proceed with the proofs.

Proof of Lemma 9. Let $r = \operatorname{rk}_L J_{\boldsymbol{x}}(f_1, \ldots, f_m)$. We may assume that the first r rows of $J(f_1, \ldots, f_m)$ are L-linearly independent. Assume, for the sake of contradiction, that $f_1, \ldots, f_r$ are algebraically dependent. Choose a non-zero polynomial $F \in K[\boldsymbol{y}] = K[y_1, \ldots, y_r]$ of minimal degree such that $F(f_1, \ldots, f_r) = 0$. Differentiating with respect to $x_1, \ldots, x_n$ using the chain rule yields the vector-matrix equation

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

Since this matrix has rank r over L, it follows that $(\partial_{y_i} F)(f_1, \ldots, f_r) = 0$ for all $i \in [r]$. Since the degree of F was chosen to be minimal, it follows that $\partial_{y_i} F = 0$ for all $i \in [r]$. If $\operatorname{char}(K) = 0$, this implies $F = 0$, a contradiction. If $\operatorname{char}(K) = p > 0$, this implies $F \in K[y_1^p, \ldots, y_r^p]$. 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

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

wee see that $G(f_1, \ldots, f_r) = 0$. By Lemma A.2, there exists a non-zero $G' \in K[\boldsymbol{y}]$ such that $G'(f_1, \ldots, f_r) = 0$ and $\deg(G') \leqslant \deg(G) < \deg(F)$. This contradicts the choice of F. Therefore, $f_1, \ldots, f_r$ are algebraically independent, hence $\operatorname{trdeg}(\{f_1, \ldots, f_m\}) \geqslant r$. □

Proof of Theorem 8. Let $r = \operatorname{trdeg}\{f_1, \ldots, f_m\}$. By Lemma 9, we have $r \geqslant \operatorname{rk}_L J(f_1, \ldots, f_m)$, so it remains to show the converse inequality.

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

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

By Theorem 5 (with $n - r + 1$ of the δ_i's being 1), we have $\deg(F_i) \leqslant \delta^r$. Hence, by the assumptions on $\operatorname{char}(K)$, we have $\partial_{y_0} F_i \neq 0$. Since the degree of F_i was chosen to be minimal, we have

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

Denote $G_{i,j} := (\partial_{y_j} F_i)(x_i, f_1, \ldots, f_r, x_{r+1}, \ldots, x_n)$ for $j \in [0, n]$. Differentiating equation (B.1) 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 $k \in [n]$. 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 $J(f_1, \ldots, f_m)$ are L-linearly independent and hence $r \leqslant \mathrm{rk}_L\, J(f_1, \ldots, f_m)$. □

References

[1] R.A. DeMillo, R.J. Lipton, A probabilistic remark on algebraic program testing, Inform. Process. Lett. 7 (4) (1978) 193–195.
[2] J.T. Schwartz, Fast probabilistic algorithms for verification of polynomial identities, J. ACM 27 (4) (1980) 701–717.
[3] R. Zippel, Probabilistic algorithms for sparse polynomials, in: Proceedings of the International Symposium on Symbolic and Algebraic Manipulation (EUROSAM), 1979, pp. 216–226.
[4] Z. Chen, M. Kao, Reducing randomness via irrational numbers, SIAM J. Comput. 29 (4) (2000) 1247–1256 (conference version in STOC 1997).
[5] D. Lewin, S. Vadhan, Checking polynomial identities over any field: Towards a derandomization? in: Proceedings of the 30th Annual Symposium on the Theory of Computing (STOC), 1998, pp. 428–437.
[6] M. Agrawal, S. Biswas, Primality and identity testing via Chinese remaindering, J. ACM 50 (4) (2003) 429–443 (conference version in FOCS 1999).
[7] L. Lovász, On determinants, matchings and random algorithms, in: Fundamentals of Computation Theory (FCT), 1979, pp. 565–574.
[8] L. Lovász, Singular spaces of matrices and their applications in combinatorics, Bull. Braz. Math. Soc. 20 (1989) 87–99.
[9] G. Ivanyos, M. Karpinski, N. Saxena, Deterministic polynomial time algorithms for matrix completion problems, SIAM J. Comput. 39 (8) (2010) 3736–3751.
[10] J. Heintz, C.P. Schnorr, 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, 1980, pp. 262–272.
[11] V. Kabanets, R. Impagliazzo, Derandomizing polynomial identity tests means proving circuit lower bounds, Comput. Complexity 13 (1) (2004) 1–46 (conference version in STOC 2003).
[12] M. Agrawal, Proving lower bounds via pseudo-random generators, in: Proceedings of the 25th Annual Foundations of Software Technology and Theoretical Computer Science (FSTTCS), 2005, pp. 92–105.
[13] M. Agrawal, Determinant versus Permanent, in: Proceedings of the 25th International Congress of Mathematicians (ICM), vol. 3, 2006, pp. 985–997.
[14] M. Agrawal, V. Vinay, Arithmetic circuits: A chasm at depth four, in: Proceedings of the 49th Annual Symposium on Foundations of Computer Science (FOCS), 2008, pp. 67–75.
[15] Z. Dvir, A. Shpilka, Locally decodable codes with 2 queries and polynomial identity testing for depth 3 circuits, SIAM J. Comput. 36 (5) (2006) 1404–1434 (conference version in STOC 2005).
[16] N. Kayal, N. Saxena, Polynomial identity testing for depth 3 circuits, Comput. Complexity 16 (2) (2007) 115–138 (conference version in CCC 2006).
[17] Z. Karnin, 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), 2008, pp. 280–291.
[18] N. Saxena, C. Seshadhri, An almost optimal rank bound for depth-3 identities, SIAM J. Comput. 40 (1) (2011) 200–224 (conference version in CCC 2009).
[19] N. Kayal, S. Saraf, Blackbox polynomial identity testing for depth 3 circuits, in: Proceedings of the 50th Annual Symposium on Foundations of Computer Science (FOCS), 2009, pp. 198–207.
[20] N. Saxena, 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), 2010, pp. 21–29.
[21] N. Saxena, 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, pp. 431–440.
[22] S. Saraf, I. Volkovich, Black-box identity testing of depth-4 multilinear circuits, in: Proceedings of the 43rd ACM Symposium on Theory of Computing (STOC), 2011, pp. 421–430.
[23] M. Anderson, D. van Melkebeek, I. Volkovich, Derandomizing polynomial identity testing for multilinear constant-read formulae, in: Proceedings of the 26th Annual IEEE Conference on Computational Complexity (CCC), 2011, pp. 273–282.
[24] N. Saxena, Progress on polynomial identity testing, Bull. EATCS – Comput. Complexity Column 99 (2009) 49–79.
[25] A. Shpilka, A. Yehudayoff, Arithmetic circuits: A survey of recent results and open questions, Found. Trends Theor. Comput. Sci. 5 (3–4) (2010) 207–388.
[26] K. Kalorkoti, A lower bound for the formula size of rational functions, SIAM J. Comput. 14 (3) (1985) 678–687 (conference version in ICALP 1982).
[27] Z. Dvir, A. Gabizon, A. Wigderson, Extractors and rank extractors for polynomial sources, Comput. Complexity 18 (1) (2009) 1–58 (conference version in FOCS 2007).
[28] Z. Dvir, D. Gutfreund, G. Rothblum, S. Vadhan, On approximating the entropy of polynomial mappings, in: Proceedings of the 2nd Symposium on Innovations in Computer Science (ICS), 2011.
[29] N. Kayal, The complexity of the annihilating polynomial, in: Proceedings of the 24th Annual IEEE Conference on Computational Complexity (CCC), 2009, pp. 184–193.

[30] O. Perron, Algebra I (Die Grundlagen), Walter de Gruyter, Berlin, 1927.
[31] C.G.J. Jacobi, De determinantibus functionalibus, J. Reine Angew. Math. 22 (4) (1841) 319–359.
[32] P. Morandi, Field and Galois Theory, Springer-Verlag, New York, 1996.
[33] J. Oxley, Matroid Theory, Oxford University Press, 2006.
[34] A. Płoski, Algebraic dependence of polynomials after O. Perron and some applications, in: S. Cojocaru, G. Pfister, V. Ufnarovski (Eds.), Computational Commutative and Non-Commutative Algebraic Geometry, IOS Press, 2005, pp. 167–173.
[35] R. Ehrenborg, G. Rota, Apolarity and canonical forms for homogeneous polynomials, European J. Combin. 14 (1993) 157–181.
[36] G. Kemper, A Course in Commutative Algebra, Springer-Verlag, Berlin, 2011.
[37] D. Eisenbud, Commutative Algebra with a View Toward Algebraic Geometry, Springer-Verlag, New York, 1995.
[38] L.M. Adleman, H.W. Lenstra, Finding irreducible polynomials over finite fields, in: Proceedings of the 18th Annual ACM Symposium on Theory of Computing (STOC), 1986, pp. 350–355.
[39] M. Bläser, M. Hardt, R.J. Lipton, N.K. Vishnoi, Deterministically testing sparse polynomial identities of unbounded degree, Inform. Process. Lett. 109 (3) (2009) 187–192.
[40] J. Zeng, A bijective proof of Muir's identity and the Cauchy–Binet formula, Linear Algebra Appl. 184 (1993) 79–82.
[41] N. Alon, Combinatorial Nullstellensatz, Combin. Probab. Comput. 8 (1999) 7–29.
[42] J. Rosser, L. Schoenfeld, Approximate formulas for some functions of prime numbers, Illinois J. Math. 6 (1) (1962) 64–94.
[43] D. Cox, J. Little, D. O'Shea, Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra, second edn., Springer-Verlag, New York, 1997.
[44] A. van den Essen, Polynomial Automorphisms and the Jacobian Conjecture, Birkhäuser Verlag, Basel, 2000.