Identity Testing for constant-width, and commutative, ROABPs

Rohit Gurjar*, Arpita Korwar, Nitin Saxena†
Aalen University and IIT Kanpur

June 1, 2016

* supported by TCS research fellowship
† supported by DST-SERB
Polynomial Identity Testing

- PIT: given a polynomial $P(x) \in \mathbb{F}[x_1, x_2, \ldots, x_n]$, $P(x) = 0$?
Polynomial Identity Testing

- PIT: given a polynomial $P(x) \in \mathbb{F}[x_1, x_2, \ldots, x_n]$, $P(x) = 0$?
- Input Models:
  - Arithmetic Circuits
  - Arithmetic Branching Programs

![Arithmetic circuit](image)

**Figure**: An Arithmetic circuit
Randomized Test

- Rephrasing the question: Given an arithmetic circuit decide if it computes the zero polynomial.
- Randomized PIT: evaluate $P(x)$ at a random point [Demillo and Lipton, 1978, Zippel, 1979, Schwartz, 1980].
Randomized Test

- Rephrasing the question: Given an arithmetic circuit decide if it computes the zero polynomial.
- Randomized PIT: evaluate $P(x)$ at a random point [Demillo and Lipton, 1978, Zippel, 1979, Schwartz, 1980].
- There is no efficient deterministic test known.
Randomized Test

- Rephrasing the question: Given an arithmetic circuit decide if it computes the zero polynomial.
- Randomized PIT: evaluate $P(x)$ at a random point [Demillo and Lipton, 1978, Zippel, 1979, Schwartz, 1980].
- There is no efficient deterministic test known.
- Two Paradigms:
  - Whitebox: one can see the input circuit.
  - Blackbox: circuit is hidden, only evaluations are allowed (hitting-sets).
**Randomized Test**

- Rephrasing the question: Given an arithmetic circuit decide if it computes the zero polynomial.
- Randomized PIT: evaluate $P(x)$ at a random point [Demillo and Lipton, 1978, Zippel, 1979, Schwartz, 1980].
- There is no efficient deterministic test known.
- Two Paradigms:
  - Whitebox: one can see the input circuit.
  - Blackbox: circuit is hidden, only evaluations are allowed (hitting-sets).
- Derandomizing PIT has connections with circuit lower bounds [Kabanets and Impagliazzo, 2003, Agrawal, 2005].
Randomized Test

- Rephrasing the question: Given an arithmetic circuit decide if it computes the zero polynomial.
- Randomized PIT: evaluate $P(x)$ at a random point [Demillo and Lipton, 1978, Zippel, 1979, Schwartz, 1980].
- There is no efficient deterministic test known.
- Two Paradigms:
  - Whitebox: one can see the input circuit.
  - Blackbox: circuit is hidden, only evaluations are allowed (hitting-sets).
- Derandomizing PIT has connections with circuit lower bounds [Kabanets and Impagliazzo, 2003, Agrawal, 2005].
- An efficient test is known only for restricted classes of circuits, e.g., Sparse polynomials, set-multilinear circuits, ROABP.
Arithmetic Branching Programs

**Figure**: An Arithmetic branching program.

- **ABP**: a directed acyclic graph $G$ with a start node and an end node.
- Each edge has a weight from $\mathbb{F}[x]$. 
**Arithmetic Branching Programs**

**Figure**: An Arithmetic branching program.

- ABP: a directed acyclic graph $G$ with a start node and an end node.
- Each edge has a weight from $\mathbb{F}[x]$.

$$C(x) = \sum_{p \in \text{paths}(s,t)} W(p), \text{ where } W(p) = \prod_{e \in p} W(e).$$
**Arithmetic Branching Programs**

**Figure:** An Arithmetic branching program.

- **ABP:** A directed acyclic graph $G$ with a start node and an end node.
- Each edge has a weight from $\mathbb{F}[x]$.

\[
C(x) = \sum_{p \in \text{paths}(s,t)} W(p), \quad \text{where } W(p) = \prod_{e \in p} W(e).
\]

- $C(x) = (x_1 + 2x_4)x_2x_1 - (x_1 + 2x_4)x_2 + (x_1 + x_2)5x_2$
**Preliminaries**

**Arithmetic Branching Programs**

**Figure**: An Arithmetic branching program.

- **ABP**: a directed acyclic graph $G$ with a start node and an end node.
- Each edge has a weight from $\mathbb{F}[x]$.

Let $C(x) = \sum_{p \in \text{paths}(s, t)} W(p)$, where $W(p) = \prod_{e \in p} W(e)$.

- $C(x) = (x_1 + 2x_4)x_2x_1 - (x_1 + 2x_4)x_2 + (x_1 + x_2)5x_2$
- **Width**: maximum number of nodes in a layer.
Arithmetic Branching Programs

Figure: An Arithmetic branching program.

- Equivalent representation:

\[
\begin{bmatrix}
  x_1 + 2x_4 & x_1 + x_2
\end{bmatrix}
\begin{bmatrix}
  x_2 & -1 \\
  0 & 5
\end{bmatrix}
\begin{bmatrix}
  x_1 \\
  x_2
\end{bmatrix}
\]

- \( C(x) = (x_1 + 2x_4)x_2x_1 - (x_1 + 2x_4)x_2 + (x_1 + x_2)5x_2 \)

- Width: maximum dimension of the matrices.
Almost as powerful as arithmetic circuits
[Valiant, 1979, Berkowitz, 1984].
**Power of ABPs**

- Almost as powerful as arithmetic circuits [Valiant, 1979, Berkowitz, 1984].
- Width-3 ABPs have the same expressive power as arithmetic formulas [Ben-Or and Cleve, 1992].
Power of ABPs

- Almost as powerful as arithmetic circuits [Valiant, 1979, Berkowitz, 1984].
- Width-3 ABPs have the same expressive power as arithmetic formulas [Ben-Or and Cleve, 1992].
- Deterministic PIT: only for special ABPs, e.g. read-once oblivious ABP.
Read-once Oblivious ABP

- Any variable occurs in at most one layer.

**Figure**: A Read-once oblivious ABP with variable order \((x_1, x_3, x_2, x_4)\)
[Raz and Shpilka, 2005] gave a polynomial time whitebox test for ROABP.
[Raz and Shpilka, 2005] gave a polynomial time whitebox test for ROABP.

Blackbox test: $n^{O(\log n)}$ time

[Forbes and Shpilka, 2013, Forbes et al., 2014, Agrawal et al., 2015].
[

[Raz and Shpilka, 2005] gave a polynomial time whitebox test for ROABP.

[Forbes and Shpilka, 2013, Forbes et al., 2014, Agrawal et al., 2015].

Blackbox test: $n^{O(\log n)}$ time

Nothing better known even for constant width.
Polynomial time blackbox test for constant width ROABPs*.

Commutative ROABP: where matrices commute (no variable order).

\[ d \cdot O(\log w) (nw) \cdot O(\log \log w) \text{-time blackbox test} \]  
Forbes et al., 2014

We improve it to \((dnw) \cdot O(\log \log w)\)-time.
Our Results

1. Polynomial time blackbox test for constant width ROABPs*.
   * known variable order.
   * zero characteristic field (or large enough).
Our Results

1. Polynomial time blackbox test for constant width ROABPs*.
   * known variable order.
   * zero characteristic field (or large enough).

2. Commutative ROABP: where matrices commute (no variable order).
Our Results

1. Polynomial time blackbox test for constant width ROABPs*.
   * known variable order.
   * zero characteristic field (or large enough).

2. Commutative ROABP: where matrices commute (no variable order).
   \[ d^{O(\log w)} (nw)^{O(\log \log w)} \] - time blackbox test [Forbes et al., 2014]
   - for \( n \) variables, width \( w \) and individual degree \( d \).
# Our Results

1. Polynomial time blackbox test for **constant width** ROABPs*.
   * known variable order.
   * zero characteristic field (or large enough).

2. Commutative ROABP: where matrices commute (**no variable order**).
   
   $d^{O(\log w)}(nw)^{O(\log \log w)}$-time blackbox test [Forbes et al., 2014]
   
   – for $n$ variables, width $w$ and individual degree $d$.

   We improve it to $(dnw)^{O(\log \log w)}$-time.
Figure: An ROBP
Pseudorandomness for ROBP

- Comes from the RL versus L question.
Pseudorandomness for ROBP

- Comes from the RL versus L question.
- A distribution is pseudorandom if any ROBP cannot distinguish it from the uniform random distribution.
Pseudorandomness for ROBP

- Comes from the RL versus L question.
- A distribution is pseudorandom if any ROBP cannot distinguish it from the uniform random distribution.
- Goal: construct a PRG with $O(\log n)$ seed length (polynomial size sample space).
Pseudorandomness for ROBP

- Comes from the RL versus L question.
- A distribution is pseudorandom if any ROBP cannot distinguish it from the uniform random distribution.
- Goal: construct a PRG with $O(\log n)$ seed length (polynomial size sample space).
- Best known result: $O(\log^2 n)$ seed length [Nisan, 1990, Impagliazzo et al., 1994, Raz and Reingold, 1999].
Pseudorandomness for ROBP

- Comes from the RL versus L question.
- A distribution is pseudorandom if any ROBP cannot distinguish it from the uniform random distribution.
- Goal: construct a PRG with $O(\log n)$ seed length (polynomial size sample space).
- Best known result: $O(\log^2 n)$ seed length [Nisan, 1990, Impagliazzo et al., 1994, Raz and Reingold, 1999].
- Nothing better known even for constant width.
Read-once Ordered Branching Programs

IMPAGLIAZZO ET AL., 1994

$r$ bits

$r + O(\log w)$ bits

Sample space size: poly($w$) × 2$r$ instead of trivial 2$r$ × 2$r$.

Gurjar, Korwar, Saxena

PIT for constant-width ROABPs

June 1, 2016 12 / 26
Sample space size: \( \text{poly}(w) \times 2^r \) instead of trivial \( 2^r \times 2^r \).
Hitting-set for Bivariate ROABP

\[ f(x_1, x_2) = \sum_{r=1}^{w} g_r(x_1) h_r(x_2) \]
Hitting-set for Bivariate ROABP

Claim: \( f(t^w, t^w + t^w - 1) \neq 0 \).

Degree = \( 2w \), where \( \deg(g_r) = d \), \( \deg(h_r) = d \).

Hitting-set size: \( 2w + 1 \), instead of trivial \( (d + 1)^2 \).
**Claim**: $f(t^w, t^w + t^{w-1}) \neq 0.$
Hitting-set for Bivariate ROABP

Claim: \( f(t^w, t^w + t^{w-1}) \neq 0 \).

Degree = 2wd, where \( \deg(g_r), \deg(h_r) = d \).
Hitting-set for Bivariate ROABP

\[ f(x_1, x_2) = \sum_{r=1}^{w} g_r(x_1) h_r(x_2) \]

**Claim:** \( f(t^w, t^w + t^{w-1}) \neq 0. \)

Degree = \( 2wd \), where \( \deg(g_r), \deg(h_r) = d \).

Hitting-set size: \( 2wd + 1 \), instead of trivial \( (d + 1) \times (d + 1) \).
**n-Variate ROABP**

\[
f = \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ \vdots \\ x_{n-1} \\ x_n \end{bmatrix}
\]

Claim:

\[f(tw_1, tw_1 + tw_{-1}, x_3, x_4, \ldots, x_n) \neq 0.\]

Proof: treat \(x_3, x_4, \ldots, x_n\) as constants.
$n$-VARIATE ROABP

\[ f = \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ \cdots \\ x_{n-1} \\ x_n \end{bmatrix} \]

\textbf{Claim:} \( f(t^w_1, t^w_1 + t^w_1 - 1, x_3, x_4, \ldots, x_n) \neq 0 \).
Claim: $f(t^w_1, t^w_1 + t^w_1 - 1, x_3, x_4, \ldots, x_n) \neq 0$.

Proof: treat $x_3, x_4, \ldots, x_n$ as constants.
**n-variate ROABP**

\[ f = \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ \cdots \\ x_{n-1} \\ x_n \end{bmatrix} \]

- **Claim:** \( f(t^w_1, t^w_1 + t^w_{1-1}, x_3, x_4, \ldots, x_n) \neq 0 \).
- **Proof:** treat \( x_3, x_4, \ldots, x_n \) as constants.

\[ f = \sum_{r=1}^{w} g_r(x_1) \cdot h_r(x_2, x_3, \ldots, x_n) \]
\( n \)-variate ROABP

\[
\begin{bmatrix}
  x_1 \\
  x_2 \\
  x_3 \\
  \vdots \\
  x_{n-1} \\
  x_n
\end{bmatrix}
\]

Claim: \( f(t^w_1, t^w_1 + t^{w-1}_1, x_3, x_4, \ldots, x_n) \neq 0 \).

Proof: treat \( x_3, x_4, \ldots, x_n \) as constants.

\[
f = \sum_{r=1}^{w} g_r(x_1) \ h_r(x_2, x_3, \ldots, x_n)
\]

\( f(t^w_1, t^w_1 + t^{w-1}_1) \neq 0 \) (bivariate ROABP).
$n$-VARIATE ROABP

- $f(t_1^w, t_1^w + t_1^{w-1}, x_3, x_4, \ldots, x_n) \neq 0$. 
\( n \)-VARIATE ROABP

- \( f(t^w_1, t^w_1 + t^{w-1}_1, x_3, x_4, \ldots, x_n) \neq 0. \)
- \( f(t^w_1, t^w_1 + t^{w-1}_1, t^w_2, t^w_2 + t^{w-1}_2, \ldots, x_n) \neq 0. \)
**n-variate ROABP**

- $f(t_1^w, t_1^w + t_1^{w-1}, x_3, x_4, \ldots, x_n) \neq 0$.
- $f(t_1^w, t_1^w + t_1^{w-1}, t_2^w, t_2^w + t_2^{w-1}, \ldots, x_n) \neq 0$.
- $f(t_1^w, t_1^w + t_1^{w-1}, t_2^w, t_2^w + t_2^{w-1}, \ldots, t_{n/2}^w, t_{n/2}^w + t_{n/2}^{w-1}) \neq 0$. 

**Known variable order.**

Gurjar, Korwar, Saxena

**PIT for constant-width ROABPs**

June 1, 2016 16 / 26
**n-variate ROABP**

- \( f(t_1^w, t_1^w + t_1^{w-1}, x_3, x_4, \ldots, x_n) \neq 0. \)
- \( f(t_1^w, t_1^w + t_1^{w-1}, t_2^w, t_2^w + t_2^{w-1}, \ldots, x_n) \neq 0. \)
- \( f(t_1^w, t_1^w + t_1^{w-1}, t_2^w, t_2^w + t_2^{w-1}, \ldots, t_{n/2}^w, t_{n/2}^w + t_{n/2}^{w-1}) \neq 0. \)

\[
f' = \begin{bmatrix} t_1 \\ \end{bmatrix} \begin{bmatrix} \vdots \\ t_1 \\ \vdots \\ \end{bmatrix} \begin{bmatrix} \vdots \\ t_2 \\ \vdots \\ \end{bmatrix} \cdots \begin{bmatrix} \vdots \\ t_{n/2} \\ \vdots \\ \end{bmatrix} \begin{bmatrix} \vdots \\ t_{n/2} \\ \vdots \\ \end{bmatrix}
\]
**n-variate ROABP**

- \( f(t_1^w, t_1^w + t_1^{w-1}, x_3, x_4, \ldots, x_n) \neq 0. \)
- \( f(t_1^w, t_1^w + t_1^{w-1}, t_2^w, t_2^w + t_2^{w-1}, \ldots, x_n) \neq 0. \)
- \( f(t_1^w, t_1^w + t_1^{w-1}, t_2^w, t_2^w + t_2^{w-1}, \ldots, t_{n/2}^w, t_{n/2}^w + t_{n/2}^{w-1}) \neq 0. \)

\[
f' = \begin{bmatrix} t_1 \\ t_2 \\ \vdots \\ t_{n/2} \end{bmatrix}
\]
\textbf{\textit{n}-variate ROABP}

- \( f(t_1^w, t_1^w + t_1^{w-1}, x_3, x_4, \ldots, x_n) \neq 0. \)
- \( f(t_1^w, t_1^w + t_1^{w-1}, t_2^w, t_2^w + t_2^{w-1}, \ldots, x_n) \neq 0. \)
- \( f(t_1^w, t_1^w + t_1^{w-1}, t_2^w, t_2^w + t_2^{w-1}, \ldots, t_{n/2}^w, t_{n/2}^w + t_{n/2}^{w-1}) \neq 0. \)

\[
f' = \begin{bmatrix} t_1 \\ t_2 \\ \vdots \\ t_{n/2} \end{bmatrix}
\]

- no. of variables = \( n \rightarrow n/2 \), individual degree = \( d \rightarrow 2wd \).
**n-vanriate ROABP**

- $f(t_1^w, t_1^w + t_1^{w-1}, x_3, x_4, \ldots, x_n) \neq 0$.
- $f(t_1^w, t_1^w + t_1^{w-1}, t_2^w, t_2^w + t_2^{w-1}, \ldots, x_n) \neq 0$.
- $f(t_1^w, t_1^w + t_1^{w-1}, t_2^w, t_2^w + t_2^{w-1}, \ldots, t_{n/2}^w, t_{n/2}^w + t_{n/2}^{w-1}) \neq 0$.

$$f' = \begin{bmatrix} t_1 \\ t_2 \\ \vdots \\ t_{n/2} \end{bmatrix}$$

- no. of variables $= n \rightarrow n/2$, individual degree $= d \rightarrow 2wd$.
- Repeat log $n$ times. 1 variable, individual degree $= (2w)^{\log n}d$. 

Hitting-set size: $O(ndw \log n)$. 
Hitting-set size: poly($n, d$), if $w$ is constant.
$n$-variate ROABP

- $f(t_1^w, t_1^w + t_1^{w-1}, x_3, x_4, \ldots, x_n) \neq 0$.
- $f(t_1^w, t_1^w + t_1^{w-1}, t_2^w, t_2^w + t_2^{w-1}, \ldots, x_n) \neq 0$.
- $f(t_1^w, t_1^w + t_1^{w-1}, t_2^w, t_2^w + t_2^{w-1}, \ldots, t_{n/2}^w, t_{n/2}^w + t_{n/2}^{w-1}) \neq 0$.

$$f' = \begin{bmatrix} t_1 \\ t_2 \\ \vdots \\ t_{n/2} \end{bmatrix}$$

- No. of variables $= n \rightarrow n/2$, individual degree $= d \rightarrow 2wd$.
- Repeat $\log n$ times. 1 variable, individual degree $= (2w)^{\log n}d$.
- Hitting-set size: $O(ndw^{\log n})$. 
**n-variate ROABP**

- \( f(t_1^w, t_1^w + t_1^{w-1}, x_3, x_4, \ldots, x_n) \neq 0. \)
- \( f(t_1^w, t_1^w + t_1^{w-1}, t_2^w, t_2^w + t_2^{w-1}, \ldots, x_n) \neq 0. \)
- \( f(t_1^w, t_1^w + t_1^{w-1}, t_2^w, t_2^w + t_2^{w-1}, \ldots, t_{n/2}^w, t_{n/2}^w + t_{n/2}^{w-1}) \neq 0. \)

\[
f' = \begin{bmatrix} t_1 \\ t_2 \\ \vdots \\ t_{n/2} \end{bmatrix}
\]

- no. of variables = \( n \rightarrow n/2 \), individual degree = \( d \rightarrow 2wd \).
- Repeat \( \log n \) times. 1 variable, individual degree = \((2w)^{\log n} d\).
- Hitting-set size: \( O(ndw^{\log n}) \).
- Hitting-set size: \( \text{poly}(n, d) \), if \( w \) is constant.
**n-variate ROABP**

- \( f(t_1^w, t_1^w + t_1^{w-1}, x_3, x_4, \ldots, x_n) \neq 0. \)
- \( f(t_1^w, t_1^w + t_1^{w-1}, t_2^w, t_2^w + t_2^{w-1}, \ldots, x_n) \neq 0. \)
- \( f(t_1^w, t_1^w + t_1^{w-1}, t_2^w, t_2^w + t_2^{w-1}, \ldots, t_{n/2}^w, t_{n/2}^w + t_{n/2}^{w-1}) \neq 0. \)

\[
f' = \begin{bmatrix}
  t_1 \\
  t_2 \\
  \vdots \\
  t_{n/2}
\end{bmatrix}
\]

- no. of variables = \( n \to n/2 \), individual degree = \( d \to 2wd \).
- Repeat \( \log n \) times. 1 variable, individual degree = \( (2w)^{\log n} d \).
- Hitting-set size: \( O(ndw^{\log n}) \).
- Hitting-set size: \( \text{poly}(n, d) \), if \( w \) is constant.
- Known variable order.
Proof of the bivariate case

Claim: If \( f(x, y) = \sum_{r=1}^{w} g_r(x) h_r(y) \), then \( f(t^w, t^w + t^{w-1}) \neq 0 \).
**Proof of the bivariate case**

- **Claim:** If \( f(x, y) = \sum_{r=1}^{w} g_r(x) h_r(y) \), then \( f(t^w, t^w + t^{w-1}) \neq 0 \).

- **Coefficient Matrix for** \( f(x, y) \) [Nisan, 1991]

\[
\begin{bmatrix}
    y^0 & \ldots & y^i & \ldots & y^d \\
    x^0 \\
    \vdots \\
    x^i \\
    \vdots \\
    x^d
\end{bmatrix}
\]

Define \( \text{rank}(f) \) as the rank of this matrix.

**Claim:** \( \text{rank}(f) \leq w \) [Nisan, 1991].
**Proof of the bivariate case**

- **Claim:** If \( f(x, y) = \sum_{r=1}^{w} g_r(x)h_r(y) \), then \( f(t^w, t^w + t^{w-1}) \neq 0 \).
- Coefficient Matrix for \( f(x, y) \) [Nisan, 1991]

\[
\begin{pmatrix}
    y^0 & \cdots & y^j & \cdots & y^d \\
    x^0 \\
    \vdots \\
    x^i \\
    \vdots \\
    x^d
\end{pmatrix}
\]

Define \( \text{rank}(f) \) as the rank of this matrix.
Proof of the bivariate case

- **Claim:** If \( f(x, y) = \sum_{r=1}^{w} g_r(x)h_r(y) \), then \( f(t^w, t^w + t^{w-1}) \neq 0 \).
- Coefficient Matrix for \( f(x, y) \) [Nisan, 1991]

\[
\begin{bmatrix}
y^0 & \ldots & y^i & \ldots & y^d \\
x^0 & & & & \\
\vdots & & & & \\
x^i & & & & \\
\vdots & & & & \\
x^d & & & & \\
\end{bmatrix}
\]

- Define \( \text{rank}(f) \) as the rank of this matrix.
- **Claim:** \( \text{rank}(f) \leq w \) [Nisan, 1991].
Proof of the bivariate case

- Define $f_r = g_r(x)h_r(y)$.
- **Claim**: $\text{rank}(f_r) \leq 1$. 
**Proof of the bivariate case**

- Define \( f_r = g_r(x)h_r(y) \).
- **Claim:** \( \text{rank}(f_r) \leq 1 \).
- Let \( g_r = a_0x^0 + a_1x^1 + \cdots + a_dx^d \) and \( h_r = b_0y^0 + b_1y^1 + \cdots + b_dy^d \).

\[
\begin{bmatrix}
  x^0 & x^1 & \cdots & x^d \\
  y^0 & y^1 & \cdots & y^d \\
\end{bmatrix}
\]

\[
\begin{bmatrix}
a_0b_0 & a_0b_1 & a_0b_d \\
a_1b_0 & a_1b_1 & a_1b_d \\
\vdots & \vdots & \vdots & \cdots & \vdots \\
a_db_0 & a_db_1 & a_db_d
\end{bmatrix}
\]
**Proof of the bivariate case**

- Define \( f_r = g_r(x)h_r(y) \).
- **Claim:** \( \text{rank}(f_r) \leq 1 \).
- Let \( g_r = a_0x^0 + a_1x^1 + \cdots + a_dx^d \) and \( h_r = b_0y^0 + b_1y^1 + \cdots + b_dy^d \).

\[
\begin{bmatrix}
    y^0 & y^1 & \cdots & y^d \\
    x^0 & \begin{bmatrix} a_0b_0 & a_0b_1 & a_0b_d \\ a_1b_0 & a_1b_1 & a_1b_d \\ \vdots & \vdots & \vdots & \vdots \\ a_db_0 & a_db_1 & a_db_d \end{bmatrix} \\ x^1 & \begin{bmatrix} a_0b_0 & a_0b_1 & a_0b_d \\ a_1b_0 & a_1b_1 & a_1b_d \\ \vdots & \vdots & \vdots & \vdots \\ a_db_0 & a_db_1 & a_db_d \end{bmatrix} \\ \vdots & \vdots & \vdots & \vdots \\ x^d & \begin{bmatrix} a_0b_0 & a_0b_1 & a_0b_d \\ a_1b_0 & a_1b_1 & a_1b_d \\ \vdots & \vdots & \vdots & \vdots \\ a_db_0 & a_db_1 & a_db_d \end{bmatrix} 
\end{bmatrix}
\]

\( \implies \text{rank}(f) = \text{rank}(\sum_{r=1}^{w} f_r) \leq w \).
**Proof of the bivariate case**

\[(x, y) \mapsto (t^w, t^w + t^{w-1}) = (t^w, t^w(1 + t^{-1})).\]
Proof of the bivariate case

\[(x, y) \mapsto (t^w, t^w + t^{w-1}) = (t^w, t^w(1 + t^{-1})).\]

\[x^i y^j \mapsto t^{(i+j)w}(1 + t^{-1})^j.\]
Proof of the bivariate case

\[(x, y) \mapsto (t^w, t^w + t^w - 1) = (t^w, t^w(1 + t^{-1})).\]

\[x^i y^j \mapsto t^{(i+j)w}(1 + t^{-1})^j.\]

- leading-term\((x^i y^j) = t^{(i+j)w}.\)
Proof of the bivariate case

\[(x, y) \mapsto (t^w, t^w + t^{w-1}) = (t^w, t^w(1 + t^{-1})).\]

\[x^i y^j \mapsto t^{(i+j)w}(1 + t^{-1})^j.\]

- leading-term\((x^i y^j) = t^{(i+j)w}.\)
- Same for all \(x^i y^j\) with \(i + j = \ell.\)
Proof of the bivariate case

\[(x, y) \mapsto (t^w, t^w + t^{w-1}) = (t^w, t^w(1 + t^{-1})).\]

\[x^i y^j \mapsto t^{(i+j)w}(1 + t^{-1})^j.\]

- \(\text{leading-term}(x^i y^j) = t^{(i+j)w}.\)
- Same for all \(x^i y^j\) with \(i + j = \ell.\)
Proof of the bivariate case

\[
\begin{bmatrix}
  x^0 & y_0 & y_1 & \ldots & y^d \\
  x^1 &   &   & \ddots &   \\
     &   &   & \ddots &   \\
  x^d &   &   &   & \ddots \\
\end{bmatrix}
\]

Leading nonzero Diagonal: at most \( w \) nonzero entries.

Leading term: \( t^w \ell \).

Leading term from the next diagonal: \( t^w (\ell - 1) \).

Focus on terms \( \{ t^w \ell, t^w (\ell - 1), \ldots, t^w (\ell - 1) + 1 \} \).

They come only from an \( \ell \)-th diagonal monomial.

\( \ell \)-th diagonal nonzero monomials: \( \{ x^{\ell - j_1} y^{j_1}, x^{\ell - j_2} y^{j_2}, \ldots, x^{\ell - j_w} y^{j_w} \} \).
**Proof of the bivariate case**

- Leading nonzero Diagonal: at most $w$ nonzero entries.
Proof of the bivariate case

- Leading nonzero Diagonal: at most $w$ nonzero entries.
- Leading term: $t^{w\ell}$.
**Proof of the bivariate case**

- Leading nonzero Diagonal: at most $w$ nonzero entries.
- Leading term: $t^{w\ell}$.
- Leading term from the next diagonal: $t^{w(\ell-1)}$. 
Proof of the bivariate case

- Leading nonzero Diagonal: at most $w$ nonzero entries.
- Leading term: $t^{w\ell}$.
- Leading term from the next diagonal: $t^{w(\ell-1)}$.
- Focus on terms $\{t^{w\ell}, t^{w\ell-1}, \ldots, t^{w(\ell-1)+1}\}$.
Proof of the bivariate case

- Leading nonzero Diagonal: at most $w$ nonzero entries.
- Leading term: $t^{w\ell}$.
- Leading term from the next diagonal: $t^{w(\ell-1)}$.
- Focus on terms $\{t^{w\ell}, t^{w\ell-1}, \ldots, t^{w(\ell-1)+1}\}$.
- They come only from an $\ell$-th diagonal monomial.
Proof of the bivariate case

- Leading nonzero Diagonal: at most \( w \) nonzero entries.
- Leading term: \( t^{w \ell} \).
- Leading term from the next diagonal: \( t^{w(\ell-1)} \).
- Focus on terms \( \{ t^{w \ell}, t^{w \ell-1}, \ldots, t^{w(\ell-1)+1} \} \).
- They come only from an \( \ell \)-th diagonal monomial.
- \( \ell \)-th diagonal nonzero monomials: \( \{ x^{\ell-j_1} y_{j_1}, x^{\ell-j_2} y_{j_2}, \ldots, x^{\ell-j_w} y_{j_w} \} \).
Proof of the bivariate case

\[ (x, y) \mapsto (t^w, t^w(1 + t^{-1})). \]

\[ x^{\ell-j_1}y^{j_1} \mapsto t^{\ell w}(1 + t^{-1})^{j_1}. \]
**Proof of the bivariate case**

\[(x, y) \mapsto (t^w, t^w(1 + t^{-1})).\]

\[x^{\ell-j_1} y^{j_1} \mapsto t^{\ell w}(1 + t^{-1})^{j_1}.\]

\[x^{\ell-j_1} y^{j_1} \mapsto t^{\ell w} \left( \binom{j_1}{0} + \binom{j_1}{1} t^{-1} + \cdots + \binom{j_1}{j_1} t^{-j_1} \right).\]
**Proof of the bivariate case**

\[(x, y) \mapsto (t^w, t^w(1 + t^{-1})).\]

\[x^\ell y_j \mapsto t^\ell w (1 + t^{-1})^j.\]

\[x^{\ell-j_1} y^{j_1} \mapsto t^\ell w \left( \binom{j_1}{0} + \binom{j_1}{1} t^{-1} + \cdots + \binom{j_1}{j_1} t^{-j_1} \right).\]

\[x^{\ell-j_1} y^{j_1} \mapsto \left( \binom{j_1}{0} t^\ell w + \binom{j_1}{1} t^{\ell w-1} + \cdots + \binom{j_1}{w-1} t^{(\ell-1)w+1} + \cdots \right).\]
Hitting-set for ROABP

Proof of the bivariate case

\[ x^{\ell-j_1} y^{j_1} \mapsto (\binom{j_1}{0}) t^{\ell w} + (\binom{j_1}{1}) t^{\ell w-1} + \ldots + (\binom{j_1}{w-1}) t^{(\ell-1)w+1} + \ldots \]
Proof of the bivariate case

\[ x^{\ell-j_1} y^{j_1} \mapsto (j_1^0) t^{\ell w} + (j_1^1) t^{\ell w-1} + \ldots + (j_1^{w-1}) t^{(\ell-1)w+1} + \ldots \]

\[ x^{\ell-j_2} y^{j_2} \mapsto (j_2^0) t^{\ell w} + (j_2^1) t^{\ell w-1} + \ldots + (j_2^{w-1}) t^{(\ell-1)w+1} + \ldots \]

Assuming \( j_k \neq j_k' \) requires nonzero characteristic.
Proof of the bivariate case

\[ x^{\ell-j_1} y^{j_1} \mapsto (\binom{j_1}{0}) t^{\ell w} + (\binom{j_1}{1}) t^{\ell w-1} + \ldots + (\binom{j_1}{w-1}) t^{(\ell-1)w+1} + \ldots \]

\[ x^{\ell-j_2} y^{j_2} \mapsto (\binom{j_2}{0}) t^{\ell w} + (\binom{j_2}{1}) t^{\ell w-1} + \ldots + (\binom{j_2}{w-1}) t^{(\ell-1)w+1} + \ldots \]

\[ \vdots \]

\[ x^{\ell-j_w} y^{j_w} \mapsto (\binom{j_w}{0}) t^{\ell w} + (\binom{j_w}{1}) t^{\ell w-1} + \ldots + (\binom{j_w}{w-1}) t^{(\ell-1)w+1} + \ldots \]
Proof of the bivariate case

\[
\begin{align*}
  x^{\ell-j_1} y^{j_1} & \mapsto (j_1^0) t^{\ell w} + (j_1^1) t^{\ell w-1} + \ldots + (j_{w-1}^1) t^{(\ell-1)w+1} + \ldots \\
  x^{\ell-j_2} y^{j_2} & \mapsto (j_2^0) t^{\ell w} + (j_2^1) t^{\ell w-1} + \ldots + (j_{w-1}^2) t^{(\ell-1)w+1} + \ldots \\
  \vdots \\
  x^{\ell-j_w} y^{j_w} & \mapsto (j_w^0) t^{\ell w} + (j_w^1) t^{\ell w-1} + \ldots + (j_{w-1}^w) t^{(\ell-1)w+1} + \ldots \\
 0 & \ast & \ldots & 0
\end{align*}
\]
**Proof of the bivariate case**

\[ x^{\ell-j_1} y^{j_1} \mapsto (j_1^0) t^{\ell w} + (j_1^1) t^{\ell w-1} + \ldots + (j_1^w) t^{(\ell-1)w+1} + \ldots \]

\[ x^{\ell-j_2} y^{j_2} \mapsto (j_2^0) t^{\ell w} + (j_2^1) t^{\ell w-1} + \ldots + (j_2^w) t^{(\ell-1)w+1} + \ldots \]

\[ \vdots \]

\[ x^{\ell-j_w} y^{j_w} \mapsto (j_w^0) t^{\ell w} + (j_w^1) t^{\ell w-1} + \ldots + (j_w^w) t^{(\ell-1)w+1} + \ldots \]

\[ 0 \quad * \quad \ldots \quad 0 \]

- Assuming \( j_k \neq j_{k'} \) requires nonzero characteristic.
Discussion

- Possible improvements:
  - Unknown variable order
  - Hitting-set for all fields.
  - Poly-time for arbitrary width.
Discussion

- Possible improvements:
  - Unknown variable order
  - Hitting-set for all fields.
  - Poly-time for arbitrary width.

- Connections between arithmetic and boolean pseudorandomness?


Derandomizing polynomial identity tests means proving circuit lower bounds.
STOC, pages 355–364.

Pseudorandom generators for space-bounded computations.

Lower bounds for non-commutative computation (extended abstract).

On recycling the randomness of states in space bounded computation.

Deterministic polynomial identity testing in non-commutative models.

Fast probabilistic algorithms for verification of polynomial identities.

Completeness classes in algebra.