Algebraic Independence and Blackbox Identity Testing

M. Beecken, J. Mittmann, N. Saxena

Presented by Zuzana Safernová

Basic definitions

Polynomial identity testing (PIT) is the problem of checking whether a given n-variate arithmetic circuit computes the zero polynomial in $K[x_1, \ldots, x_n]$.

By a *blackbox PIT test* for a family of circuits $\mathcal{F}$ we mean efficiently designing a *hitting set* $\mathcal{H} \subseteq \overline{K}^n$ such that: Given a nonzero $C \in \mathcal{F}$, there exists an $\overline{a} \in \mathcal{H}$ that *hits* C, i. e. $C(\overline{a}) = 0$.

Polynomials $\{f_1, \ldots, f_m\} \subset K[x_1, \ldots, x_n]$ (over a field K) are *algebraically independent* if there is no non-zero polynomial F such that $F(f_1, \ldots, f_m) = 0$. The *transcendence degree*, $trdeg\{f_1, \ldots, f_m\}$, is the maximal number r of algebraically independent polynomials.

Results

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 $poly(size(C')d\ell\delta)^r$ time test to check $C' = 0$ (assuming that K has characteristic zero or larger than δ^r).*

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

Perron, Jacobi & Krull

$K[\overline{x}] = K[x_1, \ldots, x_n]$, K – a field, $\overline{K}$ – the algebraic closure of K, R^* = multiplicative group of units of a ring R

Theorem 3 (Perron) *Let $f_1, \ldots, f_{n+1} \in K[\overline{x}]$ be non-constant polynomials of degree δ_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 $\deg F \leq \prod_i \delta_i / \min_i\{\delta_i\}$.*

Corollary 4 *Let $f_1, \ldots, f_m \in K[\overline{x}]$ be algebraically dependent polynomials of maximal degree $\delta \geq 1$ and* trdeg *r. Then there exists a non-zero polynomial $F \in K[y_1, \ldots, y_m]$ of degree at most δ^r such that $F(f_1, \ldots, f_m) = 0$.*

Theorem 5 (Jacobi) *Let $f_1, \ldots, f_m \in K[\overline{x}]$ be polynomials of degree at most δ and* trdeg *r. Assume that $\mathrm{ch}(K) = 0$ or $\mathrm{ch}(K) > \delta^r$. Then $\mathrm{rk}_L J_x(f_1, \ldots, f_m) = \mathrm{trdeg}_K\{f_1, \ldots, f_m\}$, where $L = K(\overline{x})$.*

Lemma 6 *Let $f_1, \ldots, f_m \in K[\overline{x}]$. Then $\mathrm{trdeg}_K\{f_1, \ldots, f_m\} \geq \mathrm{rk}_L J_x(f_1, \ldots, f_m)$, where $L = K(\overline{x})$.*

Definition 7 *A* K-algebra A *is a commutative ring (with 1) containing K as a subring. A map $A \to B$ is* K-algebra homomorfism *if it is a ring homomorphism that fixes K elementwise. Let $a_1, \ldots, a_m \in A$, consider $\varphi : K[\overline{y}] \to A$, $\varphi(F) = F(a_1, \ldots, a_m)$, where $K[\overline{y}] =$*

$K[y_1, \ldots, y_m]$. *If* $\ker \varphi = \{0\}$*, then* $\{a_1, \ldots, a_m\}$ *are* algebraically independent *over* K*. For* $S \subseteq A$ *define*

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

The image of $K[\overline{y}]$ *under* φ *is the subalgebra of* A *generated by* $a_1, \ldots, a_m$ *and is denoted by* $K[a_1, \ldots, a_m]$*. An algebra of this form is called an* affine K-algebra*, and it is called an* affine K-domain *if it is an integral domain. The* Krull dimension *of* A*, denoted by* $dim(A)$*, is defined as the supremum over all* $r \geq 0$ *for which there is a chain* $P_0 \subsetneq P_1 \subsetneq \cdots \subsetneq P_r$ *of prime ideals* $P_i \subsetneq A$*.*

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

Corollary 9 *Let* A, B *be* K*-algebras and let* $\varphi : A \to B$ *be a* K*-algebra homomorphism. If* A *is an affine algebra, then so is* $\varphi(A)$ *and we have* $dim(\varphi(A)) \leq dim(A)$*. If, in addition,* φ *is injective, then* $dim(\varphi(A)) = dim(A)$*.*

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

Faithful homomorphisms: reducing the variables

$K[\overline{z}] = K[z_1, \ldots, z_r]$, where $r = \mathrm{trdeg}\{f_1, \ldots, f_m\}$.

Definition 11 *Let* $\varphi : K[\overline{x}] \to K[\overline{z}]$ *be a* K*-algebra homomorphism. We say* φ *is* faithful *to* $\{f_1, \ldots, f_m\}$ *if* $\mathrm{trdeg}\{\varphi(f_1), \ldots, \varphi(f_m)\} = \mathrm{trdeg}\{f_1, \ldots, f_m\}$*.*

Theorem 12 *Let* $A = K[f_1, \ldots, f_m] \subseteq K[\overline{x}]$*. Then* φ *is faithful to* $\{f_1, \ldots, f_m\}$ *if and only if* $\varphi|_A : A \to K[\overline{z}]$ *is injective (iff* $A \cong K[\varphi(f_1), \ldots, \varphi(f_m)]$*).*

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

Lemma 14 (Existence). *Let* K *be an infinite field and let* $f_1, \ldots, f_m \in K[\overline{x}]$ *be polynomials of* trdeg r*. Then there exists a linear* K*-algebra homomorphism* $\varphi : K[\overline{x}] \to K[\overline{z}]$ *which is faithful to* $\{f_1, \ldots, f_m\}$*.*

Sketch of the proof of Theorem 1

We consider arithmetic circuits of the form $C(f_1, \ldots, f_m)$, where C is a circuit computing a polynomial in $K[\overline{y}] = K[y_1, \ldots, y_m]$ and $f_1, \ldots, f_m$ are subcircuits computing polynomials in $K[\overline{x}]$. 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, we construct a hitting set for r-variate degree-d polynomials, provided by the non-vanishing version of the Combinatorial Nullstellensatz.

Theorem 15 (Combinatorial Nullstellensatz) *Let* $H \subseteq K$ *be a subset of size* $d+1$*. Then* $\mathcal{H} = H^r$ *is a hitting set for* $\{f \in K[z_1, \ldots, z_r] | deg(f) \leq d\}$*.*