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 $P(\mathbf{x}) \in \mathbb{F}[x_1, x_2, \ldots, x_n]$, $P(\mathbf{x}) = 0$?

Polynomial Identity Testing

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

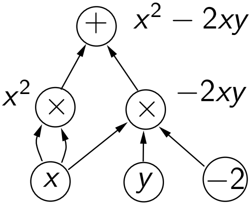


Figure : An Arithmetic circuit

Randomized Test

- Rephrasing the question: Given an arithmetic circuit decide if it computes the zero polynomial.
- Randomized PIT: evaluate $P(\mathbf{x})$ 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 $P(\mathbf{x})$ 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 $P(\mathbf{x})$ 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 $P(\mathbf{x})$ 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 $P(\mathbf{x})$ 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

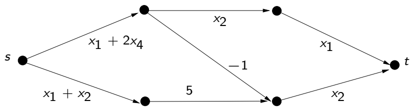


Figure : An Arithmetic branching program.

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

Arithmetic Branching Programs

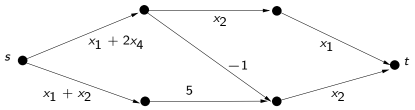


Figure : An Arithmetic branching program.

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

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

Arithmetic Branching Programs

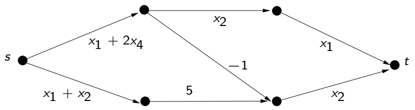


Figure : An Arithmetic branching program.

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

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

- $C(\mathbf{x}) = (x_1 + 2x_4)x_2x_1 - (x_1 + 2x_4)x_2 + (x_1 + x_2)5x_2$

Arithmetic Branching Programs

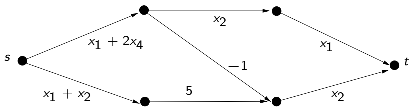


Figure : An Arithmetic branching program.

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

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

- $C(\mathbf{x}) = (x_1 + 2x_4)x_2x_1 - (x_1 + 2x_4)x_2 + (x_1 + x_2)5x_2$
- Width: maximum number of nodes in a layer.

Arithmetic Branching Programs

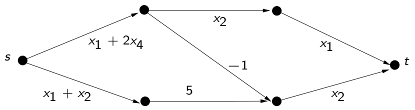


Figure : An Arithmetic branching program.

- Equivalent representation:

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

- $C(\mathbf{x}) = (x_1 + 2x_4)x_2x_1 - (x_1 + 2x_4)x_2 + (x_1 + x_2)5x_2$
- Width: maximum dimension of the matrices.

Power of ABPs

- 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.

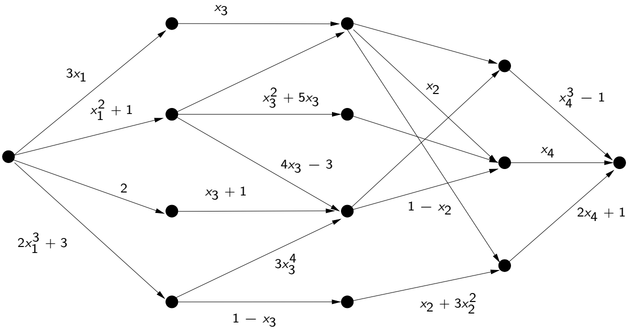


Figure : A Read-once oblivious ABP with variable order (x_1, x_3, x_2, x_4)

PIT for ROABPs

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

PIT for ROABPs

- [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].

PIT for ROABPs

- [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].
- Nothing better known even for constant width.

Our Results

1. Polynomial time blackbox test for constant width ROABPs*.

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.

Read-once Ordered Branching Programs

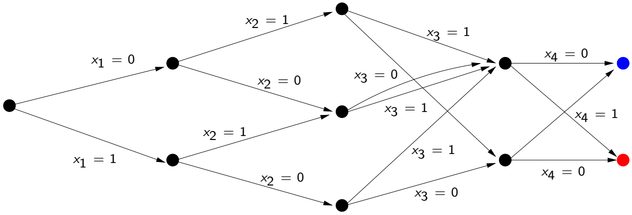


Figure : An ROBP

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).

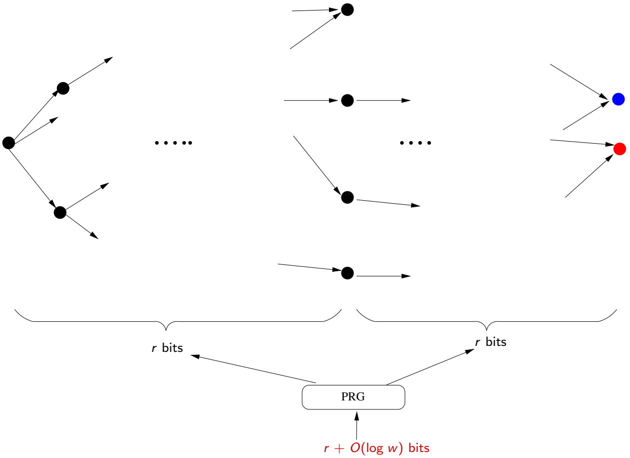
Pseudorandomness for ROBP

- 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].

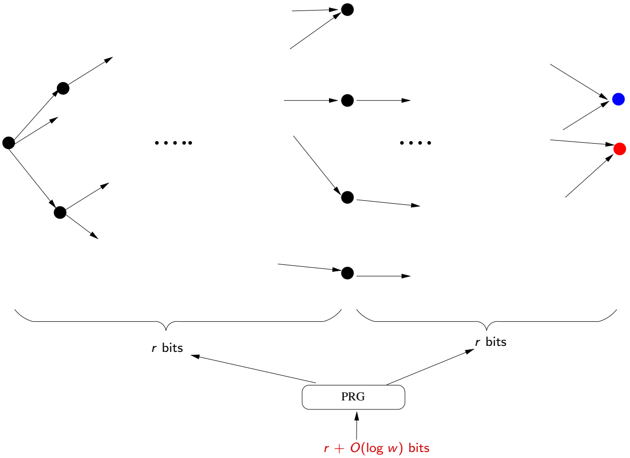
Pseudorandomness for ROBP

- 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.

[Impagliazzo et al., 1994]

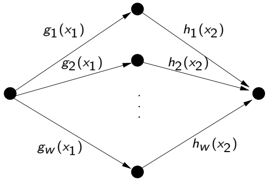


[Impagliazzo et al., 1994]



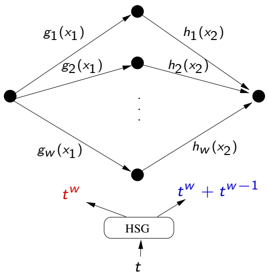
- Sample space size: poly$(w) \times 2^r$ instead of trivial $2^r \times 2^r$.

Hitting-set for Bivariate ROABP

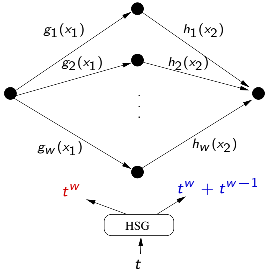


$$f(x_1, x_2) = \sum_{r=1}^{w} g_r(x_1)\ h_r(x_2)$$

Hitting-set for Bivariate ROABP

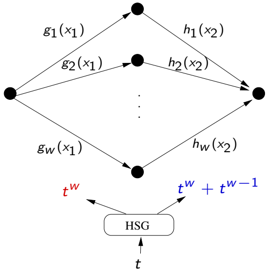


Hitting-set for Bivariate ROABP



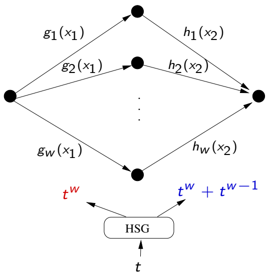
- $f(x_1, x_2) = \sum_{r=1}^{w} g_r(x_1)\ h_r(x_2)$
- *Claim*: $f(t^w, t^w + t^{w-1}) \neq 0$.

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 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

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

n-variate ROABP

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

- *Claim*: $f(t_1^w, t_1^w + t_1^{w-1}, x_3, x_4, \ldots, x_n) \neq 0$.

n-variate ROABP

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

- *Claim*: $f\big(t_1^{w}, t_1^{w} + t_1^{w-1}, x_3, x_4, \ldots, x_n\big) \neq 0$.
- *Proof*: treat $x_3, x_4, \ldots, x_n$ as constants.

n-variate ROABP

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

- *Claim*: $f(t_1^w, t_1^w + t_1^{w-1}, x_3, x_4, \ldots, x_n) \neq 0$.
- *Proof*: treat $x_3, x_4, \ldots, x_n$ as constants.

$$f = \begin{bmatrix} & x_1 & \end{bmatrix} \begin{bmatrix} \\ x_2 \\ \\ \end{bmatrix}$$

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

n-variate ROABP

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

- *Claim*: $f({\color{red}t_1^w}, {\color{blue}t_1^w + t_1^{w-1}}, x_3, x_4, \ldots, x_n) \neq 0$.
- *Proof*: treat $x_3, x_4, \ldots, x_n$ as constants.

$$f = \begin{bmatrix} & x_1 & \end{bmatrix} \begin{bmatrix} \\ x_2 \\ \\ \end{bmatrix}$$

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

- $f({\color{red}t_1^w}, {\color{blue}t_1^w + t_1^{w-1}}) \neq 0$ (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

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

n-variate ROABP

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

n-variate ROABP

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

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

n-variate ROABP

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

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

n-variate ROABP

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

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

- no. of variables $= n \to n/2$, individual degree $= d \to 2wd$.

n-variate ROABP

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

$$f' = \left[\quad t_1 \quad\right] \left[\quad t_2 \quad\right] \cdots \left[t_{n/2} \right]$$

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

n-variate ROABP

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

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

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

n-variate ROABP

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

$$f' = \left[\quad t_1 \quad\quad\right] \left[\quad t_2 \quad\quad\right] \cdots \left[t_{n/2}\right]$$

- no. of variables $= n \to n/2$, individual degree $= d \to 2wd$.
- Repeat $\log n$ times. 1 variable, indvidual 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

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

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

- no. of variables $= n \to n/2$, individual degree $= d \to 2wd$.
- Repeat $\log n$ times. 1 variable, indvidual degree $= (2w)^{\log n} d$.
- Hitting-set size: $O(ndw^{\log n})$.
- Hitting-set size: $\mathrm{poly}(n, d)$, 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]

$$
\begin{array}{c c}
 & \begin{array}{ccccc} y^0 & \cdots & y^j & \cdots & y^d \end{array} \\
\begin{array}{c} x^0 \\ \vdots \\ x^i \\ \vdots \\ x^d \end{array} &
\begin{bmatrix} & & & & \\ & & & & \\ - & & \mathrm{coef}_f(x^i y^j) & & \\ & & & & \\ & & & & \end{bmatrix}
\end{array}
$$

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]

$$
\begin{array}{c c}
 & \begin{array}{ccccc} y^0 & \cdots & y^j & \cdots & y^d \end{array} \\
\begin{array}{c} x^0 \\ \vdots \\ x^i \\ \vdots \\ x^d \end{array} &
\begin{bmatrix} & & | & & \\ & & & & \\ - & & \mathrm{coef}_f(x^i y^j) & & \\ & & & & \\ & & & & \end{bmatrix}
\end{array}
$$

- Define $\mathrm{rank}(f)$ 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]

$$\begin{array}{c|c} & \begin{array}{ccccc} y^0 & \cdots & y^j & \cdots & y^d \end{array} \\ \begin{array}{c} x^0 \\ \vdots \\ x^i \\ \vdots \\ x^d \end{array} & \begin{bmatrix} & & | & & \\ & & & & \\ - & & \mathrm{coef}_f(x^i y^j) & & \\ & & & & \\ & & & & \end{bmatrix} \end{array}$$

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

Proof of the bivariate case

- Define $f_r = g_r(x)h_r(y)$.
- *Claim:* $\mathrm{rank}(f_r) \leq 1$.

Proof of the bivariate case

- Define $f_r = g_r(x)h_r(y)$.
- *Claim:* $\text{rank}(f_r) \leq 1$.
- Let $g_r = a_0 x^0 + a_1 x^1 + \cdots + a_d x^d$ and $h_r = b_0 y^0 + b_1 y^1 + \cdots + b_d y^d$.

$$\begin{array}{cc} & \begin{array}{cccc} y^0 & y^1 & \cdots & y^d \end{array} \\ \begin{array}{c} x^0 \\ x^1 \\ \vdots \\ x^d \end{array} & \begin{bmatrix} a_0 b_0 & a_0 b_1 & & a_0 b_d \\ a_1 b_0 & a_1 b_1 & & a_1 b_d \\ \vdots & \vdots & \cdots & \vdots \\ a_d b_0 & a_d b_1 & & a_d b_d \end{bmatrix} \end{array}$$

Proof of the bivariate case

- Define $f_r = g_r(x)h_r(y)$.
- *Claim:* $\text{rank}(f_r) \leq 1$.
- Let $g_r = a_0 x^0 + a_1 x^1 + \cdots + a_d x^d$ and $h_r = b_0 y^0 + b_1 y^1 + \cdots + b_d y^d$.

$$
\begin{array}{c c}
 & \begin{array}{cccc} y^0 & y^1 & \cdots & y^d \end{array} \\
\begin{array}{c} x^0 \\ x^1 \\ \vdots \\ x^d \end{array} &
\begin{bmatrix}
a_0 b_0 & a_0 b_1 & & a_0 b_d \\
a_1 b_0 & a_1 b_1 & & a_1 b_d \\
\vdots & \vdots & \cdots & \vdots \\
a_d b_0 & a_d b_1 & & a_d b_d
\end{bmatrix}
\end{array}
$$

- $\implies \text{rank}(f) = \text{rank}(\sum_{r=1}^{w} f_r) \leq w$.

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

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

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

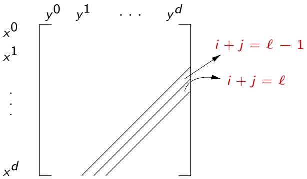
- leading-term$(x^i y^j) = t^{(i+j)w}$.
- Same for all $x^i y^j$ with $i + j = \ell$.

Proof of the bivariate case

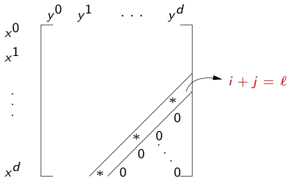
$$(x,y) \mapsto ({\color{red}t^w}, {\color{blue}t^w + t^{w-1}}) = ({\color{red}t^w}, {\color{blue}t^w(1+t^{-1})}).$$

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

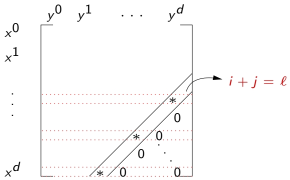
- leading-term$(x^i y^j) = t^{(i+j)w}$.
- Same for all $x^i y^j$ with $i+j=\ell$.



Proof of the bivariate case

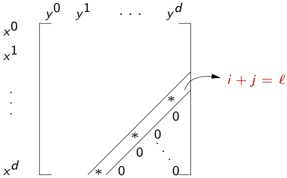


Proof of the bivariate case



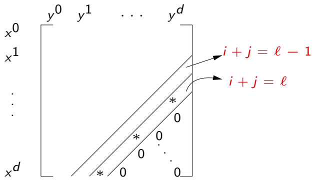
- Leading nonzero Diagonal: at most w nonzero entries.

Proof of the bivariate case



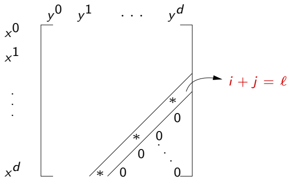
- Leading nonzero Diagonal: at most w nonzero entries.
- Leading term: $t^{w\ell}$.

Proof of the bivariate case



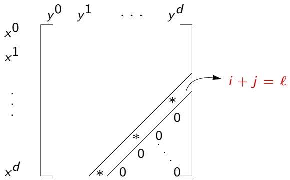
- Leading nonzero Diagonal: at most w nonzero entries.
- Leading term: $t^{w\ell}$.
- Leading term from the next diagonal: $t^{w(\ell-1)}$.

Proof of the bivariate case



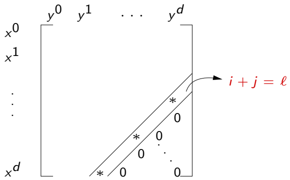
- Leading nonzero Diagonal: at most w nonzero entries.
- Leading term: $t^{w\ell}$.
- Leading term from the next diagonal: $t^{w(\ell-1)}$.
- Focus on terms $\{t^{w\ell}, t^{w\ell-1}, \cdots, t^{w(\ell-1)+1}\}$.

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 $\{t^{w\ell}, t^{w\ell-1}, \cdots, t^{w(\ell-1)+1}\}$.
- They come only from an ℓ-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 $\{t^{w\ell}, t^{w\ell-1}, \cdots, t^{w(\ell-1)+1}\}$.
- They come only from an ℓ-th diagonal monomial.
- ℓ-th diagonal nonzero monomials: $\{x^{\ell-j_1}y^{j_1}, x^{\ell-j_2}y^{j_2}, \cdots, x^{\ell-j_w}y^{j_w}\}$.

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

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

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

$$x^{\ell - j_1} y^{j_1} \mapsto \binom{j_1}{0} t^{\ell w} + \binom{j_1}{1} t^{\ell w - 1} + \cdots + \binom{j_1}{w-1} t^{(\ell - 1)w + 1} + \cdots$$

Proof of the bivariate case

$$x^{\ell-j_1}y^{j_1} \mapsto \quad \binom{j_1}{0}t^{\ell w} + \binom{j_1}{1}t^{\ell w-1} + \cdots + \binom{j_1}{w-1}t^{(\ell-1)w+1} + \cdots$$

Proof of the bivariate case

$$x^{\ell-j_1}y^{j_1} \mapsto \quad \binom{j_1}{0}t^{\ell w} + \binom{j_1}{1}t^{\ell w-1} + \cdots + \binom{j_1}{w-1}t^{(\ell-1)w+1} + \cdots$$
$$x^{\ell-j_2}y^{j_2} \mapsto \quad \binom{j_2}{0}t^{\ell w} + \binom{j_2}{1}t^{\ell w-1} + \cdots + \binom{j_2}{w-1}t^{(\ell-1)w+1} + \cdots$$

Proof of the bivariate case

$$
\begin{aligned}
x^{\ell-j_1}y^{j_1} &\mapsto \quad \binom{j_1}{0}t^{\ell w} + \binom{j_1}{1}t^{\ell w-1} + \cdots + \binom{j_1}{w-1}t^{(\ell-1)w+1} + \cdots \\
x^{\ell-j_2}y^{j_2} &\mapsto \quad \binom{j_2}{0}t^{\ell w} + \binom{j_2}{1}t^{\ell w-1} + \cdots + \binom{j_2}{w-1}t^{(\ell-1)w+1} + \cdots \\
&\qquad\qquad\qquad\qquad \vdots \\
x^{\ell-j_w}y^{j_w} &\mapsto \quad \binom{j_w}{0}t^{\ell w} + \binom{j_w}{1}t^{\ell w-1} + \cdots + \binom{j_w}{w-1}t^{(\ell-1)w+1} + \cdots
\end{aligned}
$$

Proof of the bivariate case

$$
\begin{array}{rcl}
x^{\ell-j_1}y^{j_1} & \mapsto & \binom{j_1}{0}t^{\ell w} + \binom{j_1}{1}t^{\ell w-1} + \cdots + \binom{j_1}{w-1}t^{(\ell-1)w+1} + \cdots \\
x^{\ell-j_2}y^{j_2} & \mapsto & \binom{j_2}{0}t^{\ell w} + \binom{j_2}{1}t^{\ell w-1} + \cdots + \binom{j_2}{w-1}t^{(\ell-1)w+1} + \cdots \\
 & & \vdots \\
x^{\ell-j_w}y^{j_w} & \mapsto & \binom{j_w}{0}t^{\ell w} + \binom{j_w}{1}t^{\ell w-1} + \cdots + \binom{j_w}{w-1}t^{(\ell-1)w+1} + \cdots \\
\hline
 & & 0 \qquad * \qquad \cdots \qquad 0
\end{array}
$$

Proof of the bivariate case

$$
\begin{array}{rcl}
x^{\ell-j_1}y^{j_1} & \mapsto & \binom{j_1}{0}t^{\ell w} + \binom{j_1}{1}t^{\ell w-1} + \cdots + \binom{j_1}{w-1}t^{(\ell-1)w+1} + \cdots \\
x^{\ell-j_2}y^{j_2} & \mapsto & \binom{j_2}{0}t^{\ell w} + \binom{j_2}{1}t^{\ell w-1} + \cdots + \binom{j_2}{w-1}t^{(\ell-1)w+1} + \cdots \\
 & & \vdots \\
x^{\ell-j_w}y^{j_w} & \mapsto & \binom{j_w}{0}t^{\ell w} + \binom{j_w}{1}t^{\ell w-1} + \cdots + \binom{j_w}{w-1}t^{(\ell-1)w+1} + \cdots \\
\hline
 & & 0 \qquad * \qquad \cdots \qquad 0
\end{array}
$$

- 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?

Agrawal, M. (2005).
Proving lower bounds via pseudo-random generators.
In *FSTTCS*, volume 3821 of *Lecture Notes in Computer Science*, pages 92–105.

Agrawal, M., Gurjar, R., Korwar, A., and Saxena, N. (2015).
Hitting-sets for ROABP and sum of set-multilinear circuits.
SIAM J. Comput., 44(3):669–697.

Ben-Or, M. and Cleve, R. (1992).
Computing algebraic formulas using a constant number of registers.
SIAM J. Comput., 21(1):54–58.

Berkowitz, S. J. (1984).
On computing the determinant in small parallel time using a small number of processors.
Information Processing Letters, 18(3):147 – 150.

Demillo, R. A. and Lipton, R. J. (1978).
A probabilistic remark on algebraic program testing.
Information Processing Letters, 7(4):193 – 195.

Forbes, M. A., Saptharishi, R., and Shpilka, A. (2014).
Hitting sets for multilinear read-once algebraic branching programs, in any order.
In *Symposium on Theory of Computing, STOC 2014, New York, NY, USA, May 31 - June 03, 2014*, pages 867–875.

Forbes, M. A. and Shpilka, A. (2013).
Quasipolynomial-time identity testing of non-commutative and read-once oblivious algebraic branching programs.
In *FOCS*, pages 243–252.

Impagliazzo, R., Nisan, N., and Wigderson, A. (1994).
Pseudorandomness for network algorithms.
In *Proceedings of the Twenty-sixth Annual ACM Symposium on Theory of Computing*, STOC, pages 356–364, New York, NY, USA. ACM.

Kabanets, V. and Impagliazzo, R. (2003).
Derandomizing polynomial identity tests means proving circuit lower bounds.
STOC, pages 355–364.

Nisan, N. (1990).
Pseudorandom generators for space-bounded computations.
In *Proceedings of the Twenty-second Annual ACM Symposium on Theory of Computing*, STOC '90, pages 204–212, New York, NY, USA. ACM.

Nisan, N. (1991).
Lower bounds for non-commutative computation (extended abstract).
In *Proceedings of the 23rd ACM Symposium on Theory of Computing, ACM Press*, pages 410–418.

Raz, R. and Reingold, O. (1999).
On recycling the randomness of states in space bounded computation.
In *Proceedings of the Thirty-First Annual ACM Symposium on Theory of Computing, May 1-4, 1999, Atlanta, Georgia, USA*, pages 159–168.

Raz, R. and Shpilka, A. (2005).
Deterministic polynomial identity testing in non-commutative models.
Computational Complexity, 14(1):1–19.

Schwartz, J. T. (1980).
Fast probabilistic algorithms for verification of polynomial identities.
J. ACM, 27(4):701–717.

Valiant, L. G. (1979).
Completeness classes in algebra.
In *Proceedings of the Eleventh Annual ACM Symposium on Theory of Computing*, STOC '79, pages 249–261, New York, NY, USA. ACM.

Zippel, R. (1979).
Probabilistic algorithms for sparse polynomials.
In *Proceedings of the International Symposiumon on Symbolic and Algebraic Computation*, EUROSAM '79, pages 216–226, London, UK, UK. Springer-Verlag.