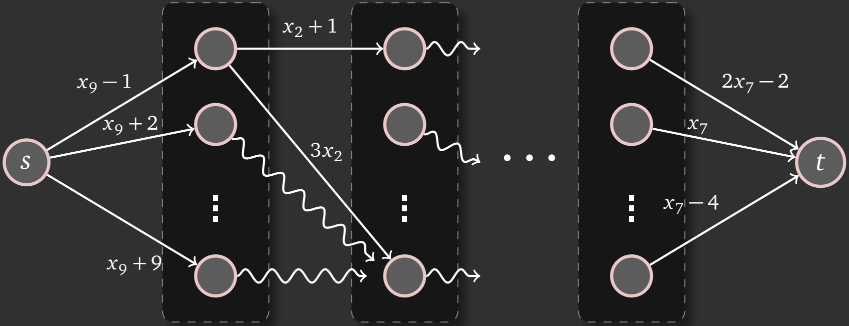
IDENTITY TESTING & LOWER BOUNDS
FOR
READ-k OBLIVIOUS ABPS

Ben Lee Volk

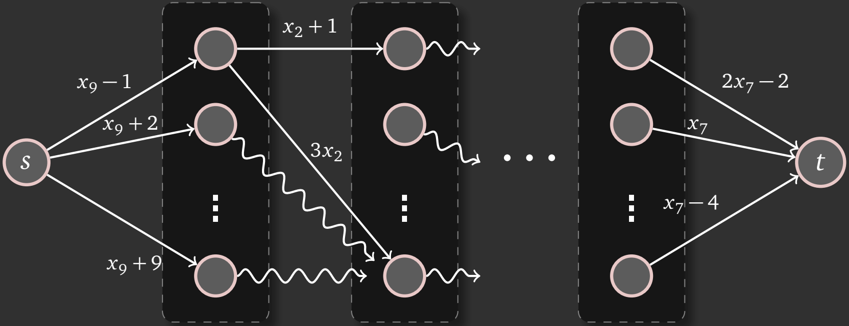
Joint with

Matthew Anderson
Michael A. Forbes
Ramprasad Saptharishi
Amir Shpilka

READ-ONCE OBLIVIOUS ABPS

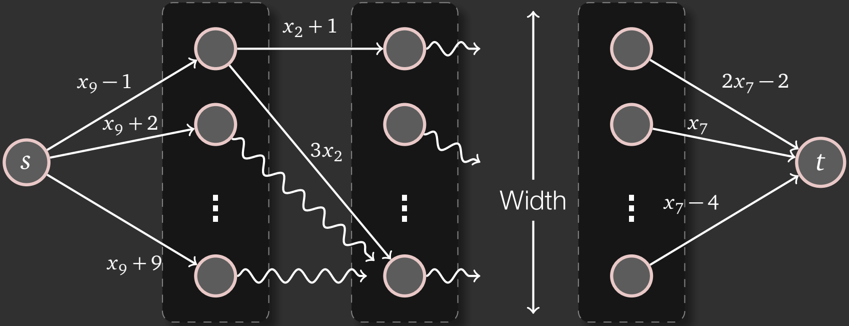


READ-ONCE OBLIVIOUS ABPS



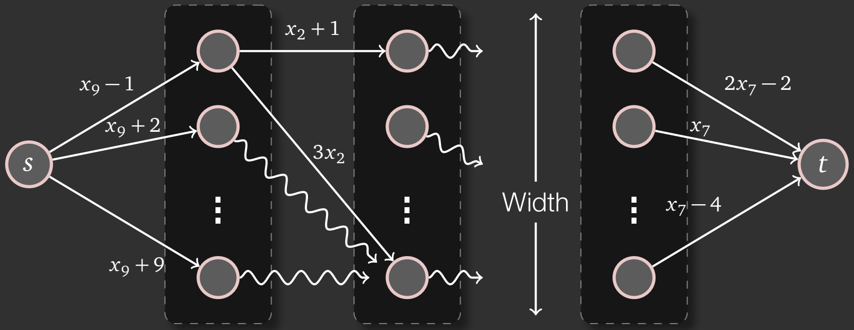
- Each $s \to t$ path computes multiplication of edge labels
- Program computes the sum of those over all $s \to t$ paths
- **Read Once**: Each var appears in one layer

READ-ONCE OBLIVIOUS ABPS



- Each $s \to t$ path computes multiplication of edge labels
- Program computes the sum of those over all $s \to t$ paths
- **Read Once**: Each var appears in one layer

READ-ONCE OBLIVIOUS ABPS



Equivalently: f is the $(1, 1)$ entry of the iterated matrix product

$$\prod_{i=1}^{n} M_i(x_{\pi(i)})$$

SOME THINGS YOU'VE ALL HEARD ABOUT

We know a lot about ROABPs :)

SOME THINGS YOU'VE ALL HEARD ABOUT

We know a lot about ROABPs :)

- Exponential lower bounds **[Nisan]**

SOME THINGS YOU'VE ALL HEARD ABOUT

We know a lot about ROABPs :)

- Exponential lower bounds [Nisan]
- Poly-time white-box PIT [Raz-Shpilka]

SOME THINGS YOU'VE ALL HEARD ABOUT

We know a lot about ROABPs :)

- Exponential lower bounds **[Nisan]**
- Poly-time white-box PIT **[Raz-Shpilka]**
- Quasipoly-size hitting sets even when order is unknown **[Forbes-Shpilka, Forbes-Shpilka-Saptharishi, Agrawal-Gurjar-Korwar-Saxena]**

SOME THINGS YOU'VE ALL HEARD ABOUT

We know a lot about ROABPs :)

- Exponential lower bounds **[Nisan]**
- Poly-time white-box PIT **[Raz-Shpilka]**
- Quasipoly-size hitting sets even when order is unknown **[Forbes-Shpilka, Forbes-Shpilka-Saptharishi, Agrawal-Gurjar-Korwar-Saxena]**

... and also PIT for sums of ROABPs and bounded-width ROABPs (all in this workshop).

SOME THINGS YOU'VE ALL HEARD ABOUT

We know a lot about ROABPs :)

- Exponential lower bounds **[Nisan]**
- Poly-time white-box PIT **[Raz-Shpilka]**
- Quasipoly-size hitting sets even when order is unknown **[Forbes-Shpilka, Forbes-Shpilka-Saptharishi, Agrawal-Gurjar-Korwar-Saxena]**

... and also PIT for sums of ROABPs and bounded-width ROABPs (all in this workshop).

This talk is about **read-k oblivious ABPs**.

SOME THINGS YOU'VE ALL HEARD ABOUT

We know a lot about ROABPs :)

- Exponential lower bounds **[Nisan]**
- Poly-time white-box PIT **[Raz-Shpilka]**
- Quasipoly-size hitting sets even when order is unknown **[Forbes-Shpilka, Forbes-Shpilka-Saptharishi, Agrawal-Gurjar-Korwar-Saxena]**

... and also PIT for sums of ROABPs and bounded-width ROABPs (all in this workshop).

This talk is about **read-k oblivious ABPs**.
(def: same as before except that now every variable appears in at most k layers)

READING k TIMES

READING k TIMES

- Generalizes sum of k ROABPs (PIT by **[Gurjar, Korwar, Saxena, Thierauf]**)

READING k TIMES

- Generalizes sum of k ROABPs (PIT by **[Gurjar, Korwar, Saxena, Thierauf]**)
- Generalizes read-k formulas (PIT by **[Anderson, van Melkbeek, Volkovich]**)

READING k TIMES

- Generalizes sum of k ROABPs (PIT by **[Gurjar, Korwar, Saxena, Thierauf]**)
- Generalizes read-k formulas (PIT by **[Anderson, van Melkbeek, Volkovich]**)
- Well-studied **boolean** analog

READING k TIMES

- Generalizes sum of k ROABPs (PIT by **[Gurjar, Korwar, Saxena, Thierauf]**)
- Generalizes read-k formulas (PIT by **[Anderson, van Melkbeek, Volkovich]**)
- Well-studied **boolean** analog

For read-k oblivious **boolean** branching programs:

READING k TIMES

- Generalizes sum of k ROABPs (PIT by **[Gurjar, Korwar, Saxena, Thierauf]**)
- Generalizes read-k formulas (PIT by **[Anderson, van Melkbeek, Volkovich]**)
- Well-studied **boolean** analog

For read-k oblivious **boolean** branching programs:

- $\exp(n/2^k)$ lower bounds **[Okolnishnikova, Borodin-Razborov-Smolensky]** even for randomized and non-deterministic variants

READING k TIMES

- Generalizes sum of k ROABPs (PIT by **[Gurjar, Korwar, Saxena, Thierauf]**)
- Generalizes read-k formulas (PIT by **[Anderson, van Melkbeek, Volkovich]**)
- Well-studied **boolean** analog

For read-k oblivious **boolean** branching programs:

- $\exp(n/2^k)$ lower bounds **[Okolnishnikova, Borodin-Razborov-Smolensky]** even for randomized and non-deterministic variants
- PRG with seed length $\sqrt{s}$ for size-s programs **[Impagliazzo-Meka-Zuckerman]**

READ-k OBLIVIOUS ABPS

READ-k OBLIVIOUS ABPS

Lower Bound: There is a polynomial $f \in \mathrm{VP}$ that requires read-k oblivious ABPs of width $\exp(n/k^k)$.

READ-k OBLIVIOUS ABPS

Lower Bound: There is a polynomial $f \in \mathrm{VP}$ that requires read-k oblivious ABPs of width $\exp(n/k^k)$.

PIT: There is a white-box* PIT algorithm for read-k oblivious ABPs, of running time $\exp(n^{1-1/2^{k-1}})$.

*only the order in which the variables appear is important

EVALUATION DIMENSION

Reminder: $f \in \mathbb{F}[x_1, \ldots, x_n]$, $S \subseteq [n]$.

$$\text{eval-dim}_{S,\overline{S}}(f) = \dim\ \text{span}\ \left\{ f|_{\mathbf{x}_S = \alpha} \mid \alpha \in \mathbb{F}^{|S|} \right\}.$$

EVALUATION DIMENSION

Reminder: $f \in \mathbb{F}[x_1, \ldots, x_n]$, $S \subseteq [n]$.

$$\text{eval-dim}_{S,\overline{S}}(f) = \dim \operatorname{span} \left\{ f|_{\mathbf{x}_S = \alpha} \mid \alpha \in \mathbb{F}^{|S|} \right\}.$$

Characterizes ROABP complexity:

Theorem [Nisan]: f has ROABP of width w in variable order $x_1, x_2, \ldots, x_n$ iff for every $i \in [n]$,

$$\text{eval-dim}_{[i],\overline{[i]}}(f) \leq w.$$

EVALUATION DIMENSION

Reminder: $f \in \mathbb{F}[x_1, \ldots, x_n]$, $S \subseteq [n]$.

$$\text{eval-dim}_{S,\overline{S}}(f) = \dim \operatorname{span} \left\{ f|_{\mathbf{x}_S = \alpha} \mid \alpha \in \mathbb{F}^{|S|} \right\}.$$

Characterizes ROABP complexity:

Theorem [Nisan]: f has ROABP of width w in variable order $x_1, x_2, \ldots, x_n$ iff for every $i \in [n]$,

$$\text{eval-dim}_{[i],\overline{[i]}}(f) \leq w.$$

(same as rank of partial derivative matrix)

WARM-UP: 2-PASS ABP

Same as ROABP but with two “passes”:

x_1	x_2	$\cdots$	x_{n-1}	x_n	x_1	x_2	$\cdots$	x_{n-1}	x_n

$$f = \left(M_1^1(x_1)M_2^1(x_2)\cdots M_n^1(x_n)\cdot M_1^2(x_1)M_2^2(x_2)\cdots M_n^2(x_n)\right)_{(1,1)}$$

WARM-UP: 2-PASS ABP

Same as ROABP but with two “passes”:

x_1	x_2	$\cdots$	x_{n-1}	x_n	x_1	x_2	$\cdots$	x_{n-1}	x_n

$$f = \left(M_1^1(x_1)M_2^1(x_2)\cdots M_n^1(x_n)\cdot M_1^2(x_1)M_2^2(x_2)\cdots M_n^2(x_n)\right)_{(1,1)}$$

Fixing $x_1 = \alpha_1$:

$$\left(N^1(\alpha_1)M_2^1(x_2)\cdots M_n^1(x_n)\cdot N^2(\alpha_1)M_2^2(x_2)\cdots M_n^2(x_n)\right)_{(1,1)}$$

WARM-UP: 2-PASS ABP

Same as ROABP but with two “passes”:

x_1	x_2	$\cdots$	x_{n-1}	x_n	x_1	x_2	$\cdots$	x_{n-1}	x_n

$$f = \left(M_1^1(x_1)M_2^1(x_2)\cdots M_n^1(x_n)\cdot M_1^2(x_1)M_2^2(x_2)\cdots M_n^2(x_n)\right)_{(1,1)}$$

Fixing $x_1 = \alpha_1, x_2 = \alpha_2$:

$$\left(N^1(\alpha_1,\alpha_2)M_3^1(x_3)\cdots M_n^1(x_n)\cdot N^2(\alpha_1,\alpha_2)M_3^2(x_3)\cdots M_n^2(x_n)\right)_{(1,1)}$$

WARM-UP: 2-PASS ABP

Same as ROABP but with two “passes”:

x_1	x_2	$\cdots$	x_{n-1}	x_n	x_1	x_2	$\cdots$	x_{n-1}	x_n

$$f = \left(M_1^1(x_1)M_2^1(x_2)\cdots M_n^1(x_n)\cdot M_1^2(x_1)M_2^2(x_2)\cdots M_n^2(x_n)\right)_{(1,1)}$$

Fixing $x_1, x_2, \ldots, x_i$:

$$f|_{\mathbf{x}_{[i]}=\alpha} = \Big(N^1(\alpha_1, \ldots, \alpha_i)M_{i+1}^1(x_{i+1})\cdots M_n^1(x_n)$$
$$N^2(\alpha_1, \ldots, \alpha_i)M_{i+1}^2(x_{i+1})\cdots M_n^2(x_n)\Big)_{(1,1)}$$

WARM-UP: 2-PASS ABP

Same as ROABP but with two "passes":

x_1	x_2	$\cdots$	x_{n-1}	x_n	x_1	x_2	$\cdots$	x_{n-1}	x_n

$$f = \left(M_1^1(x_1)M_2^1(x_2)\cdots M_n^1(x_n)\cdot M_1^2(x_1)M_2^2(x_2)\cdots M_n^2(x_n)\right)_{(1,1)}$$

Fixing $x_1, x_2, \ldots, x_i$:

$$f|_{\mathbf{x}_{[i]}=\alpha} = \big(N^1(\alpha_1,\ldots,\alpha_i)M_{i+1}^1(x_{i+1})\cdots M_n^1(x_n)$$
$$N^2(\alpha_1,\ldots,\alpha_i)M_{i+1}^2(x_{i+1})\cdots M_n^2(x_n)\big)_{(1,1)}$$

Every restriction determined by N^1, N^2 that have w^2 entries.

WARM-UP: 2-PASS ABP

Same as ROABP but with two "passes":

x_1	x_2	$\cdots$	x_{n-1}	x_n	x_1	x_2	$\cdots$	x_{n-1}	x_n

$$f = \left(M_1^1(x_1)M_2^1(x_2)\cdots M_n^1(x_n)\cdot M_1^2(x_1)M_2^2(x_2)\cdots M_n^2(x_n)\right)_{(1,1)}$$

Fixing $x_1, x_2, \ldots, x_i$:

$$f|_{\mathbf{x}_{[i]}=\alpha} = \big(N^1(\alpha_1,\ldots,\alpha_i)M_{i+1}^1(x_{i+1})\cdots M_n^1(x_n)$$
$$N^2(\alpha_1,\ldots,\alpha_i)M_{i+1}^2(x_{i+1})\cdots M_n^2(x_n)\big)_{(1,1)}$$

Every restriction determined by N^1, N^2 that have w^2 entries.
So eval-dim$_{[i],\overline{[i]}}(f) \leq w^4$.

WARM-UP: 2-PASS ABP

Same as ROABP but with two “passes”:

x_1	x_2	$\cdots$	x_{n-1}	x_n	x_1	x_2	$\cdots$	x_{n-1}	x_n

$$f = \left(M_1^1(x_1)M_2^1(x_2)\cdots M_n^1(x_n)\cdot M_1^2(x_1)M_2^2(x_2)\cdots M_n^2(x_n)\right)_{(1,1)}$$

Fixing $x_1, x_2, \ldots, x_i$:

$$f|_{\mathbf{x}_{[i]}=\alpha} = \Big(N^1(\alpha_1,\ldots,\alpha_i)M_{i+1}^1(x_{i+1})\cdots M_n^1(x_n)$$
$$N^2(\alpha_1,\ldots,\alpha_i)M_{i+1}^2(x_{i+1})\cdots M_n^2(x_n)\Big)_{(1,1)}$$

Every restriction determined by N^1, N^2 that have w^2 entries.
So eval-dim$_{[i],\overline{[i]}}(f) \le w^4$. $\implies$ f has width w^4 ROABP.

GENERALIZE: k-PASS ABP

Theorem: If f is computed by a width-w k-pass ABP in variable order $x_1, x_2, \ldots, x_n$, then for every $i \in [n]$, eval-dim$_{[i],\overline{[i]}}(f) \leq w^{2k}$.

GENERALIZE: k-PASS ABP

Theorem: If f is computed by a width-w k-pass ABP in variable order $x_1, x_2, \ldots, x_n$, then for every $i \in [n]$, eval-dim$_{[i],\overline{[i]}}(f) \leq w^{2k}$.

In particular, f is computed by a ROABP of width w^{2k}.

GENERALIZE: k-PASS ABP

Theorem: If f is computed by a width-w k-pass ABP in variable order $x_1, x_2, \ldots, x_n$, then for every $i \in [n]$, eval-dim$_{[i],\overline{[i]}}(f) \leq w^{2k}$.

In particular, f is computed by a ROABP of width w^{2k}.

$\implies$ Exp. lower bounds and quasi-poly PIT for k-pass ABPs.

GENERALIZE: k-PASS ABP

Theorem: If f is computed by a width-w k-pass ABP in variable order $x_1, x_2, \ldots, x_n$, then for every $i \in [n]$, eval-dim$_{[i],\overline{[i]}}(f) \leq w^{2k}$.

In particular, f is computed by a ROABP of width w^{2k}.

$\implies$ Exp. lower bounds and quasi-poly PIT for k-pass ABPs.

Up next: 2-pass, different order.

GENERALIZE: k-PASS ABP

Theorem: If f is computed by a width-w k-pass ABP in variable order $x_1, x_2, \ldots, x_n$, then for every $i \in [n]$, eval-dim$_{[i],\overline{[i]}}(f) \leq w^{2k}$.

In particular, f is computed by a ROABP of width w^{2k}.

$\Longrightarrow$ Exp. lower bounds and quasi-poly PIT for k-pass ABPs.

Up next: 2-pass, different order.

this is already exponentially more powerful than ROABPs and even sums of ROABPs:

GENERALIZE: k-PASS ABP

Theorem: If f is computed by a width-w k-pass ABP in variable order $x_1, x_2, \ldots, x_n$, then for every $i \in [n]$, eval-dim$_{[i],\overline{[i]}}(f) \leq w^{2k}$.

In particular, f is computed by a ROABP of width w^{2k}.

$\implies$ Exp. lower bounds and quasi-poly PIT for k-pass ABPs.

Up next: 2-pass, different order.

this is already exponentially more powerful than ROABPs and even sums of ROABPs: ∃ a polynomial computed by a 2-pass ABP with different orders that requires exponential width when computed as a sum of ROABPs.

2-PASS, DIFFERENT ORDER

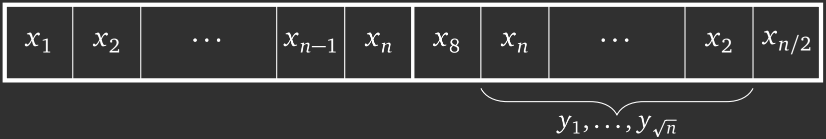
x_1	x_2	$\cdots$	x_{n-1}	x_n	x_8	x_n	$\cdots$	x_2	$x_{n/2}$

2-PASS, DIFFERENT ORDER

x_1	x_2	$\cdots$	x_{n-1}	x_n	x_8	x_n	$\cdots$	x_2	$x_{n/2}$

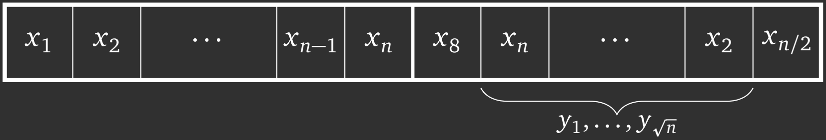
Theorem [Erdős-Szekeres]**:** Every sequence of n integers has a monotone subsequence of length $\sqrt{n}$.

2-PASS, DIFFERENT ORDER



Theorem [Erdős-Szekeres]: Every sequence of n integers has a monotone subsequence of length $\sqrt{n}$.

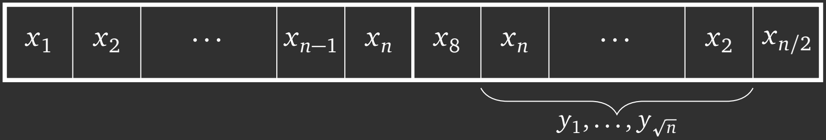
2-PASS, DIFFERENT ORDER



Theorem [Erdős-Szekeres]: Every sequence of n integers has a monotone subsequence of length $\sqrt{n}$.

Think of the ABP as computing a polynomial in the $\mathbf{y}$ vars over $\mathbb{F}(\overline{\mathbf{y}})$ (i.e. all others vars are now "constants")

2-PASS, DIFFERENT ORDER

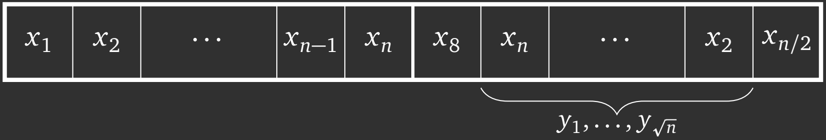


Theorem [Erdős-Szekeres]: Every sequence of n integers has a monotone subsequence of length $\sqrt{n}$.

Think of the ABP as computing a polynomial in the $\mathbf{y}$ vars over $\mathbb{F}(\bar{\mathbf{y}})$ (i.e. all others vars are now "constants")

What you get is a 2-pass ABP over $\mathbf{y}$ vars.

2-PASS, DIFFERENT ORDER



Theorem **[Erdős-Szekeres]:** Every sequence of n integers has a monotone subsequence of length $\sqrt{n}$.

Think of the ABP as computing a polynomial in the $\mathbf{y}$ vars over $\mathbb{F}(\overline{\mathbf{y}})$ (i.e. all others vars are now "constants")

What you get is a 2-pass ABP over $\mathbf{y}$ vars. In other words, ignoring $\overline{\mathbf{y}}$, for every $i \in [\sqrt{n}]$, eval-dim$_{[i],\overline{[i]}}(f) \leq w^4$.

PIT FOR 2-PASS, DIFFERENT ORDER

PIT algorithm:

PIT FOR 2-PASS, DIFFERENT ORDER

PIT algorithm:

1. Find monotone subsequence $\mathbf{y}$ of length $\sqrt{n}$

PIT for 2-pass, different order

PIT algorithm:

1. Find monotone subsequence $\mathbf{y}$ of length $\sqrt{n}$
2. Plug-in hitting set for width w^4 ROABPs to $\mathbf{y}$

PIT for 2-pass, different order

PIT algorithm:

1. Find monotone subsequence $\mathbf{y}$ of length $\sqrt{n}$
2. Plug-in hitting set for width w^4 ROABPs to $\mathbf{y}$
3. Repeat with $\bar{\mathbf{y}}$
   (plugging in a fresh copy of the hitting set each time)

PIT for 2-pass, different order

PIT algorithm:

1. Find monotone subsequence $\mathbf{y}$ of length $\sqrt{n}$
2. Plug-in hitting set for width w^4 ROABPs to $\mathbf{y}$
3. Repeat with $\bar{\mathbf{y}}$
   (plugging in a fresh copy of the hitting set each time)

PIT FOR 2-PASS, DIFFERENT ORDER

PIT algorithm:

1. Find monotone subsequence $\mathbf{y}$ of length $\sqrt{n}$
2. Plug-in hitting set for width w^4 ROABPs to $\mathbf{y}$
3. Repeat with $\bar{\mathbf{y}}$
   (plugging in a fresh copy of the hitting set each time)

PIT FOR 2-PASS, DIFFERENT ORDER

PIT algorithm:

1. Find monotone subsequence $\mathbf{y}$ of length $\sqrt{n}$
2. Plug-in hitting set for width w^4 ROABPs to $\mathbf{y}$
3. Repeat with $\bar{\mathbf{y}}$
   (plugging in a fresh copy of the hitting set each time)

PIT for 2-pass, different order

PIT algorithm:

1. Find monotone subsequence $\mathbf{y}$ of length $\sqrt{n}$
2. Plug-in hitting set for width w^4 ROABPs to $\mathbf{y}$
3. Repeat with $\overline{\mathbf{y}}$
   (plugging in a fresh copy of the hitting set each time)

PIT FOR 2-PASS, DIFFERENT ORDER

PIT algorithm:

1. Find monotone subsequence $\mathbf{y}$ of length $\sqrt{n}$
2. Plug-in hitting set for width w^4 ROABPs to $\mathbf{y}$
3. Repeat with $\bar{\mathbf{y}}$
   (plugging in a fresh copy of the hitting set each time)

PIT FOR 2-PASS, DIFFERENT ORDER

PIT algorithm:

1. Find monotone subsequence $\mathbf{y}$ of length $\sqrt{n}$
2. Plug-in hitting set for width w^4 ROABPs to $\mathbf{y}$
3. Repeat with $\bar{\mathbf{y}}$
   (plugging in a fresh copy of the hitting set each time)

Running Time: In total, $\approx \sqrt{n}$ copies of a $n^{\log n}$ size hitting set
$\implies \approx n^{\sqrt{n}}$

PIT for 2-pass, different order

PIT algorithm:

1. Find monotone subsequence $\mathbf{y}$ of length $\sqrt{n}$
2. Plug-in hitting set for width w^4 ROABPs to $\mathbf{y}$
3. Repeat with $\bar{\mathbf{y}}$
   (plugging in a fresh copy of the hitting set each time)

Running Time: In total, $\approx \sqrt{n}$ copies of a $n^{\log n}$ size hitting set $\implies \approx n^{\sqrt{n}}$

Naturally generalizes to k passes with different orders.

PIT FOR k-PASS, DIFFERENT ORDERS

By repeatedly applying the Erdős-Szekeres theorem, we can find a subsequence of size $n^{1/2^{k-1}}$ which is monotone in each of the k passes.

PIT for k-pass, different orders

By repeatedly applying the Erdős-Szekeres theorem, we can find a subsequence of size $n^{1/2^{k-1}}$ which is monotone in each of the k passes.

PIT for k-pass, different orders

By repeatedly applying the Erdős-Szekeres theorem, we can find a subsequence of size $n^{1/2^{k-1}}$ which is monotone in each of the k passes.

Same algorithm gives $n^{n^{1-1/2^{k-1}}}$ hitting set.

PIT FOR k-PASS, DIFFERENT ORDERS

By repeatedly applying the Erdős-Szekeres theorem, we can find a subsequence of size $n^{1/2^{k-1}}$ which is monotone in each of the k passes.

Same algorithm gives $n^{n^{1-1/2^{k-1}}}$ hitting set.

This is still not a general read-k oblivious ABP!

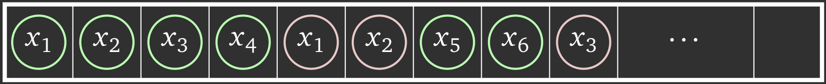
READ-TWICE OBLIVIOUS ABPS

READ-TWICE OBLIVIOUS ABPS

Begin by applying Erdős-Szekeres.

READ-TWICE OBLIVIOUS ABPS

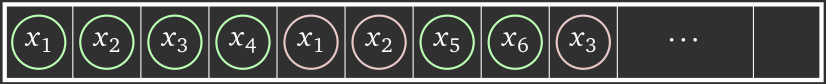
Begin by applying Erdős-Szekeres.



Monotone sequences are not disjoint...

READ-TWICE OBLIVIOUS ABPS

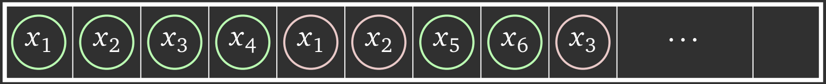
Begin by applying Erdős-Szekeres.



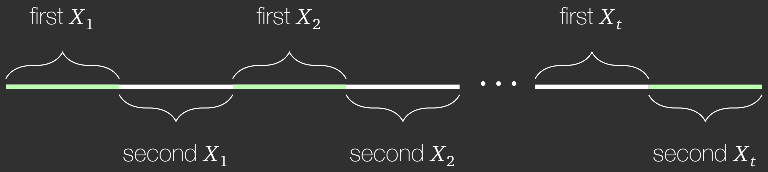
Monotone sequences are not disjoint...
BUT we can find a large set of the variables such that the resulting sequence is “regularly-interleaving”:

READ-TWICE OBLIVIOUS ABPS

Begin by applying Erdős-Szekeres.



Monotone sequences are not disjoint...
BUT we can find a large set of the variables such that the resulting sequence is “regularly-interleaving”:



REGULARLY INTERLEAVING SUBSEQUENCES

This structure is enough to carry out the original argument: with respect to the variables $\mathbf{y}$ in the regularly interleaving sequence ($|\mathbf{y}| \approx \sqrt{n}$), the evaluation dimension is at most w^4.

REGULARLY INTERLEAVING SUBSEQUENCES

This structure is enough to carry out the original argument: with respect to the variables $\mathbf{y}$ in the regularly interleaving sequence ($|\mathbf{y}| \approx \sqrt{n}$), the evaluation dimension is at most w^4.

Generalizes to read-k: apply Erdős-Szekeres to every sequence and make every pair regularly-interleaving.

Wrap-up: PIT algorithm with running time $\exp(n^{1-1/2^{k-1}})$ for read-k oblivious ABPs.

LOWER BOUNDS FOR READ-k

- These arguments are sufficient to get a lower bound of roughly $\exp(n^{1/2^k})$

LOWER BOUNDS FOR READ-k

- These arguments are sufficient to get a lower bound of roughly $\exp(n^{1/2^k})$
- But actually, for a lower bound we don't need to show that for every prefix $[i]$ the eval-dimension is small: it's enough to show it is small for some prefix $[i]$

LOWER BOUNDS FOR READ-k

- These arguments are sufficient to get a lower bound of roughly $\exp(n^{1/2^k})$
- But actually, for a lower bound we don't need to show that for every prefix $[i]$ the eval-dimension is small: it's enough to show it is small for some prefix $[i]$
- That is, to show that if f is computed by a read-k oblivious ABP, then there is i such that eval-dim$_{[i],\overline{[i]}}(f) \leq w^{2k}$

LOWER BOUNDS FOR READ-k

- These arguments are sufficient to get a lower bound of roughly $\exp(n^{1/2^k})$
- But actually, for a lower bound we don't need to show that for every prefix $[i]$ the eval-dimension is small: it's enough to show it is small for some prefix $[i]$
- That is, to show that if f is computed by a read-k oblivious ABP, then there is i such that eval-dim$_{[i],\overline{[i]}}(f) \leq w^{2k}$
- This is very close to being true

EXPONENTIAL LOWER BOUND

Claim: We can fix $n/10$ variables and partition the remaining to subsets S, T with $|S|, |T| \geq n/k^k$ and eval-dim$_{S,T}(f) \leq w^{2k}$

Exponential Lower Bound

Claim: We can fix $n/10$ variables and partition the remaining to subsets S, T with $|S|, |T| \geq n/k^k$ and eval-dim$_{S,T}(f) \leq w^{2k}$

Proof: Partition program into r contiguous blocks.

EXPONENTIAL LOWER BOUND

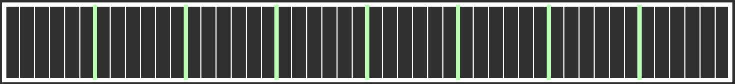
Claim: We can fix $n/10$ variables and partition the remaining to subsets S, T with $|S|,|T| \geq n/k^k$ and eval-dim$_{S,T}(f) \leq w^{2k}$

Proof: Partition program into r contiguous blocks.

EXPONENTIAL LOWER BOUND

Claim: We can fix $n/10$ variables and partition the remaining to subsets S, T with $|S|, |T| \geq n/k^k$ and eval-dim$_{S,T}(f) \leq w^{2k}$

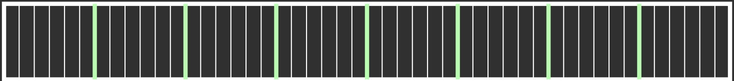
Proof: Partition program into r contiguous blocks.



EXPONENTIAL LOWER BOUND

Claim: We can fix $n/10$ variables and partition the remaining to subsets S, T with $|S|, |T| \geq n/k^k$ and eval-dim$_{S,T}(f) \leq w^{2k}$

Proof: Partition program into r contiguous blocks.

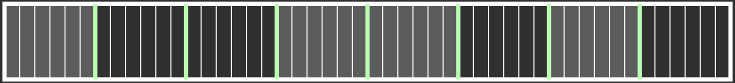


By averaging, $\exists k$ blocks that contain all reads of $n/\binom{r}{k}$ vars.

EXPONENTIAL LOWER BOUND

Claim: We can fix $n/10$ variables and partition the remaining to subsets S, T with $|S|, |T| \geq n/k^k$ and eval-dim$_{S,T}(f) \leq w^{2k}$

Proof: Partition program into r contiguous blocks.

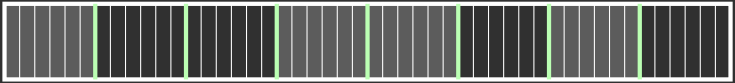


By averaging, $\exists k$ blocks that contain all reads of $n/\binom{r}{k}$ vars.

EXPONENTIAL LOWER BOUND

Claim: We can fix $n/10$ variables and partition the remaining to subsets S, T with $|S|, |T| \geq n/k^k$ and eval-dim$_{S,T}(f) \leq w^{2k}$

Proof: Partition program into r contiguous blocks.

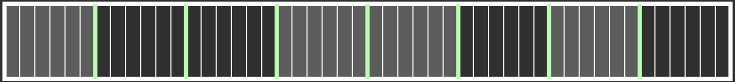


By averaging, $\exists k$ blocks that contain all reads of $n/\binom{r}{k}$ vars. Call them S and fix all other vars in those blocks.

EXPONENTIAL LOWER BOUND

Claim: We can fix $n/10$ variables and partition the remaining to subsets S, T with $|S|, |T| \geq n/k^k$ and eval-dim$_{S,T}(f) \leq w^{2k}$

Proof: Partition program into r contiguous blocks.



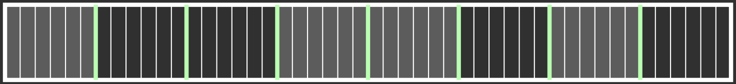
By averaging, $\exists k$ blocks that contain all reads of $n/\binom{r}{k}$ vars. Call them S and fix all other vars in those blocks.

$T =$ all remaining variables. Now compute eval-dim$_{S,T}$ using previous arguments.

EXPONENTIAL LOWER BOUND

Claim: We can fix $n/10$ variables and partition the remaining to subsets S, T with $|S|, |T| \geq n/k^k$ and eval-dim$_{S,T}(f) \leq w^{2k}$

Proof: Partition program into r contiguous blocks.



By averaging, $\exists k$ blocks that contain all reads of $n/\binom{r}{k}$ vars. Call them S and fix all other vars in those blocks.

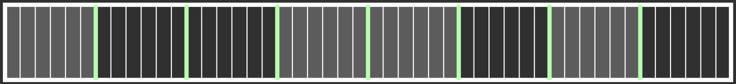
$T =$ all remaining variables. Now compute eval-dim$_{S,T}$ using previous arguments.

if $r = 10k^2$ we fix at most $n/10$ vars and $|S| \geq n/k^k$.

EXPONENTIAL LOWER BOUND

Claim: We can fix $n/10$ variables and partition the remaining to subsets S, T with $|S|,|T| \geq n/k^k$ and eval-dim$_{S,T}(f) \leq w^{2k}$

Proof: Partition program into r contiguous blocks.



By averaging, $\exists k$ blocks that contain all reads of $n/\binom{r}{k}$ vars. Call them S and fix all other vars in those blocks.

$T =$ all remaining variables. Now compute eval-dim$_{S,T}$ using previous arguments.

if $r = 10k^2$ we fix at most $n/10$ vars and $|S| \geq n/k^k$.

what's left is to find a polynomial such that eval-dim$_{S,T} \geq 2^{\min\{|S|,|T|\}}$

SUMMARY

SUMMARY

Lower Bound: An $\exp(n/k^k)$ lower bound on any read-k oblivious ABP computing some polynomial $f \in$ VP.

SUMMARY

Lower Bound: An $\exp(n/k^k)$ lower bound on any read-k oblivious ABP computing some polynomial $f \in$ VP.

PIT: A white-box PIT algorithm for read-k oblivious ABPs, with running time $\exp(n^{1-1/2^{k-1}})$.

OPEN PROBLEMS

OPEN PROBLEMS

- Faster PIT algorithm

OPEN PROBLEMS

- Faster PIT algorithm
- A complete black-box test (no dependence on order)

OPEN PROBLEMS

- Faster PIT algorithm
- A complete black-box test (no dependence on order)
- "Tighter" lower bounds (e.g. a hierarchy theorem for read-k ABPs)

OPEN PROBLEMS

- Faster PIT algorithm
- A complete black-box test (no dependence on order)
- "Tighter" lower bounds (e.g. a hierarchy theorem for read-k ABPs)
- Non-oblivious? (open even for $k = 1$)

OPEN PROBLEMS

- Faster PIT algorithm
- A complete black-box test (no dependence on order)
- “Tighter” lower bounds (e.g. a hierarchy theorem for read-k ABPs)
- Non-oblivious? (open even for $k = 1$)
- Connections with pseudorandomness for boolean branching programs?

THANK YOU