Lower Bounds for Nondeterministic Semantic Read-Once Branching Programs

Stephen Cook, Jeff Edmonds, Venkatesh Medabalimi and Toniann Pitassi

July 13, 2016

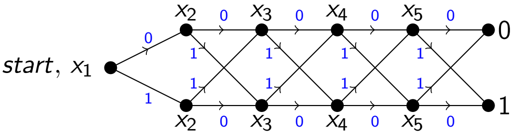
Branching Programs

$f(x_1, x_2, .., x_n) \to \{0, 1\}$ $\qquad$ $x_i \in \{0, 1\}, \forall i \in [n]$

Definition

Deterministic Branching program

- DAG with a source node and two sinks, 1-sink (for accept) and 0-sink (for reject).
- Each non-sink node is labeled by some x_i, outdegree 2 with an edge each for $x_i = 0$ and $x_i = 1$.

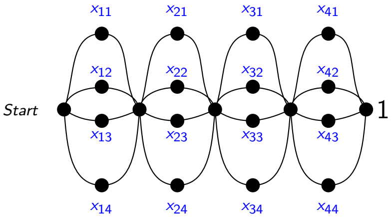


Non-det Branching Programs

Definition

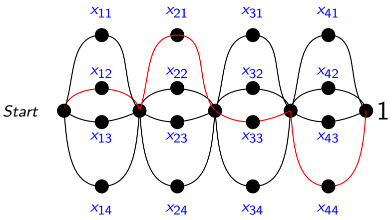
Non-deterministic Branching program (NBP)

- allow unlabelled guessing nodes and arbitrary out-degree.



The size of a NBP= number of labelled nodes.

NBP computing $f : \{0,1\}^n \to \{0,1\}$



$f(u) = 1 \quad \Longleftrightarrow \quad$ $\exists$ a path from source to accept node that is consistent with input u.

Program Size and Space Complexity of computing f

- $BP(f_n) = \min_{B \in \text{ NBP computing } f_n} \text{size}\,(B)$

- $S(f_n) = \min_{T \in \text{ non-uniform NTMs computing } f_n} \text{space complexity}\,(T)$

- $\log(BP(f_n)) \approx S(f_n)$ Cobham'66

Big Picture

- It is easy to show functions with high $S(f_n)$ exist.

Big Picture

- It is easy to show functions with high $S(f_n)$ exist.
- Can we show that some function in P requires exponential size NBP ?
  - amounts to showing NL $\subset$ P.

Big Picture

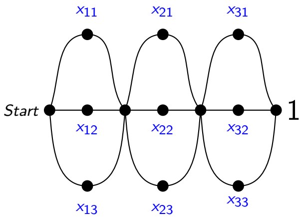
- It is easy to show functions with high $S(f_n)$ exist.
- Can we show that some function in P requires exponential size NBP ?
  - amounts to showing NL $\subset$ P.
- we study the simplest restricted setting that is not well understood.

Read Once

- *Syntactic* read once: Along any path from source to sink any variable appears atmost once.

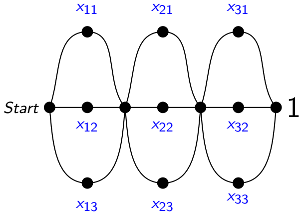
Read Once

- *Syntactic* read once: Along any path from source to sink any variable appears atmost once.



Read Once

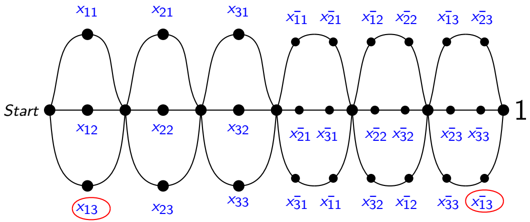
- *Syntactic* read once: Along any path from source to sink any variable appears atmost once.



- *Semantic* read once: Along any *consistent* path from source to sink no variable is read more than once.

Read Once

- *Syntactic* read once: Along any path from source to sink any variable appears atmost once.



- *Semantic* read once: Along any *consistent* path from source to sink no variable is read more than once.

Separating syntactic from semantic read once

The *Exact Perfect matching* function(EPM_n): accept a matrix iff it is a permutation matrix.

Jukna and Razborov '98 showed

Theorem

Every syntactic read once NBP computing EPM_n must have size $2^{\Omega(n)}$.

$EPM_n \in$ SEMANTIC READ ONCE

THEOREM (JUKNA)

EPM_n can be solved by a semantic read once NBP of size $O(n^3)$.

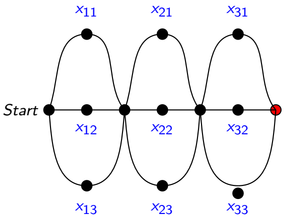
$$\begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$$

$EPM_n \in$ SEMANTIC READ ONCE

THEOREM (JUKNA)

EPM_n can be solved by a semantic read once NBP of size $O(n^3)$.

$$\begin{bmatrix} 0 & 0 & \cancel{1} \\ \cancel{1} & 0 & 0 \\ 0 & \cancel{1} & 0 \end{bmatrix}$$

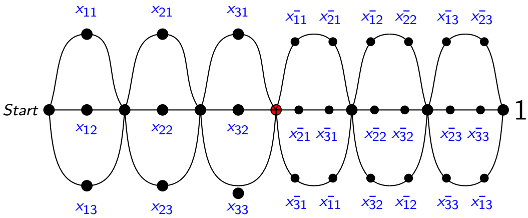


$EPM_n \in$ SEMANTIC READ ONCE

THEOREM (JUKNA)

EPM_n can be solved by a semantic read once NBP of size $O(n^3)$.

$$\begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$$

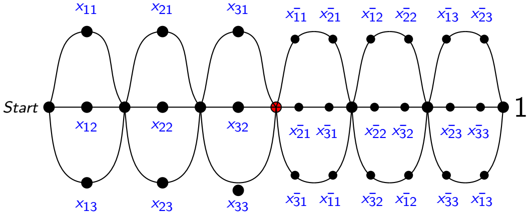


$EPM_n \in$ SEMANTIC READ ONCE

Theorem (Jukna)

EPM_n can be solved by a semantic read once NBP of size $O(n^3)$.

$$\begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$$



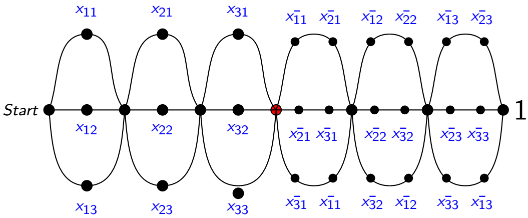
Sees only 1s

$EPM_n \in$ SEMANTIC READ ONCE

Theorem (Jukna)

EPM_n can be solved by a semantic read once NBP of size $O(n^3)$.

$$\begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$$



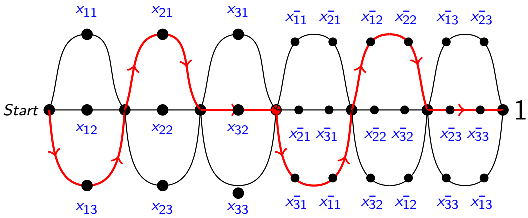
Sees only 1s Sees only 0s

$EPM_n \in$ SEMANTIC READ ONCE

Theorem (Jukna)

EPM_n can be solved by a semantic read once NBP of size $O(n^3)$.

$$\begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$$



Sees only 1s   Sees only 0s

Open Problem

Exponential lower bounds for
semantic read once Boolean NBP
are not yet known !

Our Contribution

Exponential lower bounds for
semantic read once Ternary NBPs.

$$D = \{0,1,2\}$$

Times space tradeoffs

- $t \leq kn \implies s = 2^{\Omega(n)}$ Jukna'09
- implies a read once lower bound for semantic read once NBP but applicable for $|D| > 2^{13}$.
- Earlier results by Ajtai '99 and Beame,Jayram, Saks '01

Lower Bound for D=3

The hard function: $u_0 + u_1 x + u_2 x^2 + .. + u_d x^d$

Definition

$Poly_u(x)$

- $u \in [K]^{d+1}$ is the coefficient vector.
- $x \in \{0,1,2\}^n$ encodes an element in $[K]$.

Lower Bound for D=3

$$Poly_u(x) = \begin{cases} 1, & \text{if} \quad u_0 + u_1 x + u_2 x^2 + .. + u_d x^d < K^{1-\delta} \\ 0, & \text{otherwise} \end{cases}$$

Definition

$Poly_u(x)$

- $u \in [K]^{d+1}$ is the coefficient vector.
- $x \in \{0,1,2\}^n$ encodes an element in $[K]$.
- accept $x \iff Poly(u,x) < K^{1-\delta}$.

Lower Bound for D=3

Theorem

For sufficiently large n, there exists u such that any 3-ary nondeterministic semantic read-once branching program for $Poly_u(x)$ requires size at least $2^{\Omega(n)}$.

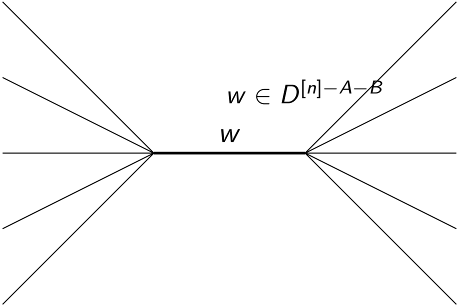
Proof Overview

- A small BP for a *dense, sensitive* f (★) $\Longrightarrow$ f accepts an r by r *balanced rectangle*.

Proof Overview

- A small BP for a *dense, sensitive* f ($\bigstar$) $\Longrightarrow$ f accepts an r by r *balanced rectangle*.
- Polynomials are dense ($\bigstar$) w.h.p
- $\exists$ many u for which $Poly_u(x)$ doesn't accept any r by r balanced rectangle.

Embedded Rectangles $C_{red} \times \{w\} \times C_{blue} \subseteq [D]^n$

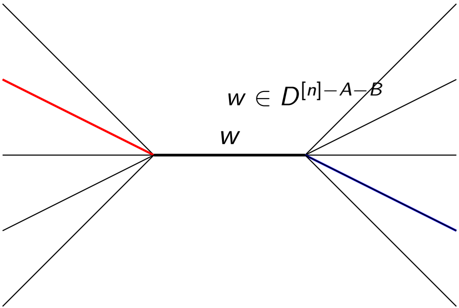


$C_{red} \subseteq D^A$ $\quad$ $C_{blue} \subseteq D^B$

$A \subset [n]$ $\quad$ $B \subset [n]$

$$\left\{\begin{array}{c} 012210101 \\ 012010201 \\ 101012202 \end{array}\right\} \times \{10210001\} \times \left\{\begin{array}{c} 012001012 \\ 201101002 \\ 110020120 \\ 210200120 \end{array}\right\}$$

Embedded Rectangles $C_{red} \times \{w\} \times C_{blue} \subseteq [D]^n$

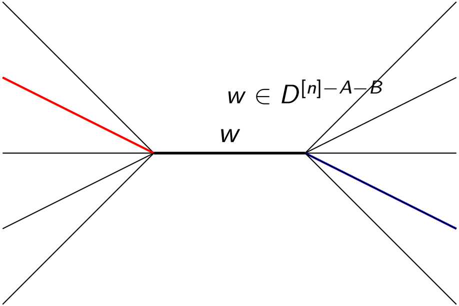


$C_{red} \subseteq D^A$ $\qquad$ $C_{blue} \subseteq D^B$

$A \subset [n]$ $\qquad$ $B \subset [n]$

$$\left\{\begin{matrix} 012210101 \\ \color{red}{012010201} \\ 101012202 \end{matrix}\right\} \times \{102101\} \times \left\{\begin{matrix} 012001012 \\ 201101002 \\ \color{blue}{110020120} \\ 210200120 \end{matrix}\right\}$$

Embedded Rectangles
$C_{red} \times \{w\} \times C_{blue} \subseteq [D]^n$

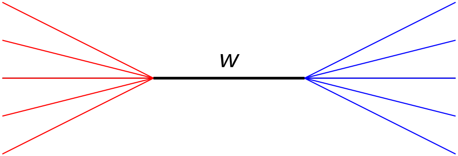


$C_{red} \subseteq D^A$ $\quad$ $C_{blue} \subseteq D^B$

$A \subset [n]$ $\quad$ $B \subset [n]$

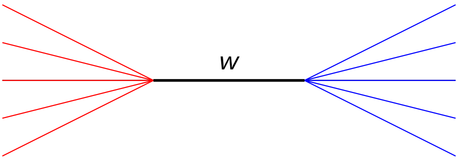
$$\left\{ \begin{matrix} 012210101 \\ \color{red}{012010201} \\ 101012202 \end{matrix} \right\} \times \{102101\} \times \left\{ \begin{matrix} 012001012 \\ 201101002 \\ \color{blue}{110020120} \\ 210200120 \end{matrix} \right\}$$

An $r \times r$ balanced embedded rectangle



$|C_{red}| = r$ $|C_{blue}| = r$

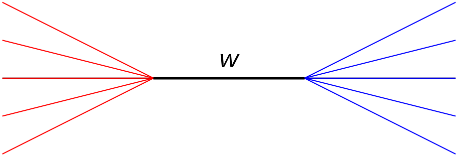
An $r \times r$ balanced embedded rectangle



$|C_{red}| = r$ $\quad$ $|C_{blue}| = r$

$$|C_{red} \times \{w\} \times C_{blue}| = r^2$$

An $r \times r$ balanced embedded rectangle



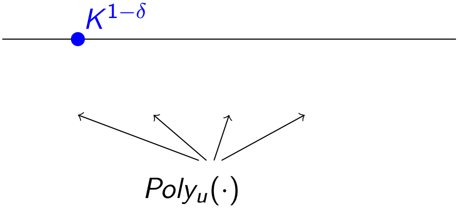
$|C_{red}| = r$ $\qquad$ $|C_{blue}| = r$

$$|C_{red} \times \{w\} \times C_{blue}| = r^2$$

$\mathcal{R}_{m,r}$ be the set of all balanced embedded rectangles.

$$|\mathcal{R}_{m,r}| \approx |D|^{O(mr)}$$

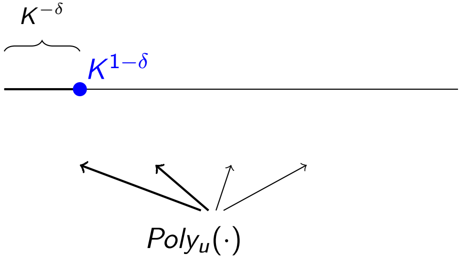
Most low degree Polynomials have close to uniform spread, hence dense



Lemma (w.h.p $Poly_u()$ is dense)

For a random u, for fixed d, δ the probability that $Poly_u(\cdot)$ does not accept a $(1 \pm o(1))K^{-\delta}$ fraction of all the inputs is at most $o(1)$.

Most low degree Polynomials have close to uniform spread, hence dense



Lemma (w.h.p $Poly_u()$ is dense)

For a random u, for fixed d, δ the probability that $Poly_u(\cdot)$ does not accept a $(1 \pm o(1))K^{-\delta}$ fraction of all the inputs is at most $o(1)$.

Make BP query every variable

f is sensitive if any two accepting instances differ in at least two coordinates.

Make BP query every variable

f is sensitive if any two accepting instances differ in at least two coordinates.

$$h_a(x) = 1 \text{ iff } x_1 + x_2 + \ldots + x_n = a \mod 3$$

Make BP query every variable

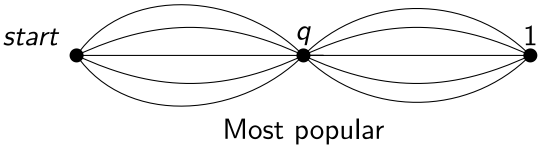
f is sensitive if any two accepting instances differ in at least two coordinates.

$$h_a(x) = 1 \text{ iff } x_1 + x_2 + \ldots + x_n = a \mod 3$$

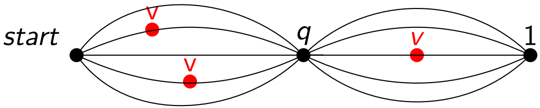
Fix an $a(u)$ for which h_a overlaps with most instances in $Poly_u^{-1}(1)$.

$$f_u(x) = Poly_u(x) \wedge h_{a(u)}(x)$$

Few states midway $\Longrightarrow$ balanced embedded rectangle



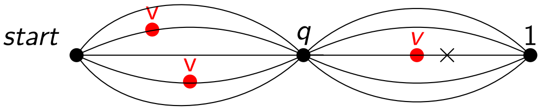
FEW STATES MIDWAY $\implies$ BALANCED EMBEDDED RECTANGLE



Most popular

- Choose a popular red variable.

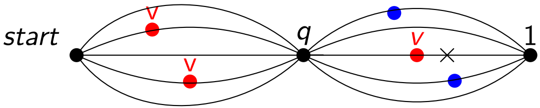
FEW STATES MIDWAY $\Longrightarrow$ BALANCED EMBEDDED RECTANGLE



Most popular

- Choose a popular red variable. Prune the input set. Continue to choose $m_r = c_1 n$ red variables for A.

FEW STATES MIDWAY $\Longrightarrow$ BALANCED EMBEDDED RECTANGLE

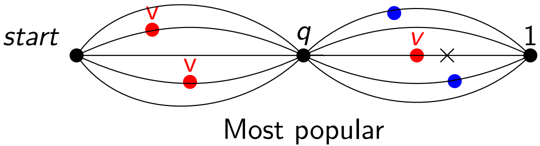


Most popular

- Choose a popular red variable. Prune the input set. Continue to choose $m_r = c_1 n$ red variables for A.

- Choose $m_b = 4m_r$ popular blue variables, B.

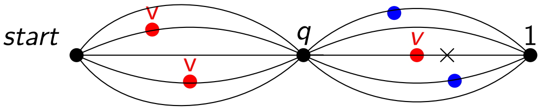
FEW STATES MIDWAY $\Longrightarrow$ BALANCED EMBEDDED RECTANGLE



- Choose a popular red variable. Prune the input set. Continue to choose $m_r = c_1 n$ red variables for A.

- Choose $m_b = 4m_r$ popular blue variables, B.
- Fix the remaining variables in $[n]$-A-B to the most popular projection 'w'.

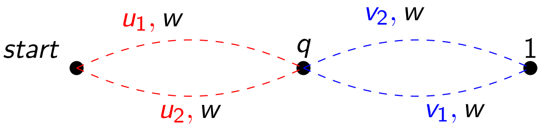
Few states midway $\implies$ balanced embedded rectangle



Most popular

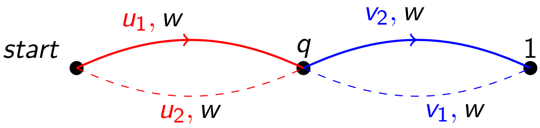
- Choose a popular red variable. Prune the input set. Continue to choose $m_r = c_1 n$ red variables for A.
- Remove vectors with few red extensions.($i.e \leq r$).
- Choose $m_b = 4m_r$ popular blue variables, B.
- Fix the remaining variables in $[n]$-A-B to the most popular projection 'w'.

Why is it a rectangle ?



$$(u_1, w, v_1), (u_2, w, v_2) \in I \implies (u_1, w, v_2), (u_2, w, v_1) \in I$$

Why is it a rectangle ?



$$(u_1, w, v_1), (u_2, w, v_2) \in I \implies (u_1, w, v_2), (u_2, w, v_1) \in I$$

A BALANCED RECTANGLE BELONGS TO FEW POLYNOMIALS.

- $|\mathcal{R}_{m,r}| \approx |D|^{O(mr)}$.

A BALANCED RECTANGLE BELONGS TO FEW POLYNOMIALS.

- $|\mathcal{R}_{m,r}| \approx |D|^{O(mr)}$.
- Each $R \in \mathcal{R}_{m,r}$ can be a 1-rectangle in at most a $|D|^{-n\delta d}$ fraction of the polynomials. Choose degree $d = r^2$.

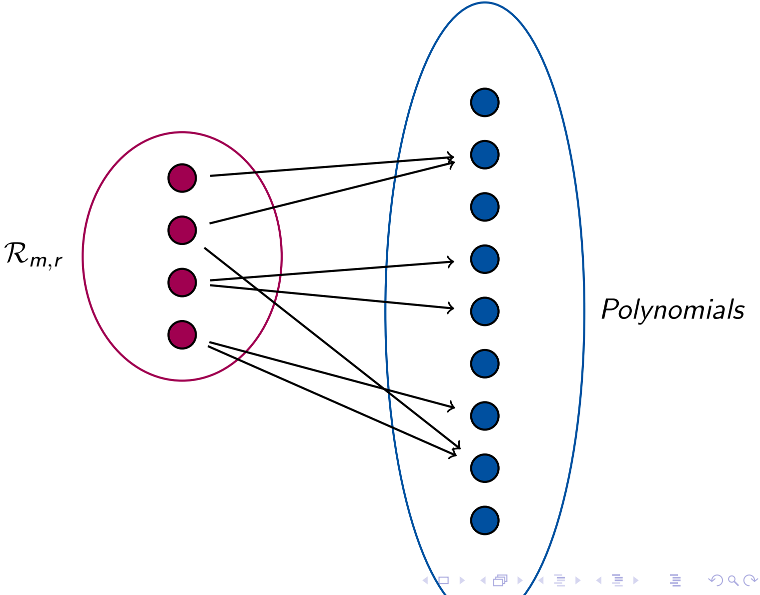
A BALANCED RECTANGLE BELONGS TO FEW POLYNOMIALS.

- $|\mathcal{R}_{m,r}| \approx |D|^{O(mr)}$.
- Each $R \in \mathcal{R}_{m,r}$ can be a 1-rectangle in at most a $|D|^{-n\delta d}$ fraction of the polynomials. Choose degree $d = r^2$.
- By union bound the probability that a random polynomial accepts any rectangle in $\mathcal{R}_{m,r}$ is

$$Prob(\ Poly_u(x) \supseteq R;\ \ R \in \mathcal{R}_{m,r})$$

$$\leq |\mathcal{R}_{m,r}| \frac{1}{|D|^{n\delta r^2}} \quad \approx \ |D|^{O(mr)} \frac{1}{|D|^{n\delta r^2}} \quad < 1$$

∃ Polynomial without a balanced rectangle



Almost there, but not quite, D=2 ?

showing a lower bound for semantic read once *boolean* NBP remains open !!

- Don't know if there exists a balanced rectangle as a consequence of BP for f being small.
- May be one can show there are other special looking sets(balanced cylinder intersections ?) that must appear in f.

Thank You !