

Polynomial Identity Testing via Evaluation of Rational Functions

Dieter van Melkebeek ✉

University of Wisconsin-Madison, Madison, WI, USA

Andrew Morgan ✉

University of Wisconsin-Madison, Madison, WI, USA

Abstract

We introduce a hitting set generator for Polynomial Identity Testing based on evaluations of low-degree univariate rational functions at abscissas associated with the variables. In spite of the univariate nature, we establish an equivalence up to rescaling with a generator introduced by Shpilka and Volkovich, which has a similar structure but uses multivariate polynomials in the abscissas.

We study the power of the generator by characterizing its vanishing ideal, i.e., the set of polynomials that it fails to hit. Capitalizing on the univariate nature, we develop a small collection of polynomials that jointly produce the vanishing ideal. As corollaries, we obtain tight bounds on the minimum degree, sparseness, and partition size of set-multi-linearity in the vanishing ideal. Inspired by an alternating algebra representation, we develop a structured deterministic membership test for the vanishing ideal. As a proof of concept we rederive known derandomization results based on the generator by Shpilka and Volkovich, and present a new application for read-once oblivious arithmetic branching programs that provably transcends the usual combinatorial techniques.

2012 ACM Subject Classification Theory of computation → Algebraic complexity theory; Theory of computation → Pseudorandomness and derandomization

Keywords and phrases Derandomization, Gröbner Basis, Lower Bounds, Polynomial Identity Testing

Digital Object Identifier 10.4230/LIPIcs.ITCS.2022.119

Funding Research partially supported by the US National Science Foundation through grant CCF-1838434.

Acknowledgements We are indebted to Gautam Prakriya for helpful discussions and detailed feedback. We also thank Amir Shpilka for helpful comments and suggestions, as well as Ilya Volkovich and the anonymous reviewers. We are grateful to Hervé Fournier and Arpita Korwar for their presentation at WACT'18 in Paris [13].

1 Overview

Polynomial identity testing (PIT) is the fundamental problem of deciding whether a given multi-variate arithmetic circuit formally computes the zero polynomial. PIT has a simple efficient randomized algorithm that only needs black-box access to the circuit: Pick a random point and check whether the circuit evaluates to zero on that particular point.

In spite of the fundamental nature of PIT and the simplicity of the randomized algorithm, no efficient deterministic algorithm is known – even in the white-box setting, where the algorithm has access to the description of the circuit. The existence of such an algorithm would imply long-sought circuit lower bounds [17, 1, 21]. Conversely, sufficiently strong circuit lower bounds yield blackbox derandomization for all of BPP, the class of decision problems admitting efficient randomized algorithms with bounded error [28, 18]. Although the known results leave gaps between the two directions, they suggest that PIT acts as a BPP-complete problem in the context of derandomization, and that derandomization of BPP can be achieved in a blackbox fashion if at all.



© Dieter van Melkebeek and Andrew Morgan;
licensed under Creative Commons License CC-BY 4.0
13th Innovations in Theoretical Computer Science Conference (ITCS 2022).
Editor: Mark Braverman; Article No. 119; pp. 119:1–119:24



Leibniz International Proceedings in Informatics
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

119:2 Polynomial Identity Testing via Evaluation of Rational Functions

Blackbox derandomization of PIT for a class of polynomials \mathcal{C} is equivalent to the efficient construction of a family $G = \{G_n\}_{n \in \mathbb{N}}$ of low-degree polynomial mappings where G_n maps a small set of l fresh variables to the set of n variables $\{x_1, \dots, x_n\}$ such that for each nonzero polynomial p from \mathcal{C} in the variables $\{x_1, \dots, x_n\}$, $p \circ G_n$ remains nonzero [34, Lemma 4.1]. We say that the generator G hits the class \mathcal{C} . If p and G_n have degree at most $n^{O(1)}$, the resulting deterministic PIT algorithm for \mathcal{C} makes $n^{O(l)}$ black-box queries.

Much progress on derandomizing PIT has been obtained by designing such polynomial mappings and analyzing their hitting properties for interesting classes \mathcal{C} . Shpilka and Volkovich [33] introduced a generator, by now dubbed the Shpilka–Volkovich generator or “SV-generator” for short, and proved that it hits sums of a bounded number of read-once formulas for $l = O(\log n)$, later improved to $l = O(1)$ [26]. The generator for $l = O(\log n)$ has also been shown to hit multi-linear depth-4 circuits with bounded top fan-in [22], multi-linear bounded-read formulas [5], commutative read-once oblivious arithmetic branching programs [10], $\Sigma\text{m} \wedge \Sigma\Pi^{O(1)}$ formulas [9], circuits with locally-low algebraic rank in the sense of [24], and orbits of simple polynomial classes under invertible linear transformations of the variables [25]. The generator is also an ingredient in other hitting set constructions, notably constructions using the technique of low-support rank concentration [3, 2, 16, 15, 31, 6]. It also forms the core of a “succinct” generator that hits a variety of classes including depth-2 circuits [12].

Vanishing ideal

In this paper we initiate a systematic study of the power of the SV-generator. For any generator G , G hits a polynomial p if and only if the composition of polynomials $p(G)$ is nonzero. The power of G , therefore, is determined by the set of p such that $p(G)$ vanishes. This set, denoted $\text{Van}[G]$, has the algebraic structure of an ideal, and is known as the *vanishing ideal* of G . Our results can be understood as precisely characterizing the vanishing ideal of the SV-generator for all choices of parameters.

There are two natural ways in which to apply a characterization of the vanishing ideal:

Derandomization To show that a generator G hits a class \mathcal{C} of polynomials, it suffices (and is necessary) to prove that the intersection of \mathcal{C} with $\text{Van}[G]$ consists of at most the zero polynomial. The vanishing ideal of SV tells us what polynomials we need to focus on when designing other generators for derandomizing PIT in combination with SV.

Lower bounds If we know that the generator G hits a class \mathcal{C} of polynomials, any expression for a nonzero element of $\text{Van}[G]$ yields an explicit polynomial that falls outside \mathcal{C} . Such a statement is often referred to as hardness of representation, and can be viewed as a lower bound in the model of computation underlying \mathcal{C} (provided the polynomial can be computed in the model at all).

We will illustrate both uses of our characterizations of the SV-generator.

Rational function evaluations

Another contribution of our paper is the development of an alternate view of the SV-generator, namely as evaluations of univariate rational functions of low degree. We would like to promote the perspective for its intrinsic appeal and its applicability. Among other things, it facilitates the study of the vanishing ideal.

The transition goes as follows. The SV-generator takes as additional parameters a positive integer l , and a choice of distinct field elements a_i for each of the original variables x_i , $i \in [n]$. We refer to the elements a_i as *abscissas*, and denote the mapping for a given value of l by

SV^l (suppressing the choice of abscissas). The mapping SV^1 uses two fresh variables, y and z , and can be described succinctly in terms of the Lagrange interpolants L_i for the set of abscissas:

$$x_i \leftarrow z \cdot L_i(y) \doteq z \cdot \prod_{i' \in [n] \setminus \{i\}} \frac{y - a_{i'}}{a_i - a_{i'}}. \quad (1)$$

By rescaling, the denominators on the right-hand side of (1) can be cleared, resulting in the following somewhat simpler polynomial mapping:

$$x_i \leftarrow z \cdot \prod_{i' \in [n] \setminus \{i\}} (y - a_{i'}). \quad (2)$$

The vanishing ideals of (2) and SV^1 are the same up to rescaling the variables to match the rescaling from (1) to (2).

More importantly, we apply the change of variables $z \leftarrow z' / \prod_{i \in [n]} (y - a_i)$, resulting in the rational map

$$x_i \leftarrow \frac{z'}{y - a_i}. \quad (3)$$

The notion of vanishing ideal naturally extends to rational maps. The change of variables from (2) to (3) establishes that any polynomial vanishing on (2) also vanishes on (3). The change of variables is invertible (the inverse is $z' \leftarrow z \prod_{i \in [n]} (y - a_i)$), so any polynomial vanishing on (3) also vanishes on (2). Therefore the vanishing ideal of (3) is the same as that of SV^1 up to rescaling the variables.

Note that, for fixed y and z' , (3) may be interpreted as first forming a univariate rational function $f(\alpha) = \frac{z'}{y - \alpha}$ (depending on y and z' , but independent of i) and then substituting $x_i \leftarrow f(a_i)$. As y and z' vary, f ranges over all rational functions with numerator degree zero and denominator degree one. We thus denote (3) by RFE_1^0 , where RFE is a short-hand for *Rational Function Evaluation*, 0 bounds the numerator degree, and 1 bounds the denominator degree.

The mapping RFE_1^0 naturally generalizes to RFE_l^k for arbitrary $k, l \in \mathbb{N}$:

► **Definition 1** (RFE Generator). *Let \mathbb{F} be a field and $X \doteq \{x_i : i \in [n]\}$ a set of variables. The Rational Function Evaluation (RFE) Generator for $\mathbb{F}[X]$ is parameterized by the following data:*

- For each $i \in [n]$, a distinct abscissa $a_i \in \mathbb{F}$.
- A non-negative integer k , the numerator degree.
- A non-negative integer l , the denominator degree.

The generator takes as seeds rational functions $f \in \mathbb{F}(\alpha)$ such that f can be written g/h for some $g, h \in \mathbb{F}[\alpha]$ with $\deg(g) \leq k$, $\deg(h) \leq l$, and $h(a_i) \neq 0$ for all $i \in [n]$. From a seed f , it generates the substitution $x_i \leftarrow f(a_i)$ for each $i \in [n]$.

There are multiple ways to parameterize the seed of RFE_l^k using scalars, such as by specifying coefficients, evaluations, or roots for each of the numerator and denominator. The flexibility to choose is a source of convenience. We refer to Appendix A for a discussion about different parameterizations, as well as how to obtain deterministic black-box PIT algorithms from the generator, and the required size of the underlying field \mathbb{F} . As is customary in the context of black-box derandomization of PIT, we will assume that \mathbb{F} is sufficiently large, possibly by taking a field extension.

119:4 Polynomial Identity Testing via Evaluation of Rational Functions

The connection between RFE_1^0 and SV^1 extends as follows. For higher values of l , SV^l is defined as the sum of l independent instantiations of SV^1 . The same transformations as above relate SV^l and the sum of l independent instantiations of RFE_1^0 . The latter in turn is equivalent to RFE_l^{l-1} by partial fraction decomposition. The conclusion is that SV^l is equivalent, up to variable rescaling, to RFE_l^{l-1} . We refer to Appendix B for a formal treatment.

For parameter values $k \neq l - 1$, there is no SV-generator that corresponds to RFE_l^k , but $\text{SV}^{\max(k+1,l)}$ encompasses RFE_l^k (up to rescaling) and uses at most twice as long of a seed. Thus, the RFE-generator and the SV-generator efficiently hit the same classes of polynomials. However, RFE's simpler univariate dependence on the abscissas – as opposed to SV's multi-variate dependence – enables our approach for determining the vanishing ideal. The moral is that, even though polynomial mappings are sufficient for derandomizing PIT, it nevertheless helps to consider rational mappings. Their use may simplify analysis, and arguably yield more elegant constructions.

Generating set

Our first result describes a small and explicit generating set for the vanishing ideal of RFE. It consists of instantiations of a single determinant expression.

► **Theorem 2.** *Let $k, l \in \mathbb{N}$, $\{x_i : i \in [n]\}$ be a set of variables, and a_i for $i \in [n]$ be distinct field elements. The vanishing ideal of RFE_l^k over the given set of variables for the given choice of abscissas $(a_i)_{i \in [n]}$ is generated by the following polynomials over all choices of $k + l + 2$ variable indices $i_1, i_2, \dots, i_{k+l+2} \in [n]$:*

$$\text{EVC}_l^k[i_1, i_2, \dots, i_{k+l+2}] \doteq \det \begin{bmatrix} a_{i_j}^l x_{i_j} & a_{i_j}^{l-1} x_{i_j} & \dots & x_{i_j} & a_{i_j}^k & a_{i_j}^{k-1} & \dots & 1 \end{bmatrix}_{j=1}^{k+l+2}. \quad (4)$$

Moreover, the polynomials $\text{EVC}_l^k[i_1, i_2, \dots, i_{k+l+2}]$ form a generating set of minimum size when $\{i_1, i_2, \dots, i_{k+l+2}\}$ ranges over all subsets of $[n]$ of size $k + l + 2$ that contain a fixed set $C \subseteq [n]$ of $k + 1$ variable indices, and $i_1 < i_2 < \dots < i_{k+l+2}$.

The name ‘‘EVC’’ is a shorthand for ‘‘Elementary Vandermonde Circulation’’. Later we discuss a representation of polynomials using alternating algebra, which connects with notions from network flow. In this representation, polynomials in the vanishing ideal coincide with circulations, and instantiations of EVC are the elementary circulations.

We refer to the set C in Theorem 2 as a *core*. The core C plays a similar role as in a sunflower except that, unlike the petals of a sunflower, the various sets S do not need to be disjoint outside the core.

As an example, for $k = 0$ and $l = 1$, one of the generators for RFE_1^0 is given by

$$\text{EVC}_1^0[1, 2, 3] \doteq \begin{vmatrix} a_1 x_1 & x_1 & 1 \\ a_2 x_2 & x_2 & 1 \\ a_3 x_3 & x_3 & 1 \end{vmatrix} = (a_1 - a_2)x_1 x_2 + (a_2 - a_3)x_2 x_3 + (a_3 - a_1)x_3 x_1.$$

For any fixed $i^* \in [n]$, the polynomials $\text{EVC}_1^0[i_1, i_2, i_3]$ form a generating set of minimum size when $\{i_1, i_2, i_3\}$ ranges over all subsets of $[n]$ containing i^* , and $i_1 < i_2 < i_3$. In general, the generators EVC_l^k are nonzero multi-linear homogeneous polynomials of degree $l + 1$ containing all multi-linear monomials of degree $l + 1$.

Each generating set of minimum size in Theorem 2 yields a Gröbner basis with respect to every monomial order that prioritizes the variables outside C . A Gröbner basis is a special basis that allows solving ideal-membership queries more efficiently as well as solving systems

of polynomial equations [7]. Computing Gröbner bases for general ideals is exponential-space complete. Theorem 2 represents a rare instance of a natural and interesting ideal for which we know an explicit Gröbner basis.

To gain some intuition about dependencies between the generators EVC_l^k , note that permuting the order of the variables used in the construction of EVC_l^k yields the same polynomial or minus that polynomial, depending on the sign of the permutation. This follows from the determinant structure of EVC_l^k , and is the reason why we need to fix the order of the variables in order to obtain a generating set of minimum size. More profoundly, the following relationship holds for every choice of $k + l + 3$ indices $i_1, i_2, \dots, i_{k+l+3} \in [n]$ and every univariate polynomial w of degree at most k :

$$\det \begin{bmatrix} w(a_{i_j}) & a_{i_j}^l x_{i_j} & a_{i_j}^{l-1} x_{i_j} & \dots & x_{i_j} & a_{i_j}^k & a_{i_j}^{k-1} & \dots & 1 \end{bmatrix}_{j=1}^{k+l+3} = 0. \quad (5)$$

The determinant in (5) vanishes because the first column of the matrix is a linear combination of the last $k+1$. A Laplace expansion across the first column allows us to write the determinant of the matrix as a linear combination of minors, and each minor is an instantiation of EVC_l^k . As the determinant vanishes, (5) represents a linear dependency for every nonzero polynomial w of degree at most k . In fact, when $\{i_1, \dots, i_{k+l+3}\}$ varies over subsets of $[n]$ containing a fixed core of size $k+1$, the equations (5) generate all linear dependencies among instances of EVC_l^k .

As corollaries to Theorem 2 we obtain the following tight bounds on $\text{Van}[\text{RFE}_l^k]$. The bounds hold for all choices of parameters, as long as the abscissas for different variables remain distinct.

- The minimum *degree* of a nonzero polynomial in $\text{Van}[\text{RFE}_l^k]$ equals $l+1$. This proves a conjecture by Fournier and Korwar [13] (additional partial results reported in [23]) that there exists a polynomial of degree $l+1$ in $n = 2l+1$ variables that SV^l fails to hit. The conjecture follows because the generators for $\text{Van}[\text{SV}^l]$ have degree $l+1$ and use $2l+1$ variables.

As none of the generators contain a monomial of support l or less, the same holds for every nonzero polynomial in $\text{Van}[\text{RFE}_l^k]$. This extends the well-known property that SV^l hits every polynomial that contains a monomial of support l or less.

- The minimum *sparseness*, i.e., number of monomials, of a nonzero polynomial in $\text{Van}[\text{RFE}_l^k]$ equals $\binom{k+l+2}{l+1}$. The generators EVC_l^k realize the bound as they exactly contain all multi-linear monomials of degree $l+1$ that can be formed out of their $k+l+2$ variables.

The claim that no nonzero polynomial in $\text{Van}[\text{RFE}_l^k]$ contains fewer than $\binom{k+l+2}{l+1}$ monomials requires an additional combinatorial argument. It is a (tight) quantitative strengthening of the well-known property that SV^l hits every polynomial with fewer than 2^l monomials [16, 9, 12]. Note that for $k = l-1$ we have that $\binom{k+l+2}{l+1} = \binom{2l+1}{l+1} = \Theta(2^{2l}/\sqrt{l})$.

- The minimum *partition class size* of a nonzero set-multi-linear polynomial of degree $l+1$ in $\text{Van}[\text{RFE}_l^k]$ equals $k+2$. Set-multi-linearity is a common restriction in works on derandomizing PIT and arithmetic circuit lower bounds. A polynomial p of degree $l+1$ in a set of variables $\{x_1, \dots, x_n\}$ is said to be set-multi-linear if $[n]$ can be partitioned as $[n] = X_1 \sqcup X_2 \sqcup \dots \sqcup X_{l+1}$ such that every monomial in p is a product $x_{i_1} \cdot x_{i_2} \cdot \dots \cdot x_{i_{l+1}}$, where $i_j \in X_j$. Note that set-multi-linearity implies multi-linearity but not the other way around.

As the generators EVC_l^k are not set-multi-linear, it is not immediately clear from Theorem 2 whether $\text{Van}[\text{RFE}_l^k]$ contains nontrivial set-multilinear polynomials. However, a variation on the construction of the generators EVC_l^k yields explicit set-multi-linear homogeneous polynomials in $\text{Van}[\text{RFE}_l^k]$ of degree $l+1$ where each X_j has size $k+2$. We denote

them by ESMVC_l^k , where ESMVC stands for ‘‘Elementary Set-Multi-linear Vandermonde Circulation’’. ESMVC_l^k contains all monomials of the form $x_{i_1} \cdot x_{i_2} \cdots x_{i_{l+1}}$ with $i_j \in X_j$. For any variable partition $X_1 \sqcup X_2 \sqcup \cdots \sqcup X_{l+1}$ with $|X_1| = \cdots = |X_{l+1}| = k+2$, ESMVC_l^k is the only set-multi-linear polynomial $\text{Van}[\text{RFE}_l^k]$ with that variable partition, up to a scalar multiple.

Membership test

Our second characterization of the vanishing ideal of RFE can be viewed as a structured membership test. There is a generic way to obtain a deterministic membership test for the vanishing ideal of any hitting set generator $G = \{G_n\}_{n \in \mathbb{N}}$, namely the well-known transformation of a hitting set generator into a deterministic blackbox PIT algorithm [29, 8, 35, 32]. A polynomial map G_n with l degrees of freedom that hits the n -variate polynomials p in a class \mathcal{C} , yields a deterministic black-box PIT algorithm for \mathcal{C} that makes no more than $n^{O(l)}$ queries as long as p and G_n have degree $n^{O(1)}$. By clearing denominators, the same follows for rational maps like RFE_l^k , which has $k+l+1$ degrees of freedom. The resulting deterministic algorithm decides PIT for $p \in \mathcal{C}$ provided RFE_l^k hits \mathcal{C} . Unconditionally, the algorithm decides membership of any p to the vanishing ideal $\text{Van}[\text{RFE}_l^k]$.

Capitalizing on the generating set of Theorem 2, we state a more structured deterministic membership test for $\text{Van}[\text{RFE}_l^k]$. In the important case of multi-linear polynomials, the test takes the following form.

► **Theorem 3.** *Let $k, l \in \mathbb{N}$, $\{x_i : i \in [n]\}$ be a set of variables, a_i for $i \in [n]$ be distinct field elements, and Z a set of at least $n - k - l - 1$ nonzero field elements. A multi-linear polynomial p in those variables belongs to $\text{Van}[\text{RFE}_l^k]$ if and only if both of the following conditions hold:*

1. p has no homogeneous components of degree l or less, nor of degree $n - k$ or more.
2. For all disjoint subsets $K, L \subseteq [n]$ with $|K| = k$ and $|L| = l$, and every $z \in Z$, $\left(\frac{\partial p}{\partial L}\right)\Big|_{K \leftarrow 0}$ evaluates to zero upon the following substitution for each $i \in \overline{K \cup L}$

$$x_i \leftarrow z \cdot \frac{\prod_{i' \in K} (a_i - a_{i'})}{\prod_{i' \in L} (a_i - a_{i'})}. \quad (6)$$

The first part of condition 1 in Theorem 3 extends the well-known property that SV^l hits every multi-linear polynomial that contains a monomial of degree l or less. Combined with the second part of the condition, it implies that all multi-linear polynomials on $n \leq k + l + 1$ variables are hit by RFE_l^k .

In condition 2, $\left(\frac{\partial p}{\partial L}\right)\Big|_{K \leftarrow 0}$ denotes the polynomial obtained by taking the partial derivative of p with respect to every variable in L , and setting all the variables in K to zero. (The order of the operations does not matter, and the resulting polynomial depends only on variables in $\overline{K \cup L}$.)

Several prior papers demonstrated the utility of partial derivatives and zero substitutions in the context of derandomizing PIT using the SV-generator, especially for syntactically multi-linear models [33, 22, 5]. By judiciously choosing variables for those operations, these papers managed to simplify p and reduce PIT for p to PIT for simpler instances, resulting in an efficient recursive algorithm. In Section 3, we develop a general framework for such algorithms, and prove correctness directly from Theorem 3. For every multi-linear polynomial p hit by RFE_l^k , the sets K and L in Theorem 3 describe how to choose k zero substitutions and l derivatives so that a recursive approach shows that p is hit by RFE_l^k . It follows that

any argument that SV or RFE hit a class of multi-linear polynomials can, in principle, be converted into one based on zero substitutions and partial derivatives. Thus, Theorem 3 shows that these tools harness the complete power of SV and RFE for multi-linear polynomials.

Applications

We illustrate the utility of our characterizations of the vanishing ideal of RFE in the two directions mentioned before.

Derandomization. For starters, we demonstrate how Theorem 3 yields an alternate proof of the result from [26] that every nonzero read-once formula F is hit by SV^1 , or equivalently, by RFE_1^0 . Whereas the original proof hinges on a clever ad-hoc argument, our proof (described in Section 3) is entirely systematic and amounts to a couple straightforward observations in order to apply Theorem 3.

As a proof of concept of the additional power of our characterization for derandomization, we develop an improvement in the model of read-once oblivious algebraic branching programs (ROABPs).

► **Theorem 4.** *For every $l \in \mathbb{N}$, SV^l hits the class of polynomials computed by read-once oblivious algebraic branching programs of width less than $1 + (l/3)$ that contain a monomial of degree at most $l + 1$.*

To the best of our knowledge, Theorem 4 is incomparable to the known results for ROABPs [30, 20, 19, 11, 10, 2, 4, 16, 15, 14, 31, 6]. Without the restriction that the polynomial has a monomial of degree at most $l + 1$, Theorem 4 would imply a fully blackbox polynomial-time identity test for the class of constant-width ROABPs. No such test has been proven to exist at this time; prior work requires either quasipolynomial time or requires opening the blackbox, such as by knowing the order in which the variables are read.

With the restriction, the well-known property that SV^{l+1} hits every polynomial containing a monomial of support $l+1$ or less implies that SV^{l+1} hits the class \mathcal{C} in Theorem 4. Our result can thus be viewed as an improvement from SV^{l+1} to SV^l . Even though the improvement is modest from this perspective, we point out that the method of proof of Theorem 4 diverges significantly from prior uses of the SV-generator, and therefore may be of independent interest. We elaborate on the method more when we discuss the techniques of this paper, but for now, we point out that most prior uses of the SV-generator rely on combinatorial arguments, i.e., arguments that depend only on which monomials are present in polynomials of \mathcal{C} . Theorem 4 necessarily goes beyond this, because there is a polynomial in $\text{Van}[SV^l]$ of degree $l + 1$ that has the same monomials as a polynomial computed by an ROABP of width 2. Namely, any instance of $ESMVC_l^{l-1}$ contains exactly all the monomials of the form $x_{i_1} \cdot x_{i_2} \cdots x_{i_{l+1}}$ with $(i_1, \dots, i_{l+1}) \in X_1 \times \cdots \times X_{l+1}$ for some disjoint sets X_j ; the same goes for $\prod_j \sum_{i_j \in X_j} x_{i_j}$, which is computed by an ROABP of width 2.

Lower bounds

The argument in the previous paragraph also illustrates this direction: our derandomization result for the class \mathcal{C} implies that every ROABP computing EVC_l^{l-1} , $ESMVC_l^{l-1}$, or any other polynomial of degree $l + 1$ in the vanishing ideal, has width at least $1 + (l/3)$. Other hardness of representation results for EVC_l^{l-1} and $ESMVC_l^{l-1}$ follow in a similar manner from prior hitting properties of SV in the literature:

119:8 Polynomial Identity Testing via Evaluation of Rational Functions

- Any syntactically multi-linear formula must read some variable at least $\Omega(\log(l)/\log\log(l))$ times [5].
- Any sum of read-once formulas must have at least $\Omega(l)$ terms [33, 26].
- There exists an order of the variables such that any ROABP with that order must have width at least $2^{\Omega(l)}$ [10].
- Any $\Sigma\text{m} \wedge \Sigma\Pi^{O(1)}$ formula must have top fan-in at least $2^{\Omega(l)}$ [9].
- Lower bounds over characteristic zero for circuits with locally-low algebraic rank [24].

Techniques

A recurring tool is the analysis of the coefficients of the Laurent expansion of $p(\text{RFE}_l^k)$ around certain abscissas. We capture the technique in our Zoom Lemma (Lemma 13). We also provide a proof from first principles that requires no knowledge of Laurent expansions. The Zoom Lemma is used in the proofs of all of Theorems 2, 3, and 4, as well as several of the other results. The basic logic is to zoom in on the projection of p onto certain monomials on a subset of the variables, and show that if the projection does not vanish at a certain point, then a particular Laurent coefficient of $p(\text{RFE}_l^k)$ is nonzero, and therefore RFE_l^k hits p .

Theorem 2 states the equality of two ideals: $\langle \text{EVC}_l^k \rangle = \text{Van}[\text{RFE}_l^k]$, where $\langle \text{EVC}_l^k \rangle$ denotes the ideal generated by all instantiations of EVC_l^k , and $\text{Van}[\text{RFE}_l^k]$ the vanishing ideal of RFE_l^k .

- The inclusion \subseteq follows from linearizing the defining equations of RFE_l^k . This is where the univariate dependency on the abscissas comes into play.
- To establish the inclusion \supseteq we first show that every equivalence class of polynomials modulo $\langle \text{EVC}_l^k \rangle$ contains a representative p whose monomials exhibit the combinatorial structure of a core. The structure enables the Zoom Lemma to exhibit a particular Laurent coefficient of $p(\text{RFE}_l^k)$ that receives a contribution from just a single monomial. As there are no other contributions that can cancel out that one contribution, the coefficient is nonzero, whence RFE_l^k hits p .

The proof of Theorem 3 also relies on Laurent expansions through the Zoom Lemma. Membership to the ideal is equivalent to the vanishing of all coefficients of the expansion. The proof can be viewed as determining a small number of coefficients sufficient to guarantee that their vanishing implies all coefficients vanish. The restriction to multi-linear polynomials p allows us to express the projections of p as the result of applying partial derivatives and zero-substitutions.

Theorem 4 makes use of the characterization of the minimum width of a read-once oblivious arithmetic branching program computing a polynomial p as the maximum rank of the monomial coefficient matrices of p for various variable partitions [27]. We reduce to the case where p is homogeneous of degree $l + 1$, whence the monomial coefficient matrices have a block-diagonal structure. An application of the Zoom Lemma in the contrapositive yields linear equations between elements of consecutive blocks under the assumption that SV^l fails to hit p . When some block is zero, the equations yield a Cauchy system of equations on the rows or columns of its neighboring blocks; since Cauchy systems have full rank, we deduce severe constraints on the row-space/column-space of the neighboring blocks. A careful analysis turns this observation into a rank lower bound of at least $1 + (l/3)$ for a well-chosen partition of the variables.

We point out that in this application the Zoom Lemma is instantiated several times in parallel to form a large system of equations on the coefficients of p , and the whole system is needed for the analysis. This stands in contrast to most prior work using SV, which uses knowledge of how p is computed to guide a search for a *single* fruitful instantiation of the Zoom Lemma.

Alternating algebra representation

The inspiration for several of our results stems from expressing the polynomials EVC_l^k using concepts from alternating algebra (also known as exterior algebra or Grassmann algebra). In fact, Theorem 3 hinges on the relationship $\partial^2 = 0$ from alternating algebra. Our original statement and proof of the theorem made use of that framework, but we managed to eliminate the alternating algebra afterwards. Still, as we find the perspective insightful and potentially helpful for future developments, we describe the connection here. We explain the intuition behind Theorem 3 for the simple case where the degree of the polynomial p equals $l + 1$. In that setting, belonging to the ideal generated by the polynomials EVC_l^k is equivalent to being in their linear span.

The alternating algebra A of a vector space V over a field \mathbb{F} consists of the closure of V under an additional binary operation, referred to as “wedge” and denoted \wedge , which is bilinear, associative, and satisfies

$$v \wedge v = 0 \tag{7}$$

for every $v \in V$. This determines a well-defined algebra. When the characteristic of \mathbb{F} is not 2, this can equivalently be understood as

$$v_1 \wedge v_2 = -(v_2 \wedge v_1) \tag{8}$$

for every $v_1, v_2 \in V$. In any case, for any $v_1, v_2, \dots, v_k \in V$,

$$v_1 \wedge v_2 \wedge \dots \wedge v_k \tag{9}$$

is nonzero iff the v_i 's are linearly independent, and any permutation of the order of the vectors in (9) yields the same element of A up to a sign. The sign equals the sign of the permutation, whence the name “alternating algebra.” If V has a basis X of size n , then a basis for A can be formed by all 2^n expressions of the form (9) where the v_i 's range over all subsets of X , and are taken in some fixed order. Considering the elements of X as vertices, the basis elements of A can be thought of as the oriented simplices of all dimensions that can be built from X .

Anti-commutativity, the relation Equation (8), arises naturally in the context of network flow, where X denotes the vertices of the underlying graph, and a wedge $v_1 \wedge v_2$ of level $k = 2$ represents one unit of flow from v_1 to v_2 . Equation (8) reflects the fact that one more unit of flow from v_1 to v_2 is equivalent to one less unit of flow from v_2 to v_1 . The adjacent levels $k = 1$ and $k = 3$ also have natural interpretations in the flow setting: v_1 (the element of A of the form (9) with $k = 1$) represents one unit of surplus flow at v_1 (the vertex of the graph), and $v_1 \wedge v_2 \wedge v_3$ abstracts an elementary circulation of one unit along the directed cycle $v_1 \rightarrow v_2 \rightarrow v_3 \rightarrow v_1$.

The different levels are related by so-called boundary maps. Boundary maps are linear transformations that map a simplex to a linear combination of its subsimplices of one dimension less. The maps are parameterized by a weight function $w : X \rightarrow \mathbb{F}$, and defined by

$$\partial_w : v_1 \wedge v_2 \wedge \dots \wedge v_m \mapsto \sum_{i=1}^m (-1)^{i+1} w(v_i) v_1 \wedge \dots \wedge v_{i-1} \wedge v_{i+1} \wedge \dots \wedge v_m, \tag{10}$$

an expression resembling the Laplace expansion of a determinant along a column $[w(v_i)]_{i=1}^m$. In the flow setting, using $w \equiv 1$, $\partial_1(v_1 \wedge v_2 \wedge v_3)$ is the superposition of the three edge flows

119:10 Polynomial Identity Testing via Evaluation of Rational Functions

that make up one unit of circulation along the directed cycle $v_1 \rightarrow v_2 \rightarrow v_3 \rightarrow v_1$, and $\partial_1(v_1 \wedge v_2)$ is the superposition of surplus at v_1 and demand at v_2 corresponding to one unit of flow from v_1 to v_2 . A linear combination p of terms (9) with $k = 2$ represents a valid circulation iff it satisfies conservation of flow at every vertex, which can be expressed as $\partial_1(p) = 0$, i.e., p is in the kernel of ∂_1 . An equivalent criterion is for p to be the superposition of circulations along 3-cycles, which can be expressed as p being in the image of ∂_1 . The relationship between the image and the kernel of boundary maps holds in general:

$$\text{Im}(\partial_{w_m} \circ \partial_{w_{m-1}} \circ \cdots \circ \partial_{w_0}) = \bigcap_{i=0}^m \ker(\partial_{w_i}). \quad (11)$$

In the context of the generators EVC_l^k , the set X creates a vertex for each variable, and simplices correspond to multilinear monomials. The anti-commutativity of \wedge coincides with the fact that swapping two arguments means swapping two rows in (4), which changes the sign of the determinant. Using the above boundary maps, the right-hand side of (4) can be viewed as $\partial_\omega(v_{i_1} \wedge v_{i_2} \wedge \cdots \wedge v_{i_{k+l+2}})$, where $\partial_\omega \doteq \partial_{w_k} \circ \partial_{w_{k-1}} \circ \cdots \circ \partial_{w_0}$ and $w_d(v_i) \doteq (a_i)^d$. By (11), this means that EVC_l^k is in the kernel of ∂_{w_d} for each $d \in \{0, 1, \dots, k\}$, or equivalently, in the kernel of $\partial_{\tilde{w}}$ for each $\tilde{w} : X \rightarrow \mathbb{F}$ of the form $\tilde{w}(v_i) = w(a_i)$ where w is a polynomial of degree at most k . This is precisely the condition (5). In fact, (11) implies that the linear span of the generators EVC_l^k consists exactly of the polynomials of degree $l+1$ in this kernel. The latter condition is precisely what the criterion in Theorem 3 expresses.

Organization

We develop the generating set for the vanishing ideal (Theorem 2) in section 2, and our ideal membership test (Theorem 3) in section 3. The proofs of our results on sparseness, set-multi-linearity, and derandomizing PIT for ROABPs (Theorem 4) as well as a further discussion of the alternating algebra representation are omitted due to space restrictions. The appendix contains some technical details about RFE and a formal treatment of the relationship between RFE and SV.

2 Generating Set

In this section we establish Theorem 2, our characterization of the vanishing ideal of RFE in terms of an explicit generating set. For every $k, l \in \mathbb{N}$, we develop a template, EVC_l^k , for constructing polynomials that belong to the vanishing ideal of RFE_l^k such that all instantiations collectively generate the vanishing ideal.

We start by deriving the template. The seeds f of RFE_l^k are of the form $f = g/h$, where $g, h \in \mathbb{F}[\alpha]$ with $\deg(g) \leq k$, $\deg(h) \leq l$, and $h(a_i) \neq 0$ for each $i \in [n]$. By definition, $\text{RFE}_l^k(f)$ substitutes each variable x_i by $f(a_i) = g(a_i)/h(a_i)$. In particular, the equation $x_i = g(a_i)/h(a_i)$ becomes satisfied for each $i \in [n]$, or, equivalently, $h(a_i)x_i - g(a_i) = 0$. Organizing the coefficients of the monomial expansions of $h(\alpha) = \sum_{d=0}^l h_d \alpha^d$ and $g(\alpha) = \sum_{d=0}^k g_d \alpha^d$ into column vectors $\vec{h} \doteq [h_l \ h_{l-1} \ \cdots \ h_1 \ h_0]^\top$ and $\vec{g} \doteq [g_k \ g_{k-1} \ \cdots \ g_1 \ g_0]^\top$, we can rewrite these equations as the following system of linear equations in the $k+l+2$ coefficients of g and h combined:

$$\begin{bmatrix} a_i^l x_i & a_i^{l-1} x_i & \cdots & x_i & a_i^k & a_i^{k-1} & \cdots & 1 \end{bmatrix}_{i \in [n]} \cdot \begin{bmatrix} \vec{h} \\ -\vec{g} \end{bmatrix} = 0. \quad (12)$$

Note that the system's coefficient matrix has no dependence on the seed f . Consider any square subsystem of Equation (12), formed by choosing $k+l+2$ indices $i_1, i_2, \dots, i_{k+l+2} \in [n]$

and looking at the corresponding rows. After substitution by $\text{RFE}(f)$ for any fixed seed f , the subsystem has a nonzero solution (namely the vector in Equation (12)) and therefore the determinant of its coefficient matrix vanishes.

Before the substitution by $\text{RFE}(f)$, the determinant of the subsystem's coefficient matrix is a polynomial in $x_{i_1}, x_{i_2}, \dots, x_{i_{k+l+2}}$, independent of the seed f :

$$p = \det \left[a_{i_j}^l x_{i_j} \quad a_{i_j}^{l-1} x_{i_j} \quad \dots \quad x_{i_j} \quad a_{i_j}^k \quad a_{i_j}^{k-1} \quad \dots \quad 1 \right]_{j=1}^{k+l+2}.$$

As p vanishes after substitution of the variables by $\text{RFE}_l^k(f)$ for every seed f , by definition p belongs to the vanishing ideal of RFE_l^k . Recalling that p is identically $\text{EVC}_l^k[i_1, i_2, \dots, i_{k+l+2}]$, we have established:

▷ **Claim 5.** For every $k, l \in \mathbb{N}$ and $i_1, i_2, \dots, i_{k+l+2} \in [n]$, $\text{EVC}_l^k[i_1, \dots, i_{k+l+2}] \in \text{Van}[\text{RFE}_l^k]$.

Before moving on, we point out the following properties.

▶ **Proposition 6.** *If any of i_1, \dots, i_{k+l+2} coincide, $\text{EVC}_l^k[i_1, \dots, i_{k+l+2}]$ is zero. Otherwise, it is nonzero, multi-linear, and homogeneous of total degree $l + 1$, and every multi-linear monomial of degree $l + 1$ in $x_{i_1}, \dots, x_{i_{k+l+2}}$ appears with a nonzero coefficient. EVC_l^k is skew-symmetric in that, for any permutation π of i_1, \dots, i_{k+l+2} ,*

$$\text{EVC}_l^k[i_1, \dots, i_{k+l+2}] = (-1)^{\text{sign}(\pi)} \cdot \text{EVC}_l^k[\pi(i_1), \dots, \pi(i_{k+l+2})].$$

The coefficient of $x_{i_1} \cdots x_{i_{l+1}}$ is the product of Vandermonde determinants

$$\left| \begin{array}{ccc|ccc} a_{i_1}^l & \cdots & 1 & a_{i_{l+2}}^k & \cdots & 1 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ a_{i_{l+1}}^l & \cdots & 1 & a_{i_{l+k+2}}^k & \cdots & 1 \end{array} \right|.$$

Proof. All the assertions to be proved follow from elementary properties of determinants, that Vandermonde determinants are nonzero unless they have duplicate rows, and the following computation: After plugging in 1 for $x_{i_1}, \dots, x_{i_{l+1}}$, and 0 for $x_{i_{l+2}}, \dots, x_{i_{l+k+2}}$, the determinant has the form

$$\left| \begin{array}{ccc|ccc} a_{i_1}^l & \cdots & 1 & * & \cdots & * \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ a_{i_{l+1}}^l & \cdots & 1 & * & \cdots & * \\ \hline 0 & \cdots & 0 & a_{i_{l+2}}^k & \cdots & 1 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & a_{i_{l+k+2}}^k & \cdots & 1 \end{array} \right|,$$

which equals the product of Vandermonde matrices in the statement. ◀

Claim 5 shows that the polynomials $\text{EVC}_l^k[i_1, \dots, i_{k+l+2}]$ belong to the vanishing ideal of RFE_l^k . To prove that they collectively generate the vanishing ideal, we use a two-phase approach:

1. We first show that, modulo the ideal $\langle \text{EVC}_l^k \rangle$ generated by the instantiations of EVC_l^k , every polynomial equals a polynomial with a particular combinatorial structure (Lemma 8).
2. We then show that every nonzero polynomial with that structure is hit by RFE_l^k (Lemma 10).

119:12 Polynomial Identity Testing via Evaluation of Rational Functions

Together, these show that every polynomial in the vanishing ideal of RFE_l^k is equal, modulo $\langle \text{EVC}_l^k \rangle$, to the zero polynomial. It follows that the vanishing ideal is generated by instantiations of EVC_l^k .

The combinatorial structure is that of a core, which is the set C in the following definition.

► **Definition 7** (Cored polynomial). *For $c, t \in \mathbb{N}$, a polynomial p is said to be (c, t) -cored if there exists a set of at most c variables such that every monomial of p depends on at most t variables outside that set.*

► **Lemma 8.** *For every $k, l \in \mathbb{N}$, and any $(k + 1)$ -subset $C \subseteq [n]$, every polynomial is equal to a $(k + 1, l)$ -cored polynomial with core $\{x_i : i \in C\}$ modulo the ideal generated by the polynomials $\text{EVC}_l^k[S]$ where S ranges over all sets of size $k + l + 2$ satisfying $C \subseteq S \subseteq [n]$.*

Proof of Lemma 8. Fix k, l , and C as in the statement, and let I be the ideal in the lemma statement. Every monomial m can be uniquely factored as $m_0 m_1$, where m_0 is supported on variables indexed by C and m_1 involves no variable indexed by C . Call m_1 the *non-core* of m . We show the following:

▷ **Claim 9.** Every monomial with more than l variables in its non-core is equivalent, modulo I , to a linear combination of monomials that all have non-cores of lower degree.

This lets us prove Lemma 8 as follows. Claim 9 implies that, for any polynomial p , we may, without changing $p \bmod I$, eliminate any monomial in p that violates the $(k + 1, l)$ -cored condition, while possibly introducing monomials with lower non-core degree. Thus we can systematically eliminate all monomials that violate the cored condition by eliminating them in order of decreasing non-core degree. After that, p is $(k + 1, l)$ -cored with core $\{x_i : i \in C\}$, and the lemma follows.

It remains to show Claim 9. Let m be a monomial with more than l variables in its non-core. Let $L \subseteq [n]$ index a set of $l + 1$ of the variables in the non-core, let m' be their product, and let m'' satisfy $m = m' m''$. Combined, L and C have size exactly $k + l + 2$. Consider $q \doteq \text{EVC}_l^k[L \cup C]$, where the variables in $L \cup C$ are ordered arbitrarily. By Proposition 6, m' appears in q , and every other monomial in q has lower non-core degree than m' . It follows that every monomial in $m'' \cdot q$ either is m , or else has lower non-core degree than m . By the definitions of I and q , $m'' \cdot q$ is in I , so rearranging the equation $m'' \cdot q \equiv 0 \pmod{I}$ to isolate m gives the desired equivalence. ◀

The following lemma completes the proof of the main part of Theorem 2, that the polynomials EVC_l^k generate the vanishing ideal of RFE_l^k .

► **Lemma 10.** *Suppose p is nonzero and $(k + 1, l)$ -cored. Then RFE_l^k hits p .*

Before proving Lemma 10, let us argue how the “moreover” part of Theorem 2 also follows. The combination of Claim 5, Lemma 8, and Lemma 10 shows that, for every core $C \subseteq \{x_1, \dots, x_n\}$ of $k + 1$ variables, each instance p of EVC_l^k that does not use all variables in C lies in the ideal generated by those instances that do use all of C . Since all polynomials of the form EVC_l^k have the same degree, this implies that p is actually linearly dependent on the latter instances. Meanwhile, instances of EVC_l^k with distinct variable sets that use all of C are linearly independent, because they each have a distinct monomial. This shows that the instances in the “moreover” part of Theorem 2 form a linearly independent set that generate all the instances of EVC_l^k . This completes the proof of Theorem 2 modulo the proof of Lemma 10.

Our proof of Lemma 10 involves a key technical analysis that we repeatedly need throughout the paper, and have abstracted into the Zoom Lemma below. In order to state the lemma, we first define the following notions.

► **Definition 11** (Projection of a polynomial). *Let $X \subseteq [n]$, let $p \in \mathbb{F}[x_1, \dots, x_n]$, and consider the expansion of p as a sum of monomials in $\{x_i : i \in X\}$ with coefficients in $\mathbb{F}[x_i : i \notin X]$. For any monomial m supported in $\{x_i : i \in X\}$, the X -projection of p onto m , denoted $\langle m | p \rangle_X$, is the coefficient of m in the aforementioned expansion of p .*

Note that m need not use every variable indexed by X , and in any case $\langle m | p \rangle_X$ depends on no variables indexed by X . The notation in Definition 11 is inspired by the bra-ket notation from physics.

► **Definition 12** (Minorization). *Let $K, L \subseteq [n]$, $p \in \mathbb{F}[x_1, \dots, x_n]$, and m^* a monomial supported in $\{x_i : i \in K \cup L\}$. We say that m^* is (K, L) -unminored in p if, for every monomial m in p , at least one of the following holds:*

- $\deg_{x_i}(m) = \deg_{x_i}(m^*)$ for every $i \in K \cup L$,
- $\deg_{x_i}(m) > \deg_{x_i}(m^*)$ for some $i \in K$, or
- $\deg_{x_i}(m) < \deg_{x_i}(m^*)$ for some $i \in L$.

Equivalently, m^* is (K, L) -unminored in p if $\langle m | p \rangle_{K \cup L} = 0$ for every monomial $m \neq m^*$ supported in $\{x_i : i \in K \cup L\}$ with $\deg_{x_i}(m) \leq \deg_{x_i}(m^*)$ for all $i \in K$, and $\deg_{x_i}(m) \geq \deg_{x_i}(m^*)$ for all $i \in L$.

The above notation lets us state our key technical lemma succinctly. We refer to it as the Zoom Lemma because it lets us zoom in on particular monomial parts of the polynomial p , namely the $(K \cup L)$ -projection onto a (K, L) -unminored monomial m^* .

► **Lemma 13** (Zoom Lemma). *Let $K, L \subseteq [n]$ be sets of variables. Let $p \in \mathbb{F}[x_1, \dots, x_n]$, and m^* a monomial supported in $\{x_i : i \in K \cup L\}$ that is (K, L) -unminored in p . If $\langle m^* | p \rangle_{K \cup L}$ is nonzero at the point*

$$x_i \leftarrow z \cdot \frac{\prod_{i' \in K \setminus L} (a_i - a_{i'})}{\prod_{i' \in L \setminus K} (a_i - a_{i'})} \quad \forall i \in [n] \setminus (K \cup L), \quad (13)$$

for some $z \in \mathbb{F}$ then RFE_i^k hits p with $k = |K|$ and $l = |L|$.

Note that since the $(K \cup L)$ -projection of p depends on no variable indexed by $K \cup L$, the result of the substitution Equation (13) is simply a scalar in \mathbb{F} .

Most of our uses of the Zoom Lemma will moreover have K and L be disjoint, but disjointness is not necessary for the lemma to hold.

Let us first see how the Zoom Lemma allows us complete the proof of Theorem 2.

Proof of Lemma 10 from Lemma 13. Let $C \subseteq [n]$ denote a core for p . Without loss of generality, C is nonempty. Let M denote the set of monomials with nonzero coefficients in p . Let m_1 be a monomial supported in $\{x_i : i \notin C\}$ that is of maximum degree subject to dividing some monomial of p . Let $L \subseteq [n]$ be the indexes of the variables appearing in m_1 ; since p is cored, L has size at most l . Fix $i^* \in C$ arbitrarily, and let $K = C \setminus \{i^*\}$; K has size at most k and is disjoint from L . Finally, among the choices for a monomial m_0 supported on K such that $\langle m_0 m_1 | p \rangle_{K \cup L} \neq 0$, choose one of minimum degree.

The choice of m_1 ensures that every $m \in M$ either has $\deg_{x_i}(m) < \deg_{x_i}(m_1)$ for some $i \in L$, or else $\deg_{x_i}(m) = \deg_{x_i}(m_1)$ for all $i \in L$. In turn, the choice of m_0 ensures that every m in the latter case has $\deg_{x_i}(m) > \deg_{x_i}(m_0)$ for some $i \in K$, or else $\deg_{x_i}(m) = \deg_{x_i}(m_0)$ for all $i \in K$. In the latter of those cases, m must be $m_0 m_1 \cdot x_{i^*}^d$ for some d . In other words, if we set $m^* = m_0 m_1$, then every $m \in M$ satisfies at least one of the following:

119:14 Polynomial Identity Testing via Evaluation of Rational Functions

- $m = m^* \cdot x_{i^*}^d$ for some d ,
- $\deg_{x_i}(m) > \deg_{x_i}(m^*)$ for some $i \in K$, or
- $\deg_{x_i}(m) < \deg_{x_i}(m^*)$ for some $i \in L$.

In particular, m^* is (K, L) -unminored in p , and $\langle m^* | p \rangle_{K \cup L}$ is a nonzero univariate polynomial in x_{i^*} . It follows that for all but finitely many $z \in \mathbb{F}$, substituting Equation (13) into $\langle m^* | p \rangle_{K \cup L}$ has a nonzero result. By the Zoom Lemma, RFE_l^k hits p . ◀

Finally, we establish the Zoom Lemma. Below we provide a proof from first principles. However, we take intuition from thinking in terms of Laurent expansions, which are like power series, except that the exponents may go negative. We describe the underlying intuition for readers familiar with the notion.

Consider RFE_l^k in the roots parameterization, where the seed $f = g/h$ is specified by the k roots of the numerator g , the l roots of the denominator h , and an additional scaling parameter ζ (cf. Appendix A, or Equation (14) below). We match each of the roots of g to a unique index in K , and each of the roots of h to a unique index in L . For each $i \in [n]$, $f(a_i)$ is a rational function in the root parameters and ζ , and moreover is a product of univariate rational functions. For each i and root parameter σ with matching index i , we can expand the univariate rational function in σ to its Laurent series about $\sigma = a_i$. Then we carry these expansions into $p(\text{RFE}_l^k(f))$ and expand fully, collecting terms according to the powers of the various $\sigma - a_i$. The result is a multivariate Laurent expansion of $p(\text{RFE}_l^k(f))$ with respect to the root parameters around their matching abscissas, with coefficients that are polynomials in ζ . According to our matching between the root parameters and the variables in K and L , we can index the coefficients in the Laurent expansion of $p(\text{RFE}_l^k(f))$ by the monomials supported in $\{x_i : i \in K \cup L\}$. The point is that, since m^* is (K, L) -unminored in p , the only contribution to the coefficient indexed by m^* comes from the constant term in the corresponding Laurent expansion of $q(\text{RFE}_l^k(f))$, where q is the $(K \cup L)$ -projection of p onto m^* . Since q does not depend on any variable indexed by $K \cup L$, this Laurent expansion of $q(\text{RFE}_l^k(f))$ has no terms of negative exponent, so the constant term may be computed by substituting $\sigma \leftarrow a_i$ into $q(\text{RFE}_l^k(f))$ for each root parameter σ with matching index i . After moreover substituting $\zeta \leftarrow z$, this equals the substitution of (13) into q . Since the substitution of (13) into q is nonzero, we conclude that $p(\text{RFE}_l^k(f))$ is a nonzero function of the parameters, and so RFE_l^k hits p .

Proof of Lemma 13. Let ζ, σ_i for each $i \in K$, and τ_i for each $i \in L$ be fresh, distinct indeterminates. Let $\widehat{\mathbb{F}}$ be the field of rational functions in those indeterminates with coefficients in \mathbb{F} , and let

$$\hat{f}(\alpha) \doteq \zeta \cdot \frac{\prod_{i \in K} (\alpha - \sigma_i)}{\prod_{i \in L} (\alpha - \tau_i)} \in \widehat{\mathbb{F}}(\alpha). \quad (14)$$

Let $\text{RFE}_l^k(\hat{f}) \in \widehat{\mathbb{F}}^n$ be the point $(\hat{f}(a_i) : i \in [n])$, and consider $p(\text{RFE}_l^k(\hat{f})) \in \widehat{\mathbb{F}}$. Any substitution of ζ, σ_i , and τ_i by scalars in \mathbb{F} such that each $\tau_i \notin \{a_1, \dots, a_n\}$ sends \hat{f} to some f in the domain of RFE_l^k , and $p(\text{RFE}_l^k(\hat{f}))$ to $p(\text{RFE}_l^k(f))$. If $p(\text{RFE}_l^k(f))$ is nonzero, then a random such substitution will have nonzero outcome. So if we can show that $p(\text{RFE}_l^k(\hat{f}))$ is nonzero, then p is hit by RFE_l^k .

Recall m^* and z from the lemma statement, and consider the following process Φ . Given an element of $\widehat{\mathbb{F}}$, first multiply it by

$$\frac{\prod_{i \in L} (a_i - \tau_i)^{\deg_{x_i}(m^*)}}{\prod_{i \in K} (a_i - \sigma_i)^{\deg_{x_i}(m^*)}},$$

then cancel any common factors in the numerator and denominator, and then substitute

$$\begin{aligned}\sigma_i &\leftarrow a_i && \text{for } i \in K \\ \tau_i &\leftarrow a_i && \text{for } i \in L \quad . \\ \zeta &\leftarrow z\end{aligned}$$

For any monomial m such that both

$$\begin{aligned}\deg_{x_i}(m) &\geq \deg_{x_i}(m^*) && \text{for all } i \in K, \text{ and} \\ \deg_{x_i}(m) &\leq \deg_{x_i}(m^*) && \text{for all } i \in L,\end{aligned}\tag{15}$$

applying Φ to $m(\text{RFE}_l^k(\hat{f}))$ yields a defined result, which is just a scalar in \mathbb{F} . (For other monomials the result has a division by zero, but this will not matter.) If any of the inequalities in Equation (15) is strict, the result is zero. Otherwise, $m = m^* \cdot m'$ for some monomial m' supported on $\{x_i : i \notin K \cup L\}$, and the result is

$$\left[\prod_{i \in K \cup L} \left(\zeta \cdot \frac{\prod_{i' \in K \setminus \{i\}} a_i - a_{i'}}{\prod_{i' \in L \setminus \{i\}} a_i - a_{i'}} \right)^{\deg_{x_i}(m^*)} \right] \cdot m'(x_i \leftarrow f^*(a_i))\tag{16}$$

where $f^*(\alpha)$ is $\hat{f}(\alpha)$ with each occurrence of σ_i and τ_i substituted by the corresponding a_i , and ζ replaced by z . Note that m' is supported on $\{x_i : i \in [n] \setminus (K \cup L)\}$, and $f^*(a_i)$ is well-defined for all $i \in [n] \setminus (K \cup L)$. Note also that the first factor in Equation (16) is nonzero and independent of m' .

Our hypothesis that m^* is (K, L) -unminored in p implies that p is a linear combination of monomials that satisfy Equation (15). Thus applying Φ to $p(\text{RFE}_l^k(\hat{f}))$ has a defined output. This output is precisely the first factor in Equation (16) times the evaluation of $\langle m^* | p \rangle_{K \cup L}$ at $(f^*(a_i) : i \in [n] \setminus (K \cup L))$. Meanwhile, $(f^*(a_i) : i \in [n] \setminus (K \cup L))$ is identically Equation (13), and we have hypothesized that $\langle m^* | p \rangle_{K \cup L}$ does not vanish there. It follows that applying Φ to $p(\text{RFE}_l^k(\hat{f}))$ has a nonzero outcome. On the other hand, if $p(\text{RFE}_l^k(\hat{f}))$ were zero, applying Φ would result in zero. It follows that $p(\text{RFE}_l^k(\hat{f})) \neq 0$, proving the lemma. \blacktriangleleft

3 Membership Test

In this section we develop the structured membership test for the vanishing ideal $\text{Van}[\text{RFE}_l^k]$ given in Theorem 3. We start by observing that it suffices to establish the following simpler version of Theorem 3 for the case where p is homogeneous.

► **Lemma 14.** *A nonzero homogeneous multi-linear polynomial p in the variables x_1, \dots, x_n belongs to $\text{Van}[\text{RFE}_l^k]$ if and only if both of the following conditions hold:*

1. *The degree of p satisfies $l < \deg(p) < n - k$.*
2. *For all disjoint subsets $K, L \subseteq [n]$ with $|K| = k$ and $|L| = l$, $\left(\frac{\partial p}{\partial L} \right) \Big|_{K \leftarrow 0}$ evaluates to zero upon substituting for each $i \in [n] \setminus (K \cup L)$*

$$x_i \leftarrow \frac{\prod_{i' \in K} (a_i - a_{i'})}{\prod_{i' \in L} (a_i - a_{i'})}.\tag{17}$$

To see why the general case reduces to the homogeneous case, we make use of the following property, well-known in the context of SV. We include a proof for completeness.

119:16 Polynomial Identity Testing via Evaluation of Rational Functions

► **Proposition 15.** *For any polynomial p , p vanishes at RFE if and only if every homogeneous part of p vanishes at RFE.*

Proof of Proposition 15. For any seed f for RFE and $\zeta \in \mathbb{F}$, $\zeta \cdot f$ is another seed for RFE over the extended field $\mathbb{F}(\zeta)$ of rational functions in ζ . Write $p = \sum_d p_d$ as a sum of homogeneous polynomials, where p_d has degree d . Since p_d is homogeneous, $p_d(\text{RFE}(\zeta \cdot f)) = \zeta^d \cdot p_d(\text{RFE}(f))$. Thus for every f ,

$$p(\text{RFE}(\zeta \cdot f)) = \sum_d p_d(\text{RFE}(\zeta \cdot f)) = \sum_d \zeta^d \cdot p_d(\text{RFE}(f))$$

is a polynomial $q_f(\zeta) \in \mathbb{F}[\zeta]$. If, for all f and d , $p_d(\text{RFE}(f)) = 0$, then q_f is the zero polynomial for all f , so $p(\text{RFE}(f)) = q_f(1) = 0$ for all f . Conversely, if $p(\text{RFE}(z \cdot f)) = q_f(z) = 0$ for all f and $z \in \mathbb{F}$, then q_f is the zero polynomial for all f , so $p_d(\text{RFE}(f)) = 0$ for all f and d . ◀

Here is how Theorem 3 follows from Lemma 14.

Proof of Theorem 3 from Lemma 14. Write $p = \sum_d p_d$ as a sum of homogeneous parts. By Proposition 15, $p \in \text{Van}[\text{RFE}_l^k]$ if and only if every $p_d \in \text{Van}[\text{RFE}_l^k]$. The degree constraints in Lemma 14 show that condition 1 in Theorem 3 is necessary. Thus, in order to establish Theorem 3, we only need to consider polynomials p for which $p_d = 0$ for $d \leq l$ and $d \geq n - k$, and show that for any such p , all the evaluations Equation (6) of p are zero if and only if for all d , all the evaluations Equation (17) of p_d are zero.

Fix K, L, Z as in the statements of Theorem 3 and Lemma 14, and let $Y = [n] \setminus (K \cup L)$. Let $\lambda \in \mathbb{F}^Y$ be the point Equation (17), and for $z \in Z$, let $z \cdot \lambda$ denote the point Equation (6). We claim $\left(\frac{\partial p}{\partial L}\right)\Big|_{K \leftarrow 0}$ vanishes at $z\lambda$ for all $z \in Z$ if and only if $\left(\frac{\partial p_d}{\partial L}\right)\Big|_{K \leftarrow 0}$ vanishes at λ for all d . Let ζ be an indeterminate. We have

$$\left(\frac{\partial p}{\partial L}\right)\Big|_{K \leftarrow 0}(\zeta\lambda) = \sum_{l < d < n-k} \left(\frac{\partial p_d}{\partial L}\right)\Big|_{K \leftarrow 0}(\zeta\lambda) = \sum_{l < d < n-k} \zeta^{d-l} \left(\frac{\partial p_d}{\partial L}\right)\Big|_{K \leftarrow 0}(\lambda).$$

This is a polynomial in ζ , say $q(\zeta)$. Evaluating q at $\zeta \leftarrow z$ coincides with evaluating $\left(\frac{\partial p}{\partial L}\right)\Big|_{K \leftarrow 0}$ at $z\lambda$, while the coefficient of ζ^{d-l} coincides with evaluating $\left(\frac{\partial p_d}{\partial L}\right)\Big|_{K \leftarrow 0}$ at λ . q factors as $\zeta \cdot q'$ where q' has degree at most $n - k - l - 2$. Therefore q vanishes on any fixed set of at least $n - k - l - 1$ nonzero field elements – in particular Z – if and only if it is the zero polynomial. Theorem 3 follows. ◀

It remains to prove Lemma 14. We once again make use of the Zoom Lemma (Lemma 13). Note that for multi-linear polynomials and disjoint K and L , $\left(\frac{\partial p}{\partial L}\right)\Big|_{K \leftarrow 0}$ coincides with the projection $\langle m^* | p \rangle_{K \cup L}$ where $m^* = \prod_{i \in L} x_i$. Moreover, since p is multi-linear, the condition that m^* be (K, L) -unminored in p is automatically satisfied: the only multi-linear monomial m supported in $K \cup L$ with $\deg_{x_i}(m) \leq \deg_{x_i}(m^*)$ for all $i \in K$ and $\deg_{x_i}(m) \geq \deg_{x_i}(m^*)$ for all $i \in L$ is $m = m^*$. This leads to the following specialization of the Zoom Lemma for multi-linear polynomials with disjoint K and L :

► **Lemma 16.** *Let $K, L \subseteq [n]$ be disjoint, and let $p \in \mathbb{F}[x_1, \dots, x_n]$ be a multi-linear polynomial. If $\langle \prod_{i \in L} x_i | p \rangle_{K \cup L}$ is nonzero at the point*

$$x_i \leftarrow z \cdot \frac{\prod_{i' \in K} (a_i - a_{i'})}{\prod_{i' \in L} (a_i - a_{i'})} \quad \forall i \in [n] \setminus (K \cup L), \quad (18)$$

for some $z \in \mathbb{F}$ then RFE_l^k hits p with $k = |K|$ and $l = |L|$.

In proving Lemma 14, we will apply Lemma 16 only to homogeneous polynomials, in which case we can take $z = 1$ without loss of generality. With that in mind, observe that Equation (17) in Lemma 14 coincides with the substitution Equation (18) from Lemma 16. So Lemma 14 amounts to saying that a homogeneous multilinear polynomial p is hit by RFE_l^k if and only if its degree is too low, its degree is too high, or else there is a way to apply Lemma 16 to prove that p is hit by RFE_l^k .

Proof of Lemma 14. Suppose that $\deg(p) \leq l$. Set L to be the indices of the variables appearing in some monomial with nonzero coefficient in p , and set $K \leftarrow \emptyset$. $\langle \prod_{i \in L} x_i \mid p \rangle_{K \cup L}$ is a nonzero constant. Lemma 16 applies, concluding that RFE_l^0 , and hence RFE_l^k , hits p .

Suppose now that $\deg(p) \geq n - k$. Set K to be the indices of the variables *not* appearing in some monomial with nonzero coefficient in p , and set $L \leftarrow \emptyset$. $\langle 1 \mid p \rangle_{K \cup L}$ is a single monomial, namely the product of the variables indexed by $[n] \setminus (K \cup L)$. Lemma 16 applies. Since none of the substitutions in Equation (18) is zero, we conclude that RFE_0^k , and hence RFE_l^k , hits p .

Now consider the case $l < \deg(p) < n - k$. We start by writing p as a multi-linear element of $\text{Van}[\text{RFE}_l^k]$ plus a structured remainder term. It can be shown similarly to Lemma 8; we include a proof below.

▷ **Claim 17.** Let $l < d < n - k$. Every homogeneous degree- d multi-linear polynomial can be written as $p_0 + r$ where p_0 and r are degree- d homogeneous multi-linear polynomials, $p_0 \in \text{Van}[\text{RFE}_l^k]$ and r is $(d + k - l, l)$ -cored.

Let p_0, r be the result of applying the claim to p . By the contrapositive of Lemma 16, it holds that for every pair of disjoint subsets $K, L \subseteq [n]$ of sizes k and l respectively, the projection $\langle \prod_{i \in L} x_i \mid p_0 \rangle_{K \cup L}$ evaluates to zero at Equation (17). Since $\langle \prod_{i \in L} x_i \mid p \rangle_{K \cup L} = \langle \prod_{i \in L} x_i \mid p_0 \rangle_{K \cup L} + \langle \prod_{i \in L} x_i \mid r \rangle_{K \cup L}$, it follows that evaluating $\langle \prod_{i \in L} x_i \mid p \rangle_{K \cup L}$ at Equation (17) has the same result as evaluating $\langle \prod_{i \in L} x_i \mid r \rangle_{K \cup L}$. In light of this, Lemma 14 follows from the following claim, proven below:

▷ **Claim 18.** Let $l < d < n - k$. Let r be a nonzero degree- d homogeneous multi-linear polynomial that is $(d + k - l, l)$ -cored. There are disjoint sets $K, L \subseteq [n]$ with $|K| = k$ and $|L| = l$ so that $\langle \prod_{i \in L} x_i \mid r \rangle_{K \cup L}$ is a single monomial.

Substituting Equation (17) into a single monomial yields a nonzero value. ◀

We complete the argument by proving Claim 17 and Claim 18. Claim 17 is similar to Lemma 8, and is obtained using a variant of polynomial division suited to multi-linear polynomials:

Proof of Claim 17. Let $C \subseteq [n]$ have size $d + k - l$. Every multi-linear monomial m can be uniquely factored as $m_0 m_1$, where m_0 and m_1 are multi-linear monomials supported in $\{x_i : i \in C\}$ and $\{x_i : i \notin C\}$ respectively. Call m_1 the *non-core* of m . We show the following:

▷ **Claim 19.** Every multi-linear monomial with more than l variables in its non-core is equivalent, modulo a multi-linear element of $\text{Van}[\text{RFE}_l^k]$, to a linear combination of multi-linear monomials that all have non-cores of lower degree.

This lets us prove Claim 17 as follows. Claim 19 implies that, for any multi-linear polynomial p , we may, without changing p modulo multi-linear elements of $\text{Van}[\text{RFE}_l^k]$, eliminate any monomial in p that violates the $(d + k - l, l)$ -cored condition, while possibly

119:18 Polynomial Identity Testing via Evaluation of Rational Functions

introducing multi-linear monomials with lower non-core degree. Thus we can systematically eliminate all monomials that violate the cored condition by eliminating them in order of decreasing non-core degree. After that, p is $(d + k - l, l)$ -cored (with core $\{x_i : i \in C\}$), and Claim 17 follows.

We now show Claim 19. Factor $m = m_0 m_1$ as above, and suppose there are more than l variables in m_1 . Let L index some $l + 1$ of the variables in m_1 , let m' be their product, and let m'' satisfy $m = m' m''$. There are at most $d - l - 1$ variables in m_0 ; let K be any $k + 1$ elements of C that index variables not in m_0 . Combined, L and K have size exactly $k + l + 2$. Consider $q = \text{EVC}_l^k[L \cup K]$, where the variables in $L \cup K$ are ordered arbitrarily. By Proposition 6, m' appears as a monomial in q ; moreover, every other monomial in q has lower non-core degree. It follows that every monomial in $m'' \cdot q$ either is m , or else has lower non-core degree. Moreover, every such monomial is multi-linear and is supported in $\{x_i : i \in K \cup L\}$, which is disjoint from the support of m'' . As q is in $\text{Van}[\text{RFE}_l^k]$, rearranging the equation $m'' \cdot q \equiv 0 \pmod{\text{Van}[\text{RFE}_l^k]}$ to isolate m gives the desired equivalence. \triangleleft

Claim 18 is similar to the proof of Lemma 10:

Proof of Claim 18. Let $C \subseteq [n]$ be the indices of variables that form a core for r . Recall that $l < d < n - k$. By shrinking C if need be, we can assume there is a multi-linear monomial m with nonzero coefficient in r that involves exactly l variables not indexed by C . Let L be the variables appearing in m that are not indexed by C . Now extend C to have size $d + k - l$ while remaining disjoint from L . There are precisely k variables indexed by C that do not appear in m ; let K be this set. Since r is multi-linear, homogeneous of degree d , and $(d + k - l, l)$ -cored with core C , there is exactly one monomial with nonzero coefficient in r that is divisible by $\prod_{i \in L} x_i$ and by no variable in K : it is precisely m . It follows that the projection $\langle \prod_{i \in L} x_i | r \rangle_{K \cup L}$ is a single monomial. \triangleleft

We conclude this section by detailing the connection between Theorem 3 and some prior applications of the SV-generator.

Application to read-once formulas

We start with the theorem that SV^1 hits read-once formulas. The original proof in [26] goes by induction on the depth of F , showing that $F(\text{SV}^1)$ is nonconstant whenever F is nonconstant, or, equivalently, that SV^1 hits $F + c$ for every $c \in \mathbb{F}$ whenever F is nonconstant. The inductive step consists of two cases, depending on whether the top gate is a multiplication gate or an addition gate. The case of a multiplication gate follows from the general property that the product of a nonconstant polynomial with any nonzero polynomial is nonconstant. The case of an addition gate, say $F = F_1 + F_2$, involves a clever analysis that uses the variable-disjointness of F_1 and F_2 to show that $F_1(\text{SV}^1)$ and $F_2(\text{SV}^1)$ cannot cancel each other out.

The case of an addition gate $F = F_1 + F_2$ alternately follows from Theorem 3 with $k = 0$ and $l = 1$ and the following two observations, each corresponding to one of the conditions in Theorem 3. Both observations are immediate because of the variable-disjointness of F_1 and F_2 :

1. If at least one of F_1 or F_2 has a homogeneous component of degree 1 or at least n , then so does F .
2. If for $L = \{i\} \subseteq [n]$ at least one of the derivatives $\frac{\partial F_1}{\partial x_i}$ or $\frac{\partial F_2}{\partial x_i}$ is nonzero at some point (6), then the same goes for $\frac{\partial F}{\partial x_i}$.

In particular, under the hypothesis that $F_1 + c$ is hit by RFE_1^0 for all $c \in \mathbb{F}$, F_1 must violate one of the conditions of Theorem 3 besides the one that requires F_1 have no constant term. Similarly for F_2 . By the above observations, any such a violation is inherited by F , and the inductive step follows.

In the overview, we mentioned that we originally proved Theorem 3 from a perspective that carries a geometric interpretation. The case of an addition gate in the above proof takes a particularly clean form in that perspective, which we sketch now.

Recall from the overview that we can think of the variables as vertices, and multi-linear monomials simplices made from those vertices. A multi-linear polynomial is a weighted collection of such simplices with weights from \mathbb{F} . In this view, Theorem 3 translates to the following characterization: a weighted collection of simplices corresponds to a polynomial in the vanishing ideal of RFE_1^0 if and only if there are no simplices of zero, one, or all vertices, and the remaining weights satisfy a certain system of linear equations. Crucially, for each equation in the system, there is a vertex such that the equation reads only weights of the simplices *that contain that vertex*. Meanwhile, the sum of two variable-disjoint polynomials corresponds to taking the vertex-disjoint union of two weighted collections of simplices. It follows directly that if either term in the sum violates a requirement besides the “no simplex of zero vertices” requirement, then the sum violates the same requirement.

Zero-substitutions and partial derivatives

As mentioned in the overview, several prior papers demonstrated the utility of partial derivatives and zero substitutions in the context of derandomizing PIT using the SV-generator, especially for syntactically multi-linear models. By judiciously choosing variables for those operations, these papers managed to simplify p and reduce PIT for p to PIT for simpler instances, resulting in an efficient recursive algorithm. Such recursive arguments can be naturally reformulated to use Theorem 3, according to the following prototype.

Let \mathcal{C} be a family of multi-linear polynomials, such as those computable with some bounded complexity in some syntactic model. For the argument, we break up $\mathcal{C} = \bigcup_{k,l} \mathcal{C}_{k,l}$ such that for every k, l and $p \in \mathcal{C}_{k,l}$, at least one of the following holds:

- $k = l = 0$ and p is either zero or hit by RFE_0^0 .
- $k > 0$ and there is a zero substitution such that the result is in $\mathcal{C}_{k-1,l}$.
- $l > 0$ and there is a derivative such that the result is in $\mathcal{C}_{k,l-1}$.

We also make the mild assumption that each $\mathcal{C}_{k,l}$ is closed under rescaling variables. With these hypotheses in place, we establish the following claim through direct applications of Theorem 3:

▷ **Claim 20.** Under the above hypotheses, RFE_l^k hits $\mathcal{C}_{k,l}$ for every k, l .

Proof. The proof is by induction on k and l . The base case is $k = l = 0$, where the claim is immediate. When $k > 0$ or $l > 0$, our hypotheses are such that p either simplifies under a zero substitution $x_{i^*} \leftarrow 0$ or a derivative $\frac{\partial}{\partial x_{i^*}}$. We analyze each case separately. By condition 1 of Theorem 3, we may assume that p only has homogeneous parts with degrees in the range $l + 1, \dots, n - k - 1$.

- If p simplifies under a zero substitution $x_{i^*} \leftarrow 0$, then let $p' \in \mathcal{C}_{k-1,l}$ be the simplified polynomial where moreover the remaining variables have been rescaled according to $x_i \leftarrow x_i \cdot (a_{i^*} - a_i)$. That is, write p as $p = qx_{i^*} + r$ where q and r are polynomials that do not depend on x_{i^*} , and set $p'(\dots, x_i, \dots) \doteq r(\dots, x_i \cdot (a_{i^*} - a_i), \dots)$. By induction, p' is hit by RFE_l^{k-1} . We apply Theorem 3 to p' with respect to the set of variables

$\{x_1, \dots, x_{i^*-1}, x_{i^*+1}, \dots, x_n\}$ and k replaced by $k - 1$. As p only has homogeneous parts with degrees in the range $l + 1, \dots, n - k - 1$, so does p' , and condition 1 of Theorem 3 fails. By condition 2, there must be $z \in Z$ and disjoint $K, L \subseteq [n] \setminus \{i\}$ with $|K| = k - 1$ and $|L| = l$ so that substituting (6) yields a nonzero value. It follows directly that, with respect to the same z , $K' = K \cup \{i\}$, and the same L , the substitution (6) yields a nonzero value when applied to p .

- If p simplifies under a partial derivative $\frac{\partial}{\partial x_{i^*}}$, then a similar analysis works. Set $p' \in \mathcal{C}_{k,l-1}$ to be the simplification with variables rescaled according to $x_i \leftarrow x_i / (a_{i^*} - a_i)$. That is, write p as $p = qx_{i^*} + r$ where q and r are polynomials that do not depend on x_{i^*} , and set $p'(\dots, x_i, \dots) \doteq q(\dots, x_i / (a_{i^*} - a_i), \dots)$. By induction, p' is hit by RFE_{l-1}^k . We apply Theorem 3 to p' with respect to the set of variables $\{x_1, \dots, x_{i^*-1}, x_{i^*+1}, \dots, x_n\}$ and l replaced by $l - 1$. As p' has homogeneous parts of degrees one less than p does, condition 1 of Theorem 3 fails. By condition 2, there is $z \in Z$ and disjoint $K, L \subseteq [n] \setminus \{i\}$ with $|K| = k$ and $|L| = l - 1$ so that substituting (6) yields a nonzero value. It follows directly that, with respect to the same z , the same K , and $L' = L \cup \{i^*\}$, the substitution (6) yields a nonzero value when applied to p . ◀

Theorem 3 tells us that derivatives and zero substitutions suffice to witness when a multi-linear polynomial p is hit by SV or RFE. One can ask, if we know more information about p , can we infer *which* derivatives and zero substitutions form a witness? In some cases we know. For example, if p has a low-support monomial $x_1 \cdots x_l$, then it suffices to take derivatives with respect to each of x_1, \dots, x_l . On the other hand, consider that whenever two polynomials p and q are hit by SV, then so is their product pq . Given explicit witnesses for p and q , we do not know how to obtain an explicit witness for the product pq .

References

- 1 Manindra Agrawal. Proving lower bounds via pseudo-random generators. In *International Conference on Foundations of Software Technology and Theoretical Computer Science (FSTTCS)*, pages 92–105. Springer, 2005.
- 2 Manindra Agrawal, Rohit Gurjar, Arpita Korwar, and Nitin Saxena. Hitting-sets for ROABP and sum of set-multilinear circuits. *SIAM Journal on Computing*, 44(3):669–697, 2015.
- 3 Manindra Agrawal, Chandan Saha, and Nitin Saxena. Quasi-polynomial hitting-set for set-depth- Δ formulas. In *ACM Symposium on Theory of Computing (STOC)*, pages 321–330, 2013.
- 4 Matthew Anderson, Michael A Forbes, Ramprasad Satharishi, Amir Shpilka, and Ben Lee Volk. Identity testing and lower bounds for read- k oblivious algebraic branching programs. *ACM Transactions on Computation Theory*, 10(1):1–30, 2018.
- 5 Matthew Anderson, Dieter van Melkebeek, and Ilya Volkovich. Deterministic polynomial identity tests for multilinear bounded-read formulae. *Computational Complexity*, 24(4):695–776, 2015.
- 6 Vishwas Bhargava and Sumanta Ghosh. Improved Hitting Set for Orbit of ROABPs. In *Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques (APPROX/RANDOM 2021)*, pages 30:1–30:23, 2021.
- 7 David A Cox, John Little, and Donal O’Shea. *Ideals, varieties, and algorithms: an introduction to computational algebraic geometry and commutative algebra*. Springer Science & Business Media, 2013.
- 8 Richard A Demillo and Richard J Lipton. A probabilistic remark on algebraic program testing. *Information Processing Letters*, 7(4):193–195, 1978.
- 9 Michael A Forbes. Deterministic divisibility testing via shifted partial derivatives. In *IEEE Symposium on Foundations of Computer Science (FOCS)*, pages 451–465, 2015.

- 10 Michael A Forbes, Ramprasad Satharishi, and Amir Shpilka. Hitting sets for multilinear read-once algebraic branching programs, in any order. In *ACM Symposium on Theory of Computing (STOC)*, pages 867–875, 2014.
- 11 Michael A Forbes and Amir Shpilka. Quasipolynomial-time identity testing of non-commutative and read-once oblivious algebraic branching programs. In *IEEE Symposium on Foundations of Computer Science (FOCS)*, pages 243–252, 2013.
- 12 Michael A Forbes, Amir Shpilka, and Ben Lee Volk. Succinct hitting sets and barriers to proving algebraic circuits lower bounds. In *ACM SIGACT Symposium on Theory of Computing (STOC)*, pages 653–664, 2017.
- 13 Hervé Fournier and Arpita Korwar. Limitations of the Shpilka–Volkovich generator. Workshop on Algebraic Complexity Theory (WACT), Paris, 2018.
- 14 Zeyu Guo and Rohit Gurjar. Improved explicit hitting-sets for ROABPs. In *Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques (APPROX/RANDOM)*, 2020.
- 15 Rohit Gurjar, Arpita Korwar, and Nitin Saxena. Identity testing for constant-width, and any-order, read-once oblivious arithmetic branching programs. *Theory of Computing*, 13(2):1–21, 2017.
- 16 Rohit Gurjar, Arpita Korwar, Nitin Saxena, and Thomas Thierauf. Deterministic identity testing for sum of read-once oblivious arithmetic branching programs. *Computational Complexity*, 26(4):835–880, 2017.
- 17 Joos Heintz and Claus-Peter Schnorr. Testing polynomials which are easy to compute. In *ACM Symposium on Theory of Computing (STOC)*, pages 262–272, 1980.
- 18 Russell Impagliazzo and Avi Wigderson. P=BPP if E requires exponential circuits: Derandomizing the XOR lemma. In *ACM Symposium on Theory of Computing (STOC)*, pages 220–229, 1997.
- 19 Maurice Jansen, Youming Qiao, and Jayalal Sarma M.N. Deterministic Black-Box Identity Testing π -Ordered Algebraic Branching Programs. In *IARCS Conference on Foundations of Software Technology and Theoretical Computer Science (FSTTCS)*, volume 8, pages 296–307, 2010.
- 20 Maurice Jansen, Youming Qiao, and Jayalal Sarma. Deterministic identity testing of read-once algebraic branching programs. *arXiv preprint arXiv:0912.2565*, 2009.
- 21 Valentine Kabanets and Russell Impagliazzo. Derandomizing polynomial identity tests means proving circuit lower bounds. *Computational Complexity*, 13(1-2):1–46, 2004.
- 22 Zohar S Karnin, Partha Mukhopadhyay, Amir Shpilka, and Ilya Volkovich. Deterministic identity testing of depth-4 multilinear circuits with bounded top fan-in. *SIAM Journal on Computing*, 42(6):2114, 2013.
- 23 Arpita Korwar. Personal communication, February 2021.
- 24 Mrinal Kumar and Shubhangi Saraf. Arithmetic circuits with locally low algebraic rank. *Theory of Computing*, 13(1):1–33, 2017.
- 25 Dori Medini and Amir Shpilka. Hitting Sets and Reconstruction for Dense Orbits in VP_e and $\Sigma\Pi\Sigma$ Circuits. In *Computational Complexity Conference (CCC)*, volume 200, pages 19:1–19:27, 2021.
- 26 Daniel Minahan and Ilya Volkovich. Complete derandomization of identity testing and reconstruction of read-once formulas. *ACM Transactions on Computation Theory (TOCT)*, 10(3):1–11, 2018.
- 27 Noam Nisan. Lower bounds for non-commutative computation. In *ACM Symposium on Theory of Computing (STOC)*, pages 410–418, 1991.
- 28 Noam Nisan and Avi Wigderson. Hardness vs randomness. *Journal of Computer and System Sciences*, 49(2):149–167, 1994.
- 29 Øystein Ore. Über höhere Kongruenzen. *Norsk Mat. Forenings Skrifter*, 1(7):15, 1922.
- 30 Ran Raz and Amir Shpilka. Deterministic polynomial identity testing in non-commutative models. *Computational Complexity*, 14(1):1–19, 2005.

- 31 Chandan Saha and Bhargav Thankey. Hitting Sets for Orbits of Circuit Classes and Polynomial Families. In *Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques (APPROX/RANDOM 2021)*, pages 50:1–50:26, 2021.
- 32 Jacob T Schwartz. Fast probabilistic algorithms for verification of polynomial identities. *Journal of the ACM*, 27(4):701–717, 1980.
- 33 Amir Shpilka and Ilya Volkovich. Read-once polynomial identity testing. *Computational Complexity*, 24(3):477–532, 2015.
- 34 Amir Shpilka and Amir Yehudayoff. *Arithmetic circuits: A survey of recent results and open questions*. Now Publishers Inc, 2010.
- 35 Richard Zippel. Probabilistic algorithms for sparse polynomials. In *International symposium on symbolic and algebraic manipulation*, pages 216–226, 1979.

A RFE as a Hitting Set Generator

An ambiguity in Definition 1 is how to parameterize the seed by scalars. There are qualitatively distinct ways to go about this. They are all equivalent over large enough fields, however, so the option to choose is a source of convenience. Some natural parameterizations are the following:

Coefficients. Select scalars $g_0, \dots, g_k, h_0, \dots, h_l \in \mathbb{F}$ and set

$$f(\alpha) = \frac{g_k \alpha^k + g_{k-1} \alpha^{k-1} + \dots + g_1 \alpha + g_0}{h_l \alpha^l + h_{l-1} \alpha^{l-1} + \dots + h_1 \alpha + h_0},$$

ignoring choices of h_0, \dots, h_l for which the denominator vanishes on some a_x .

Evaluations. Fix two collections, $B = \{b_1, \dots, b_{k+1}\}$ and $C = \{c_1, \dots, c_{l+1}\}$, each of distinct scalars from \mathbb{F} . Then select scalars g_1, \dots, g_{k+1} and h_1, \dots, h_{l+1} and set

$$f(\alpha) = \frac{g(\alpha)}{h(\alpha)}$$

where g is the unique degree- k polynomial with $g(b_1) = g_1, g(b_2) = g_2, \dots, g(b_{k+1}) = g_{k+1}$, and h is defined similarly with respect to C . Choices of h_1, \dots, h_{l+1} that imply $h(a_i) = 0$ for some $i \in [n]$ are ignored.

Note that an explicit formula for g and h in terms of the parameters can be obtained using the Lagrange interpolants with respect to B and C .

Roots. Select scalars $z, s_1, \dots, s_{k'}, t_1, \dots, t_{l'} \in \mathbb{F}$ for some $k' \leq k$ and $l' \leq l$ and set

$$f(\alpha) = z \cdot \frac{(\alpha - s_1) \cdots (\alpha - s_{k'})}{(\alpha - t_1) \cdots (\alpha - t_{l'})},$$

where $\{t_1, \dots, t_{l'}\}$ is disjoint from $\{a_i : i \in [n]\}$.

In fact, it is no loss of power to restrict to $k' = k$ and $l' = l$.

Hybrids are of course possible, too. For example, Lemma 23 uses the evaluations parameterization for the numerator and roots parameterization for the denominator.

Quantitative bounds on the number of substitutions to perform follow from the following extension of the corresponding well-known result for polynomials [29, 8, 35, 32]:

► **Lemma 21.** *Let \mathbb{F} be field, and $f = g/h \in \mathbb{F}(\tau_1, \dots, \tau_l)$ be a rational function in l variables with $\deg(g) \leq d$ and $\deg(h) \leq d$. Let $S \subseteq \mathbb{F}$ be finite. Then the probability that f vanishes or is undefined when each τ_i is substituted by a uniformly random element of S is at most $2d/|S|$.*

If \mathbb{F} is not large enough to allow making the probability bound in Lemma 21 sufficiently small, we work with a sufficiently large extension field of \mathbb{F} instead of \mathbb{F} itself.

In this paper we analyze RFE by using fresh formal variables in the above parameterizations of the seed, and calculate in the field of rational functions in those variables. Evaluating $p(\text{RFE}_l^k)$ for a polynomial p thus yields a rational function in those variables. Lemma 21 justifies that as long as \mathbb{F} is large enough, this rational function is the zero rational function if and only if for every choice of scalars for the seed parameters, $p(\text{RFE}_l^k)$ is zero.

B Equivalence between RFE and SV

The Shpilka-Volkovich generator can be defined as follows in the format of our definition of RFE.

► **Definition 22** (SV Generator). *The Shpilka–Volkovich (SV) Generator for polynomials in the variables x_1, \dots, x_n is parameterized by the following data:*

- For each $i \in [n]$, a distinct $a_i \in \mathbb{F}$.
- A positive integer, l .

The generator takes as seed l pairs of scalars $(y_1, z_1), \dots, (y_l, z_l)$ and substitutes

$$x_i \leftarrow \sum_{j=1}^l \left(z_j \cdot \prod_{i' \in [n] \setminus \{i\}} \frac{y_j - a_{i'}}{a_i - a_{i'}} \right).$$

We abbreviate the generator to SV^l or just SV.

Shpilka and Volkovich designed the mapping SV^l so that any selection of l of the variables could remain independent while the others were forced to zero. This can be viewed as an algebraic version of l -wise independence. SV^1 was realized with two seed variables, y and z , using Lagrange interpolation. The fresh variable y enables selecting one of the original variables x_i , namely by setting $y = a_i$. The selected variable x_i is then set to z , while the other variables are set to zero. For larger l , SV^l is the sum of l independent copies of SV^1 .

We now formally state and argue the close relationship between SV^l and RFE_l^{l-1} that we sketched in section 1.

► **Lemma 23.** *Let $\{x_1, \dots, x_n\}$ be a set of variables and $l \geq 1$. There is an invertible diagonal transformation $A : \mathbb{F}^n \rightarrow \mathbb{F}^n$ such that, for any polynomial $p \in \mathbb{F}[x_1, \dots, x_n]$, $p(\text{SV}^l) = 0$ if and only if $(p \circ A)(\text{RFE}_l^{l-1}) = 0$.*

In particular, the vanishing ideals of RFE_l^{l-1} and of SV^l are the same up to the rescaling of Lemma 23.

Proof of Lemma 23. Let $\widehat{\mathbb{F}}$ be the field of rational functions in indeterminates $v_1, \dots, v_l, \zeta_1, \dots, \zeta_l$ over \mathbb{F} . A polynomial $p \in \mathbb{F}[x_1, \dots, x_n]$ has $p(\text{SV}^l) = 0$ if and only if p vanishes at the point

$$\left(\sum_{j=1}^l \zeta_j \prod_{i' \in [n] \setminus \{i\}} \frac{v_j - a_{i'}}{a_i - a_{i'}} : i \in [n] \right) \in \widehat{\mathbb{F}}^n. \quad (19)$$

Set $A : \mathbb{F}^n \rightarrow \mathbb{F}^n$ to be the diagonal linear transformation that divides the coordinate for x_i by $\prod_{i' \in [n] \setminus \{i\}} (a_i - a_{i'})$. It is invertible. Applying A^{-1} to Equation (19) yields the point

$$\left(\sum_{j=1}^l \zeta_j \prod_{i' \in [n] \setminus \{i\}} (v_j - a_{i'}) : i \in [n] \right) = \left(\sum_{j=1}^l \left(\zeta_j \prod_{i' \in [n] \setminus \{i\}} (v_j - a_{i'}) \right) \frac{1}{v_j - a_i} : i \in [n] \right). \quad (20)$$

119:24 Polynomial Identity Testing via Evaluation of Rational Functions

p vanishes at Equation (19) if and only if $p \circ A$ vanishes at Equation (20). Now let $\widehat{\mathbb{F}}'$ be the field of rational functions in indeterminates $\tau_1, \dots, \tau_l, \sigma_1, \dots, \sigma_l$ over \mathbb{F} . After the invertible change of variables

$$\zeta_j \leftarrow \frac{1}{\prod_{i' \in [n]} (\tau_j - a_{i'})} \cdot \frac{-\sigma_j}{\prod_{j' \neq j} (\tau_j - \tau_{j'})} \quad \text{and} \quad v_j \leftarrow \tau_j$$

(20) becomes

$$\left(\sum_{j=1}^l \frac{\sigma_j}{\prod_{j' \neq j} (\tau_j - \tau_{j'})} \frac{1}{a_i - \tau_j} : i \in [n] \right) = \left(\frac{\sum_{j=1}^l \sigma_j \prod_{j' \neq j} \frac{a_i - \tau_{j'}}{\tau_j - \tau_{j'}}}{\prod_{j=1}^l a_i - \tau_j} : i \in [n] \right) \in \widehat{\mathbb{F}}'^m. \quad (21)$$

Since the change of variables is invertible, $p \circ A$ vanishes at Equation (20) if and only if it vanishes at Equation (21).

Now, viewing $\sigma_1, \dots, \sigma_l, \tau_1, \dots, \tau_l$ as seed variables, observe that the right-hand side of Equation (21) is $\text{RFE}_l^{l-1}(g/h)$ where g is parameterized by evaluations $(g(\tau_j) = \sigma_j)$ and h is parameterized by roots (τ_1, \dots, τ_l) . (See Appendix A for a discussion on parameterizations of RFE.) It follows that $p \circ A$ vanishes at Equation (21) if and only if $(p \circ A)(\text{RFE}_l^{l-1}) = 0$. The lemma follows. \blacktriangleleft