Limitations of the Shpilka-Volkovich Generator

Arpita Korwar
joint work with Hervé Fournier

Université Denis Diderot - Paris 7

March 16, 2018
1. Polynomial Identity Testing

2. Shpilka-Volkovich (SV) Generator

3. Finding the Annihilating polynomial
Section 1

Polynomial Identity Testing
Polynomial Identity Testing (PIT)

PIT: Is a given input polynomial identically zero?
**Input model: Arithmetic circuits**

- A natural and succinct representation of a polynomial.
PIT can be classified according to how the polynomial is given to the algorithm.
PIT can be classified according to how the polynomial is \textit{given} to the algorithm.

- \(\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_h\)
- \(P \in \mathcal{P}\)
- \(P(a_1), P(a_2), \ldots, P(a_h)\)
- \(\mathbf{a}_i = (a_{i1}, a_{i2}, \ldots, a_{in})\).
PIT can be classified according to how the polynomial is given to the algorithm.

- \( a_1, a_2, \ldots, a_h \)
- \( P \subseteq \mathcal{P} \)
- \( P(a_1), P(a_2), \ldots, P(a_h) \)

- \( a_i = (a_{i1}, a_{i2}, \ldots, a_{in}) \).

Example: PIT for univariate polynomials of degree bounded by \( d \).
Blackbox test (a.k.a. Hitting set)

- PIT can be classified according to how the polynomial is given to the algorithm.

- $a_1, a_2, \ldots, a_h \rightarrow P \in \mathcal{P}$

- $P(a_1), P(a_2), \ldots, P(a_h)$

- $a_i = (a_{i1}, a_{i2}, \ldots, a_{in})$.

- Example: PIT for univariate polynomials of degree bounded by $d$.

- For $n$-variate $\mathcal{P}$, a small-degree univariate substitution is enough.
Hitting set generator

- For a family $\mathcal{P}$ of $n$-variate, a polynomial map to $k$-variate polynomials $(f_1(y), f_2(y), \ldots, f_n(y))$ is a hitting set generator if for all polynomials $P(x_1, x_2, \ldots, x_n) \neq 0 \in \mathcal{P}$, $P(f_1(y), f_2(y), \ldots, f_n(y)) \neq 0$.
- Final time complexity $= (\delta d + 1)^k$, where $d$ is the degree of $f_i$s and the polys in $\mathcal{P}$ are of degree $\delta$.
- Poly when $k$ is constant. Quasipoly when $k$ is $\log n$. 
Section 2

Shpilka-Volkovich (SV) Generator
Applications of the SV generator

- $s^{O(1)}$-size hitting set for Read-once formulas [Shpilka and Volkovich, 2009, Minahan and Volkovich, 2016].
- $s^{O(1)}$-size hitting set for Constant-read multilinear formulas [Anderson et al., 2015].
- $s^{O(\log \log s)}$-size hitting set for Commutative Read-once ABPs [Forbes et al., 2014].
Building blocks of the SV generator.

Choose \((a_1, a_2, \ldots, a_n)\) such that all \(a_i\)'s are unique.

\[ L_r(y) := \prod_{j \neq r} \frac{(y-a_j)}{(a_r-a_j)}. \]

\[ L_r(b) = \begin{cases} 
1 & \text{if } b = a_r, \\
0 & \text{if } b \in \{a_1, a_2, \ldots, a_n\}, \ b \neq a_r.
\end{cases} \]
Shpilka-Volkovich (SV) Generator

Shpilka-Volkovich map
\((SV_{n,k})\) [Shpilka and Volkovich, 2009]

- \(SV_{n,1}(y, z) : \mathbb{F}[x] \rightarrow \mathbb{F}[y, z]\), given by \(SV_{n,1}(y, z) : x_r \mapsto zL_r(y)\).
- \(SV_{n,1}\) is a bivariate map.
- \(SV_{n,k}(y_1, z_1, y_2, z_2, \ldots, y_k, z_k) : \mathbb{F}[x] \rightarrow \mathbb{F}[y, z]\), given by
  \(SV_{n,k}(y, z) : x_r \mapsto \sum_{i=1}^{k} z_i L_r(y_i)\).
- \(SV_{n,k}\) is a \(2k\)-variate map.
Some properties

- $\text{SV}_{n,k}$ of each $x_i$ is a linear form\(^1\) in $z$.
- $\text{SV}_{n,k}$ is a hitting set generator for $2^k$-sparse polynomials.
- $\text{SV}_{n,k}$ is a hitting set generator for degree-$k$ polynomials.

\(^1\text{constant part of the linear polynomial is 0}\)
**Question**

- We want $f$ such that $\text{SV}_{n,k}(f) = 0$.
- What is the smallest degree polynomial that evaluates to 0 at $\text{SV}_{n,k}$?
- Conjecture: There exists a degree $k + 1$ multilinear polynomial on $n = 2k + 1$ variables that maps to 0 on applying $\text{SV}_{n,k}$.
- I.e. A multilinear, degree $k + 1$ annihilating polynomial for $\text{SV}_{n,k}$ exists.
Section 3

**Finding the Annihilating polynomial**
Finding the Annihilating polynomial

**Finding a small annihilating polynomial - homogeneity**

- Let

\[
  f(x_1, x_2, \ldots, x_n) = \sum_{S: |S| \leq k+1} \gamma_S \prod_{r \in S} x_r.
\]

- Recall that \( SV_{n,k}(y, z) : x_r \mapsto \sum_{i=1}^{k} z_i L_r(y_i) \).

- The polynomial \( SV_{n,k}(f) \) can be seen as a polynomial in \( F[y][z] \).

- After the map is applied, the \( z \)-degree of a degree-\( d \) monomial is \( d \).

- So, without loss of generality, \( f \) is homogeneous.

\[
  f(x_1, x_2, \ldots, x_n) = \sum_{S: |S|=k+1} \gamma_S \prod_{r \in S} x_r.
\]
Coefficients of each monomials

- The coefficient of any such monomial after the map should be 0.
- This gives a set of linear constraints on $\gamma S$.
After cleaning the conditions on the coefficients, our problem reduces to finding $(\alpha_R)_{R:|R|=k}$ such that the following linear constraints are satisfied:

$$\forall S \subseteq [n], |S| = k - 1 : \sum_{R:|R|=k, S \subseteq R} \alpha_R = 0$$

and

$$\sum_{R:|R|=k, S \subseteq R} a_{R \setminus S} \cdot \alpha_R = 0.$$ 

E.g. when $k = 1$, $n = 2k + 1 = 3$. Then, we want to find $(\alpha_1, \alpha_2, \alpha_3)$ such that $\sum \alpha_i = 0$ and $\sum a_i \cdot \alpha_i = 0$. 
The \((\alpha_R)_R\)s that satisfy the first set of constraints are nullvectors of the *inclusion matrix* \(M\) with the rows indexed by \(\{S : |S| = k - 1\}\) and the columns indexed by \(\{R : |R| = k\}\) with

\[
M_{S,R} = \begin{cases} 
1 \text{ if } S \subseteq R, \\
0 \text{ otherwise.}
\end{cases}
\]

The \((\alpha_R)_R\)s that satisfy the second set of constraints are null vectors of \(N\), where

\[
N_{S,R} = \begin{cases} 
a_{R \setminus S} \text{ if } S \subseteq R, \\
0 \text{ otherwise.}
\end{cases}
\]

When \(k = 1, n = 2k + 1 = 3\),

\[
M = \begin{bmatrix} 1 & 1 & 1 \end{bmatrix}
\]

and

\[
N = \begin{bmatrix} a_1 & a_2 & a_3 \end{bmatrix}.
\]
\[ N = D' MD, \text{ where} \]

- \( D' \) is a \( \binom{n}{k-1} \) diagonal matrix. \( D'_{S,S} = \prod_{i \in S} 1/a_i = 1/a_S. \)
- \( D \) is a \( \binom{n}{k} \) diagonal matrix. \( D_{R,R} = \prod_{i \in R} a_i = a_R. \)

- \( D' \) does not affect the nullvector of \( N. \)

- Hence, we need to show that
  \[ \mathcal{N}(M) \cap \mathcal{N}(MD) \neq \emptyset. \]

- \( \mathcal{N}(M) \) has dimension \( \binom{n}{k} - \binom{n}{k-1} \) and has been described by [Graham et al., 1980] and others.
Some notation [Graham et al., 1980]:

- View the nullvector as a multilinear homogeneous polynomial of degree $k$.
- Take $n$ variables $\{x_1, x_2, \ldots, x_n\}$. With a vector $(\alpha_R)_R$, associate $\sum_R \alpha_R x_R$.
- Define
  $$ g(x_1, x_2, \ldots, x_n) = (x_1 - x_2)(x_3 - x_4) \cdots (x_{2k-1} - x_{2k}) $$

Lemma [Graham et al., 1980]

$$ \mathcal{N}(M) = \text{span} \{ g^\sigma | \sigma \in S_n \} $$

where, $h^\sigma(x_1, x_2, \ldots, x_n) = h(x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(n)})$.

Thus, $\mathcal{N}([1 \ 1 \ 1]) = \text{span} \{ x_1 - x_2, x_1 - x_3, x_3 - x_2, \ldots \}$. 
Finding the Annihilating polynomial

1. \( Mv = MDD^{-1}v \).
2. Thus, \( \mathcal{N}(MD) = \text{span}\{\psi(g^\sigma)|\sigma \in S_n\} \), where \( \psi : x_i \mapsto \frac{1}{a_i}x_i \).
3. Let \( b_i = \frac{1}{a_i} \).
4. Thus, \( \mathcal{N}([a_1 \quad a_2 \quad a_3]) = \text{span}\{b_1x_1 - b_2x_2, b_1x_1 - b_3x_3, b_3x_3 - b_2x_2, \ldots\} \).
Conjecture: \( \dim(\mathcal{N}(M) \cap \mathcal{N}(MD)) = 1. \)

When \( k = 1, n = 3 \), this common nullvector is

\[
a_1 a_2 (x_1 - x_2) + a_2 a_3 (x_2 - x_3) + a_3 a_1 (x_3 - x_1)
= -a_3 (a_1 x_1 - a_2 x_2) - a_1 (a_2 x_2 - a_3 x_3) - a_2 (a_3 x_3 - a_1 x_1).
\]
Thank you


*SIAM. J. on Algebraic and Discrete Methods*, 1:8–14.


*Electronic Colloquium on Computational Complexity (ECCC)*, 23:171.