Polynomial Identity Testing via Evaluation of Rational Functions

Andrew Morgan
with Dieter van Melkebeek

January, 2022

Polynomial Identity Testing

- Given an arithmetic formula computing $p \in \mathbb{F}[x_1, \ldots, x_n]$, decide whether $p = 0$
- Simple randomized algo: evaluate p at a random point
- Goal: deterministic algo
  - Whitebox: full access to formula
  - Blackbox: only evaluations allowed

Polynomial Identity Testing

Generator

- Fresh seed variables $u_1, \ldots, u_\ell$
- Substitute $x_i \leftarrow \mathrm{G}_i(u_1, \ldots, u_\ell)$, G_i polynomial
- We want $p \neq 0 \implies p(\mathrm{G}) \neq 0$ for all p in a class $\mathcal{C} \subseteq \mathbb{F}[x_1, \ldots, x_n]$

Blackbox Derandomization

- Design a generator with $\ell \ll n$, small $\deg \mathrm{G}_i$
- Test $p(\mathrm{G}) = 0$ using random evaluations of seed variables
- If $\deg(p) = n^{O(1)}$, $\deg(\mathrm{G}_i) = n^{O(1)}$
  then $n^{O(\ell)}$ evaluations suffices

Conceptual Contributions

Use of Rational Functions as Generators

- Substitutions are *rational functions* of the seed
- Rational Function Evaluation generator (RFE)

Systematic Approach via Vanishing Ideal

- $\mathrm{Van}[\mathrm{G}] \doteq$ the set of polynomials such that $p(\mathrm{G}) = 0$
- For any $\mathcal{C} \subseteq \mathbb{F}[x_1, \ldots, x_n]$, G works for $\mathcal{C}$ **iff** $\mathrm{Van}[\mathrm{G}] \cap \mathcal{C} \subseteq \{0\}$
- Derandomization $\Leftrightarrow$ lower bounds for $\mathrm{Van}[\mathrm{G}]$
- Focuses research on the generator rather than syntactic classes, where progress is easier

Technical Contribution #1

Rational Function Evaluation Generator (RFE) $\equiv$
Shpilka–Volkovich Generator (SV)

- $\mathrm{Van}[\mathrm{SV}] = \mathrm{Van}[\mathrm{RFE}]$ up to variable rescaling
- If $\mathcal{C}$ closed under variable rescaling
  then SV works for $\mathcal{C} \iff$ RFE works for $\mathcal{C}$

Technical Contribution #2

Generating Set for Vanishing Ideal of RFE/SV

- Small, explicit
- Gröbner basis

Implications

- Tight bounds for $\mathsf{Van}[\mathsf{RFE}], \mathsf{Van}[\mathsf{SV}]$ for
  - minimum degree
  - minimum sparsity
  - minimum partition class size of set-multi-linearity
- Lower bounds: SV is known to work for some $\mathcal{C}$; the explicit generators cannot be in such $\mathcal{C}$

Technical Contribution #3

Membership Test for Vanishing Ideal of RFE/SV

- For multi-linear p, can be expressed in terms of partial derivatives and zero substitutions

Implications

- Derivatives and zero substitutions are *complete* for reasoning with RFE and SV
- Alternate proof for polynomial-time blackbox derandomization for read-once formulas
- Progress on derandomization for read-once oblivious algebraic branching programs (ROABPs)

Outline

- Define SV and RFE
- Equivalence of RFE and SV
- Generators for vanishing ideal of RFE/SV
- Membership test for vanishing ideal

Shpilka–Volkovich Generator

Parameters

- for each x_i, a distinct *abscissa* $a_i \in \mathbb{F}$

Generator SV^1

- Seed: y, z
- Substitute $x_i \leftarrow z \cdot L_i(y) \doteq z \prod_{j \in [n] \setminus \{i\}} \frac{y - a_j}{a_i - a_j}$

Generator SV^ℓ

- $\mathrm{SV}^\ell \doteq$ sum of ℓ copies of SV^1 with fresh seeds

Properties

- Range includes all points with Hamming weight $\leq \ell$
- ℓ-wise independence

Rational Function Evaluation Generator

Parameters

- For each x_i, a distinct *abscissa* $a_i \in \mathbb{F}$
- k, the *numerator degree*
- ℓ, the *denominator degree*

Generator RFE_ℓ^k

- Seed: univariate rational function $f = g/h \in \mathbb{F}(\alpha)$ with $\deg(g) \leq k$ and $\deg(h) \leq \ell$
- Substitute $x_i \leftarrow f(a_i)$

Example: $k = 1, \ell = 2$

$$f(\alpha) = \frac{c_1\alpha + c_0}{d_2\alpha^2 + d_1\alpha + d_0} \qquad x_i \leftarrow \frac{c_1 a_i + c_0}{d_2 a_i^2 + d_1 a_i + d_0}$$

Equivalence of SV^1 with RFE_1^0

- Starting with $X \leftarrow \mathsf{SV}^1$:

$$x_i \leftarrow z \prod_{j \in [n] \setminus \{i\}} \frac{y - a_j}{a_i - a_j}$$

- Remove denominator by rescaling variables:

$$\tilde{x}_i \leftarrow z \prod_{j \in [n] \setminus \{i\}} (y - a_j) = \underbrace{\left(z \cdot \prod_{j \in [n]} (y - a_j) \right)}_{z'} \cdot \frac{1}{y - a_i}$$

- Reparametrize seed:

$$\tilde{x}_i \leftarrow \frac{z'}{y - a_i} = f(a_i) \quad \text{where } f(\alpha) = \frac{z'}{y - \alpha}$$

Conclusion

- $p(X \leftarrow \mathsf{SV}^1) = 0 \iff p(\tilde{X} \leftarrow \mathsf{RFE}_1^0) = 0$
- $\mathsf{Van}[\mathsf{SV}^1] \equiv \mathsf{Van}[\mathsf{RFE}_1^0]$; i.e., $\mathsf{SV}^1 \equiv \mathsf{RFE}_1^0$

Equivalence of SV with RFE

General ℓ

- $\mathrm{SV}^{\ell} \equiv$ sum of ℓ independent copies of RFE_1^0
- Latter $\equiv \mathrm{RFE}_{\ell}^{\ell-1}$ by partial fraction decomposition

Derandomization

- If $\mathcal{C}$ closed under variable rescaling
  then SV^{ℓ} works for $\mathcal{C} \Leftrightarrow \mathrm{RFE}_{\ell}^{\ell-1}$ works for $\mathcal{C}$
- If RFE_{ℓ}^{k} works for $\mathcal{C}$, then $\mathrm{SV}^{\max(k+1,\ell)}$ works for $\mathcal{C}$

Conclusion
RFE and SV are equivalent in power for derandomization

Some Explicit Polynomials in the Vanishing Ideal of RFE

- Let g/h be a seed to RFE_ℓ^k with $\deg(g) \le k$, $\deg(h) \le \ell$
- $h(a_i)x_i - g(a_i) = 0 \quad$ when $x_i \leftarrow g(a_i)/h(a_i)$
- Write equations in terms of coefficients of g and h:

$$g(\alpha) = \sum_d g_d \alpha^d \quad h(\alpha) = \sum_d h_d \alpha^d$$

$$\begin{bmatrix} a_1^\ell x_1 & a_1^{\ell-1} x_1 & \dots & x_1 & a_1^k & a_1^{k-1} & \dots & 1 \\ a_2^\ell x_2 & a_2^{\ell-1} x_2 & \dots & x_2 & a_2^k & a_2^{k-1} & \dots & 1 \\ \vdots & \vdots & & \vdots & \vdots & \vdots & & \vdots \\ a_n^\ell x_n & a_n^{\ell-1} x_n & \dots & x_n & a_n^k & a_n^{k-1} & \dots & 1 \end{bmatrix} \begin{bmatrix} \vec{h} \\ -\vec{g} \end{bmatrix} = 0$$

- For any choice of $k + \ell + 2$ rows, the determinant vanishes upon substituting RFE_ℓ^k
  - Without the substitution, the determinant is nonzero
  - The determinant is a nonzero element of $\mathrm{Van}[\mathrm{RFE}_\ell^k]$

Elementary Vandermonde Circulation (EVC)

- Select distinct rows $i_1, \ldots, i_{k+\ell+2}$
- $\mathrm{EVC}_\ell^k[i_1, \ldots, i_{k+\ell+2}]$ is the determinant

$$\begin{vmatrix} a_{i_1}^{\ell} x_{i_1} & a_{i_1}^{\ell-1} x_{i_1} & \ldots & x_{i_1} & a_{i_1}^{k} & a_{i_1}^{k-1} & \ldots & 1 \\ a_{i_2}^{\ell} x_{i_2} & a_{i_2}^{\ell-1} x_{i_2} & \ldots & x_{i_2} & a_{i_2}^{k} & a_{i_2}^{k-1} & \ldots & 1 \\ \vdots & \vdots & & \vdots & \vdots & \vdots & & \vdots \\ a_{i_{k+\ell+2}}^{\ell} x_{i_{k+\ell+2}} & a_{i_{k+\ell+2}}^{\ell-1} x_{i_{k+\ell+2}} & \ldots & x_{i_{k+\ell+2}} & a_{i_{k+\ell+2}}^{k} & a_{i_{k+\ell+2}}^{k-1} & \ldots & 1 \end{vmatrix}$$

Elementary Vandermonde Circulation (EVC)

Example

$$\mathrm{EVC}_1^0[1,2,3] \doteq \begin{vmatrix} a_1x_1 & x_1 & 1 \\ a_2x_2 & x_2 & 1 \\ a_3x_3 & x_3 & 1 \end{vmatrix}$$
$$= (a_1 - a_2)x_1x_2 + (a_2 - a_3)x_2x_3 + (a_3 - a_1)x_3x_1$$

Properties

- Homogeneous, degree $\ell + 1$, multi-linear
- All consistent monomials are present

EVCs Generate the Vanishing Ideal of RFE

Theorem
For every $k, \ell \geq 0$*, the instantiations of* $\mathsf{EVC}_\ell^k[i_1, \ldots, i_{k+\ell+2}]$ *generate* $\mathsf{Van}[\mathsf{RFE}_\ell^k]$.

Proof Sketch

- Let $\langle \mathsf{EVC}_\ell^k \rangle$ be ideal generated by instances of EVC_ℓ^k
- We saw that $\langle \mathsf{EVC}_\ell^k \rangle \subseteq \mathsf{Van}[\mathsf{RFE}_\ell^k]$; now show the reverse
- Multivariate polynomial division by instances of EVC_ℓ^k leaves a structured remainder
    - Set C of $k+1$ variables
    - Every monomial in the remainder uses only variables in C and at most ℓ other variables.
- Show directly that RFE_ℓ^k works for every nonzero remainder

Implications

Properties of $\mathrm{Van}[\mathrm{RFE}_\ell^k]$

- Minimum degree is $\ell + 1$
- Minimum sparsity is $\binom{k+\ell+2}{k+1}$
- Minimum set-multi-linear partition class size is $k + 2$ for degree-$(\ell + 1)$

Lower Bounds

- Computational lower bounds for EVC follow from prior derandomization results based on SV

Membership Test for Multi-Linear Polynomials

Let $p \in \mathbb{F}[x_1, \ldots, x_n]$ multi-linear

Theorem
$p \in \mathrm{Van}[\mathrm{RFE}_\ell^k]$ *iff both*

1. *p has no monomials with $\leq \ell$ variables nor $\geq n - k$ variables*
2. *For every way to choose*
   - *k zero substitutions, $K \subseteq \{x_1, \ldots, x_n\}$*
   - *ℓ partial derivatives, $L \subseteq \{x_1, \ldots, x_n\}$*
   - *K, L disjoint*

   the resulting polynomial vanishes at $x_i \leftarrow f_{K,L}(a_i)$ where

$$f_{K,L}(\alpha) \doteq z \cdot \frac{\prod_{i^* \in K}(\alpha - a_{i^*})}{\prod_{i^* \in L}(\alpha - a_{i^*})}$$

   and z is a fresh variable

Sidenote: when $k = \ell = O(1)$, there are $n^{O(1)}$ conditions

Completeness of Derivatives and Zero Substitutions

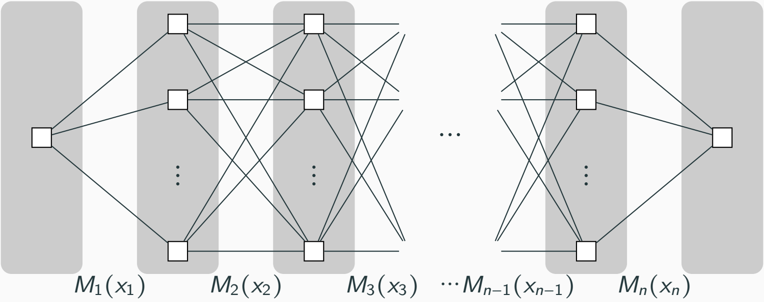
Derivatives and Zero Substitutions Suffice

- Suppose we know that RFE_ℓ^k works for a multi-linear p
  …perhaps through some very difficult proof
- By Membership Test, there is a structured proof of this:
  - p has a monomial with ℓ variables, or
  - p has a monomial with all but k variables, or
  - there are k zero substitutions and ℓ derivatives so that the result is nonzero at $\mathrm{RFE}_\ell^k(f_{K,L})$

Example: Read-Once Formulas

- SV^1 works for ROFs [MV18]
- If $p = p_1 + p_2$, and p_1, p_2 are variable-disjoint,
  then p inherits above obstructions from p_1, p_2

Read-Once Oblivious Algebraic Branching Programs



ROABP

- Product of matrices with univariate polynomials as entries
- Each variable appears in at most one matrix in the product
- Width = largest dimension of a matrix in the product
- Constant-width ROABPs are at the frontier of PIT research

Proof of Concept: Derandomization for ROABPs

Lemma
Every ROABP computing a nonzero $p \in \mathrm{Van}[\mathrm{SV}^{\ell}]$ *with* $\deg(p) = \ell + 1$ *has width at least* $1 + (\ell/3)$.

- Includes $\mathrm{EVC}_{\ell}^{\ell-1}$ and others
- Extends to p with nonzero degree-$(\ell + 1)$ homogeneous part

Theorem
SV^{ℓ} *works for ROABPs of width less than* $1 + (\ell/3)$ *that contain a monomial of degree at most* $\ell + 1$.

- Generalizing lemma to all degrees would imply full derandomization for constant-width ROABPs

Zoom Lemma for Multi-Linear Polynomials

- Prove $p(\mathrm{RFE}_\ell^k) \neq 0$ by "zooming in" on a subset of monoms
- For disjoint $K, L \subseteq [n]$, let $\hat{p} = \left(\frac{\partial p}{\partial L}\right)\Big|_{K \leftarrow 0}$

Lemma
If $\hat{p}$ does not vanish after substituting $x_i \leftarrow f_{K,L}(a_i)$, where

$$f_{K,L}(\alpha) \doteq z \cdot \frac{\prod_{i^* \in K}(\alpha - a_{i^*})}{\prod_{i^* \in L}(\alpha - a_{i^*})}$$

then RFE_ℓ^k *works for p where $k = |K|$ and $\ell = |L|$.*

Proof Sketch

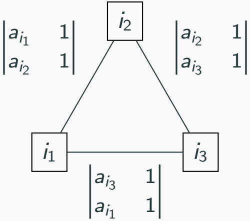
- Parametrize RFE in terms of seed's *roots* and *poles*
- Expand $p(\mathrm{RFE}_\ell^k)$ as Laurent series near roots/poles of $f_{K,L}$
- Degree considerations and the lemma hypothesis imply that one of the coefficients is nonzero

Alternating Algebra Representation

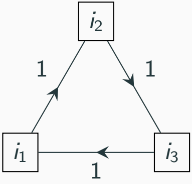
Focus: $k = 0$, $\ell = 1$, degree-2 polynomials

$$\mathrm{EVC}_1^0[i_1, i_2, i_3] = \begin{vmatrix} a_{i_1} & 1 \\ a_{i_2} & 1 \end{vmatrix} x_{i_1} x_{i_2} + \begin{vmatrix} a_{i_3} & 1 \\ a_{i_1} & 1 \end{vmatrix} x_{i_3} x_{i_1} + \begin{vmatrix} a_{i_2} & 1 \\ a_{i_3} & 1 \end{vmatrix} x_{i_2} x_{i_3}$$

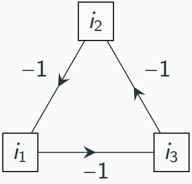
$\cong$



$\cong$

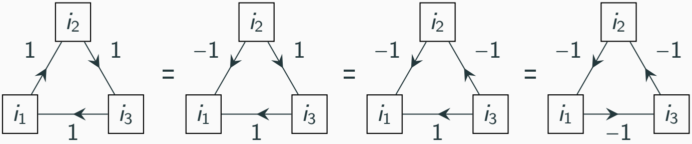


$=$



- Any multi-linear degree-2 polynomial can be represented
- Weight $i \to j$ = the coefficient of $x_i x_j$ divided by $\begin{vmatrix} a_i & 1 \\ a_j & 1 \end{vmatrix}$

Intuition from Network Flow



Elementary Circulations

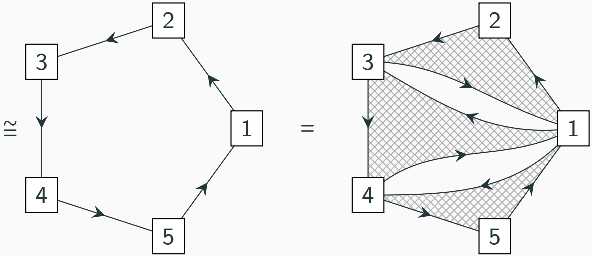
- EVC_1^0: from three vertices, construct elementary circulation
- Closed under linear combinations, EVC_1^0's generate the degree-2 part of $\mathsf{Van}[\mathsf{RFE}_1^0]$
- Elementary circulations similarly generate all circulations
- Degree-2 part of the vanishing ideal $\cong$ circulations

Circulation $\Leftrightarrow$ Conservation of Flow

- Circulations = flow that satisfies conservation
- Membership test: check for conservation of flow

Example

$$
\begin{aligned}
p \doteq\; & (a_1 - a_2)x_1x_2 + (a_2 - a_3)x_2x_3 + (a_3 - a_4)x_3x_4 \\
& + (a_4 - a_5)x_4x_5 + (a_5 - a_1)x_5x_1
\end{aligned}
$$



$$
\cong \mathrm{EVC}_1^0[1,2,3] + \mathrm{EVC}_1^0[1,3,4] + \mathrm{EVC}_1^0[1,4,5]
$$

Summary

Conceptual Contributions

- Use of rational functions as generators
- Systematic approach to derandomization via the vanishing ideal

Technical Contributions

- RFE $\equiv$ SV
- Generating set for vanishing ideal of RFE/SV
- Membership test for vanishing ideal of RFE/SV

Thank you!!

(Back-up Slides)

Completeness of Derivatives and Zero Substitutions

Sum of Variable-Disjoint Polynomials

- Suppose $p = p_1 + p_2$ with p_1 and p_2 variable-disjoint
- If p_j hit by RFE_1^0, either
  1. p_j has a constant term
  2. p_j has a linear term
  3. p_j has the product of all the variables
  4. For some i^*, $\frac{\partial}{\partial x_{i^*}} p_j$ is nonzero at $\mathrm{RFE}_1^0(f_{\emptyset,\{i^*\}})$
- Variable-disjointness implies
  - $p_1 + p_2$ has the union of their nonconstant monomials
  - For each i^*, there is $j \in \{1, 2\}$ so that $\frac{\partial}{\partial x_{i^*}} p = \frac{\partial}{\partial x_{i^*}} p_j$
  - p inherits any of 2–4 from p_1 or p_2
- Let p^*, p_1^*, p_2^* be constant-free p, p_1, p_2
- RFE_1^0 works for p_1^* or $p_2^* \implies \mathrm{RFE}_1^0$ works for p^*

Application: Systematic Derandomization of ROFs [MV18]

Read-Once Formula (ROF)

- formula: $+$, $\times$, variable reads, constants
- each variable read at most **once**

Theorem
Let $F \neq 0$ be ROF. Then $F(\mathrm{SV}^1) \neq 0$.

Proof

- Induction on F: $\quad F^* \neq 0 \implies F^*(\mathrm{SV}^1) \neq 0$
- Base cases: F = read or constant
- $F = F_1 + F_2$: use previous slide
- $F = F_1 \times F_2$:
  - $F^*(\mathrm{SV}^1) \neq 0 \Leftrightarrow F(\mathrm{SV}^1)$ nonconstant
  - $F(\mathrm{SV}^1) = F_1(\mathrm{SV}^1) \times F_2(\mathrm{SV}^1)$
  - (nonconstant poly) $\times$ (nonzero poly) = (nonconstant poly)

Zoom Lemma for General Polynomials

Lemma
If $\hat{p}$ does not vanish after substituting $x_i \leftarrow f_{K,L}(a_i)$, then RFE_ℓ^k works for p where $k = |K|$ and $\ell = |L|$.

Generalization

- Replace $\hat{p} \leftarrow \left(\frac{\partial p}{\partial L}\right)\Big|_{K \leftarrow 0}$ by projection
  - Write p as sum of monomials in $K \cup L$, coeffs in $\mathbb{F}[\overline{K \cup L}]$
  - Pick monomial m^* supported on $K \cup L$
  - $\hat{p} \leftarrow$ coefficient of m^* in the expansion
- Proof requires that for every m in p, either
  - $\deg_{i^*}(m) = \deg_{i^*}(m^*)$ for all $i^* \in K \cup L$
  - $\deg_{i^*}(m) > \deg_{i^*}(m^*)$ for some $i^* \in K$
  - $\deg_{i^*}(m) < \deg_{i^*}(m^*)$ for some $i^* \in L$
- OK if K, L overlap