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 $x_i \leftarrow G_i(u_1, \ldots, u_\ell)$, $G_i$ polynomial
- We want $p \neq 0 \iff p(G) \neq 0$ for all $p$ in a class $C \subseteq \mathbb{F}[x_1, \ldots, x_n]$

**Blackbox Derandomization**
- Design a generator with $\ell \ll n$, small deg $G_i$
- Test $p(G) = 0$ using random evaluations of seed variables
- If $\deg(p) = n^{O(1)}$, $\deg(G_i) = n^{O(1)}$
  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
- $\text{Van}[G] = \{p \in \mathbb{F}[x_1, \ldots, x_n] \mid p(G) = 0\}$
- For any $C \subseteq \mathbb{F}[x_1, \ldots, x_n]$, $G$ works for $C$ iff $\text{Van}[G] \cap C \subseteq \{0\}$
- Derandomization $\iff$ lower bounds for $\text{Van}[G]$
- Focuses research on the generator rather than syntactic classes, where progress is easier
Rational Function Evaluation Generator (RFE) $\equiv$ Shpilka–Volkovich Generator (SV)

- $\text{Van}[SV] = \text{Van}[RFE]$ 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 Van[RFE], Van[SV] for
  • minimum degree
  • minimum sparsity
  • minimum partition class size of set-multi-linearity

• Lower bounds: SV is known to work for some \( C \); the explicit generators cannot be in such \( C \)
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)
• 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 $x_i \leftarrow z \cdot L_i(y) \div z \prod_{j \in [n] \setminus \{i\}} \frac{y - a_j}{a_i - a_j}$

Generator $SV^\ell$

• $SV^\ell \doteq$ sum of $\ell$ copies of $SV^1$ with fresh seeds

Properties

• Range includes all points with Hamming weight $\leq \ell$
• $\ell$-wise independence
Rational Function Evaluation Generator

Parameters

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

Generator $\text{RFE}_\ell^k$

• 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: $k = 1, \ell = 2$

$$f(\alpha) = \frac{c_1 \alpha + c_0}{d_2 \alpha^2 + d_1 \alpha + d_0} \quad \quad x_i \leftarrow \frac{c_1 a_i + c_0}{d_2 a_i^2 + d_1 a_i + d_0}$$
Equivalence of $SV^1$ with $RFE_1^0$

• Starting with $X \leftarrow SV^1$:

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

• Remove denominator by rescaling variables:

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

• Reparametrize seed:

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

Conclusion

• $p(X \leftarrow SV^1) = 0 \iff p(\tilde{X} \leftarrow RFE_1^0) = 0$

• $\text{Van}[SV^1] \equiv \text{Van}[RFE_1^0]$; i.e., $SV^1 \equiv RFE_1^0$
Equivalence of SV with RFE

General $\ell$

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

Derandomization

- If $C$ closed under variable rescaling
  then $SV^\ell$ works for $C \iff RFE_{\ell-1}^\ell$ works for $C$
- If $RFE_{\ell}^k$ works for $C$, then $SV^{\max(k+1,\ell)}$ works for $C$

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 $\text{RFE}_k^\ell$ with $\deg(g) \leq k$, $\deg(h) \leq \ell$
• $h(a_i)x_i - g(a_i) = 0$ when $x_i \leftarrow g(a_i)/h(a_i)$
• Write equations in terms of coefficients of $g$ and $h$:

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

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

• For any choice of $k + \ell + 2$ rows, the determinant vanishes upon substituting $\text{RFE}_k^\ell$
  • Without the substitution, the determinant is nonzero
  • The determinant is a nonzero element of $\text{Van}[\text{RFE}_k^\ell]$
**Elementary Vandermonde Circulation (EVC)**

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

$$
\begin{vmatrix}
 a_{i_1}^\ell x_{i_1} & a_{i_1}^{\ell-1} x_{i_1} & \ldots & x_{i_1} & a_{i_1}^k & a_{i_1}^{k-1} & \ldots & 1 \\
 a_{i_2}^\ell x_{i_2} & a_{i_2}^{\ell-1} x_{i_2} & \ldots & x_{i_2} & a_{i_2}^k & a_{i_2}^{k-1} & \ldots & 1 \\
 \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\
 a_{i_{k+\ell+2}}^\ell x_{i_{k+\ell+2}} & a_{i_{k+\ell+2}}^{\ell-1} x_{i_{k+\ell+2}} & \ldots & x_{i_{k+\ell+2}} & a_{i_{k+\ell+2}}^k & a_{i_{k+\ell+2}}^{k-1} & \ldots & 1 
\end{vmatrix}
$$
**Elementary Vandermonde Circulation (EVC)**

**Example**

\[
EVC_1^0[1, 2, 3] = \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 $EVC_{k}^{\ell}[i_1, \ldots, i_{k+\ell+2}]$ generate $\text{Van}[RFE_{\ell}^{k}]$.

**Proof Sketch**

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

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

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

**Theorem**

$p \in \text{Van}[\text{RFE}_k^\ell]$ 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, $K \subseteq \{x_1, \ldots, x_n\}$
   - $\ell$ 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 $\text{RFE}_k^\ell$ 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 $\ell$ variables, or
  - $p$ has a monomial with all but $k$ variables, or
  - there are $k$ zero substitutions and $\ell$ derivatives so that the result is nonzero at $\text{RFE}_k^\ell(f_{K,L})$

Example: Read-Once Formulas

- $\text{SV}^1$ 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 \( p \in \text{Van}[SV^\ell] \) with \( \deg(p) = \ell + 1 \) has width at least \( 1 + (\ell/3) \).

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

**Theorem**
\( SV^\ell \) 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 $p(RFE_\ell^k) \neq 0$ by “zooming in” on a subset of monoms
• For disjoint $K, L \subseteq [n]$, let $\hat{p} = \left( \frac{\partial p}{\partial L} \right)_{K \leftarrow 0}$

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

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

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

Proof Sketch
• Parametrize RFE in terms of seed’s roots and poles
• Expand $p(RFE_\ell^k)$ 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

\[
EVC_1^0[i_1, i_2, i_3] = \begin{vmatrix} a_{i_1} & 1 \\ a_{i_2} & 1 \end{vmatrix} x_{i_1} x_{i_2} + \begin{vmatrix} a_{i_3} & 1 \\ a_{i_1} & 1 \end{vmatrix} x_{i_3} x_{i_1} + \begin{vmatrix} a_{i_2} & 1 \\ a_{i_3} & 1 \end{vmatrix} x_{i_2} x_{i_3}
\]

- 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**

\[ i_1 \quad 1 \quad i_3 \]

\[ i_2 \quad 1 \quad i_3 \]

\[ i_1 \quad 1 \quad i_3 \]

\[ i_2 \quad 1 \quad i_3 \]

Elementary Circulations

- \( \text{EVC}_1^0 \): from three vertices, construct elementary circulation
- Closed under linear combinations, \( \text{EVC}_1^0 \)'s generate the degree-2 part of \( \text{Van}[\text{RFE}_1^0] \)
- 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

\[ p \doteq (a_1 - a_2)x_1x_2 + (a_2 - a_3)x_2x_3 + (a_3 - a_4)x_3x_4 + (a_4 - a_5)x_4x_5 + (a_5 - a_1)x_5x_1 \]

\[ \cong \quad EVC_1^0[1, 2, 3] + EVC_1^0[1, 3, 4] + EVC_1^0[1, 4, 5] \]
Conceptual Contributions

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

Technical Contributions

• RFE ≡ 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 $\text{RFE}^0_1$, 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 $\text{RFE}^0_1(f_\emptyset, \{i^*\})$

- 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 $p$, $p_1$, $p_2$
- $\text{RFE}^0_1$ works for $p_1^*$ or $p_2^*$ $\implies$ $\text{RFE}^0_1$ works for $p^*$
Read-Once Formula (ROF)

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

Theorem

Let $F \neq 0$ be ROF. Then $F(SV^1) \neq 0$.

Proof

- Induction on $F$: $F^* \neq 0 \implies F^*(SV^1) \neq 0$
- Base cases: $F =$ read or constant
- $F = F_1 + F_2$: use previous slide
- $F = F_1 \times F_2$:
  - $F^*(SV^1) \neq 0 \iff F(SV^1)$ nonconstant
  - $F(SV^1) = F_1(SV^1) \times F_2(SV^1)$
  - (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 \( \text{RFE}_k^l \) works for \( p \) where \( k = |K| \) and \( l = |L| \).

Generalization

- Replace \( \hat{p} \leftarrow \left( \frac{\partial p}{\partial L} \right)|_{K \leftarrow 0} \) by projection
  - Write \( p \) as sum of monomials in \( K \cup L \), coeffs in \( \mathbb{F}[K \cup L] \)
  - 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