ALGEBRAIC CIRCUIT LOWER BOUNDS

VIA MATRIX RANK

SRIKANTH SRINIVASAN

UNIV. OF COPENHAGEN

Algebraic / Arithmetic Circuit Complexity

→ Polynomial problems $(P_n)_{n \geq 1}$ $\deg(P_n) \leq n^{O(1)}$.

Input: $x_1, \ldots, x_n \in \mathbb{F}$

Output: $P_n(x_1, \ldots, x_n)$

Algebraic / Arithmetic Circuit Complexity

→ Polynomial problems $(P_n)_{n\geq 1}$ $\deg(P_n) \leq n^{O(1)}$.

Input: $x_1, \ldots, x_n \in \mathbb{F}$

Output: $P_n(x_1, \ldots, x_n)$

Eg: $\det_n$, per_n, Matrix-Mult, DFT

Algebraic / Arithmetic Circuit Complexity

→ Polynomial problems $(P_n)_{n\geq 1}$, $\deg(P_n) \leq n^{O(1)}$.

Input: $x_1, \ldots, x_n \in \mathbb{F}$

Output: $P_n(x_1, \ldots, x_n)$

Eg: $\det_n$, per_n, Matrix-Mult, DFT

→ Note: Algorithms must compute correctly on any input & typically, $|\mathbb{F}|$ large (eg. $\mathbb{C}$)

↳ not only Boolean.

Algebraic / Arithmetic Circuit Complexity

→ Polynomial problems $(P_n)_{n \geq 1}$, $\deg(P_n) \leq n^{O(1)}$.

Input: $x_1, \ldots, x_n \in \mathbb{F}$

Output: $P_n(x_1, \ldots, x_n)$

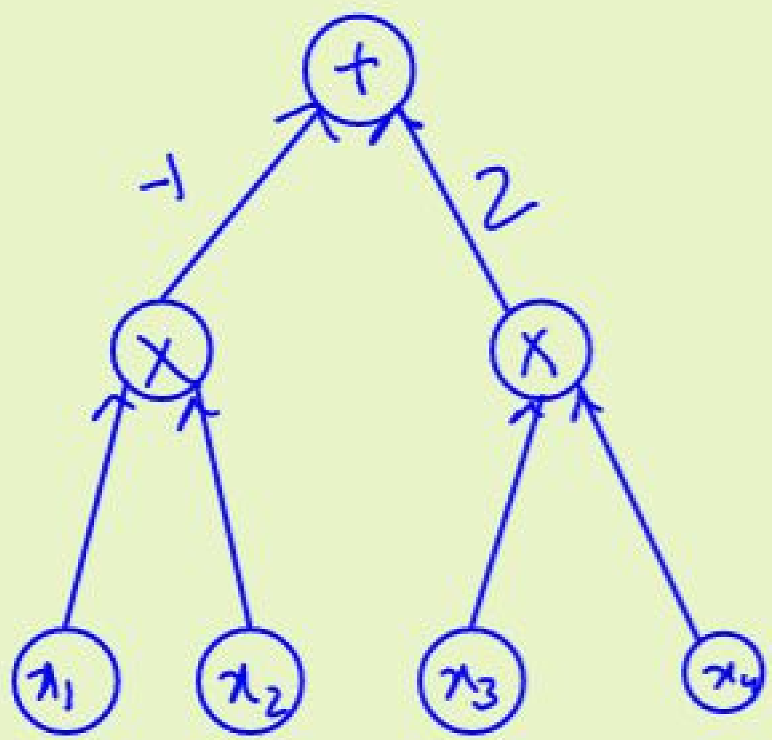
Eg: $\det_n$, per_n, Matrix-Mult, DFT

→ **Note**: Algorithms must compute correctly on **any** input & typically, $|\mathbb{F}|$ large (eg. $\mathbb{C}$)

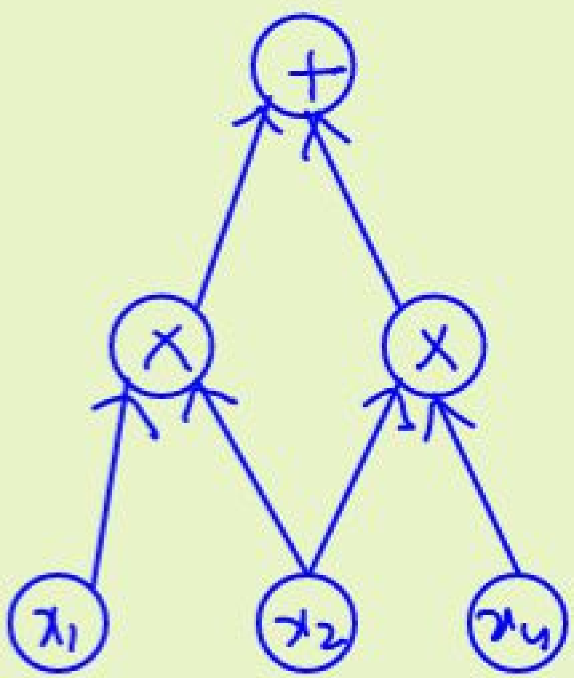
↳ not only Boolean.

→ Important to understand IPS.

Algebraic / Arithmetic Circuit Complexity

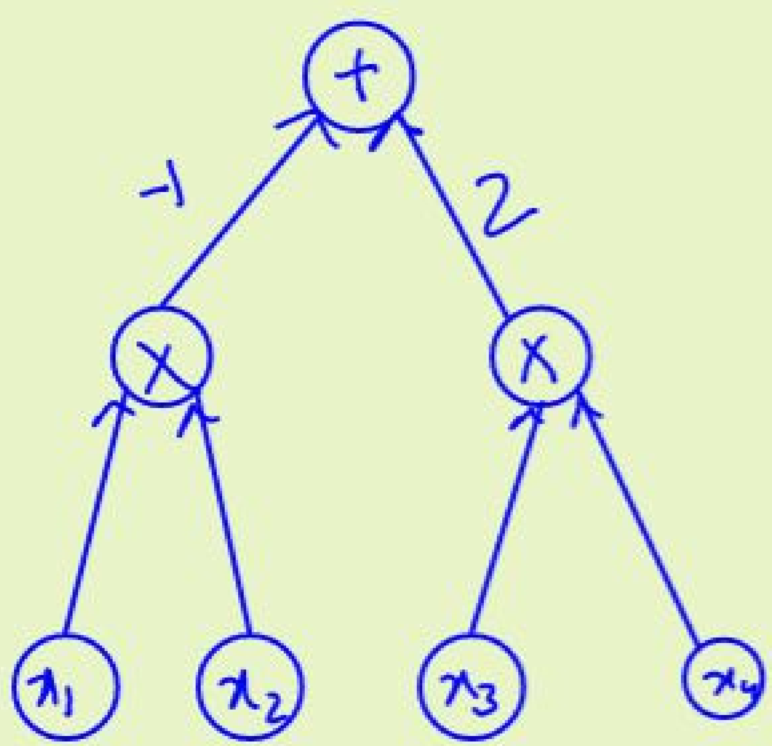


Algebraic formulas

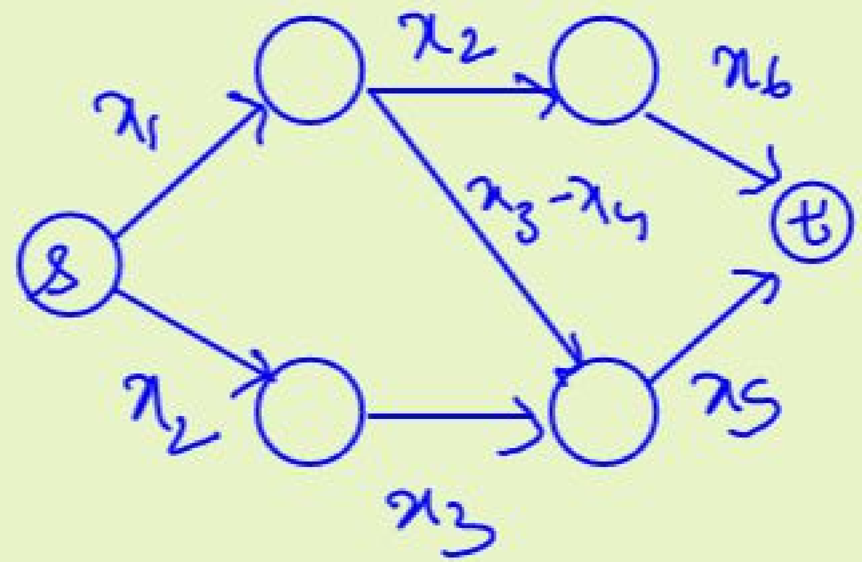


Algebraic Circuits

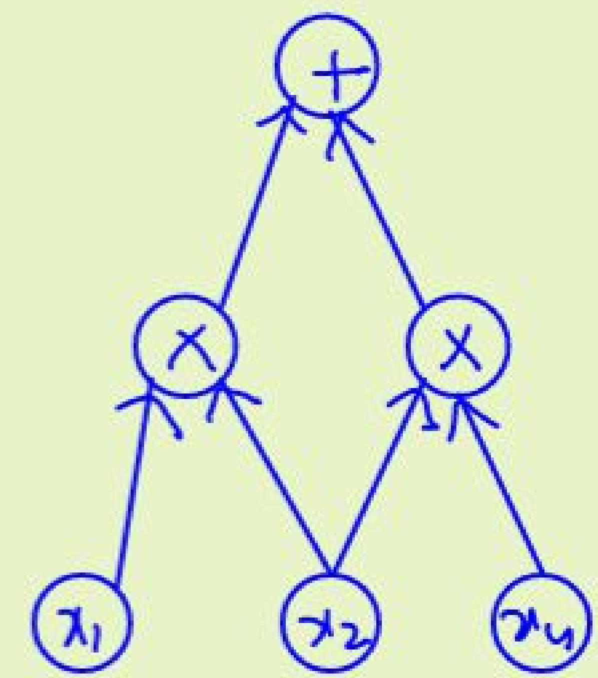
Algebraic / Arithmetic Circuit Complexity



Algebraic formulas

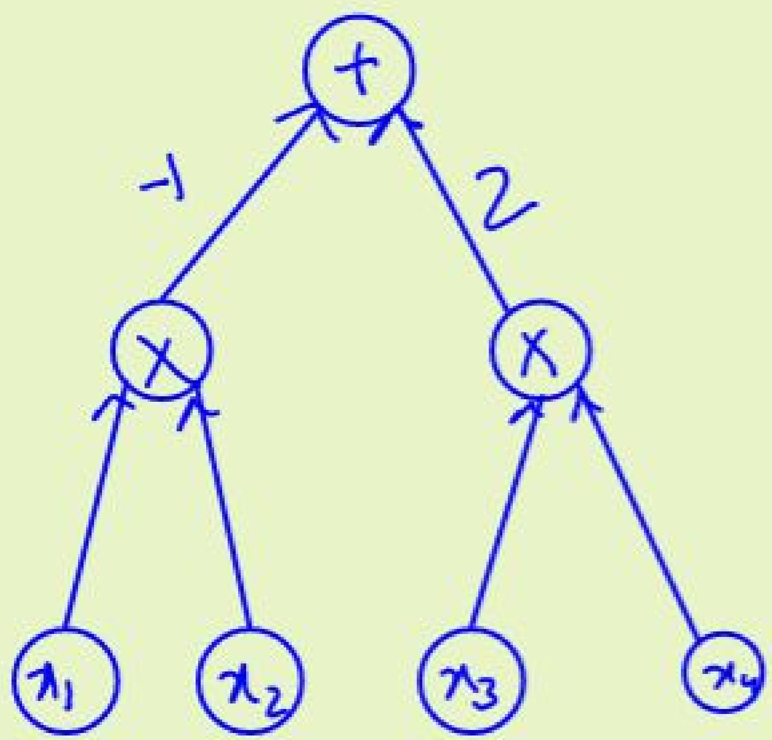


Algebraic Branching Programs

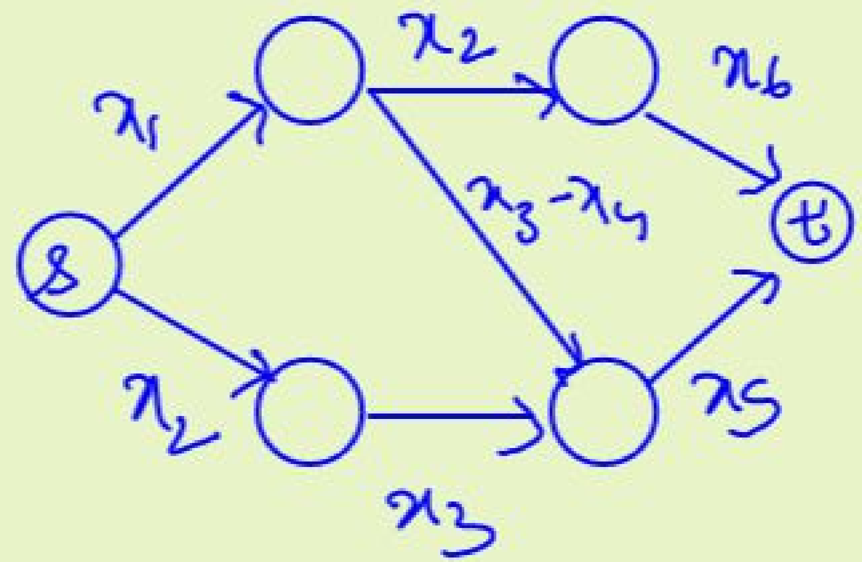


Algebraic Circuits

Algebraic / Arithmetic Circuit Complexity

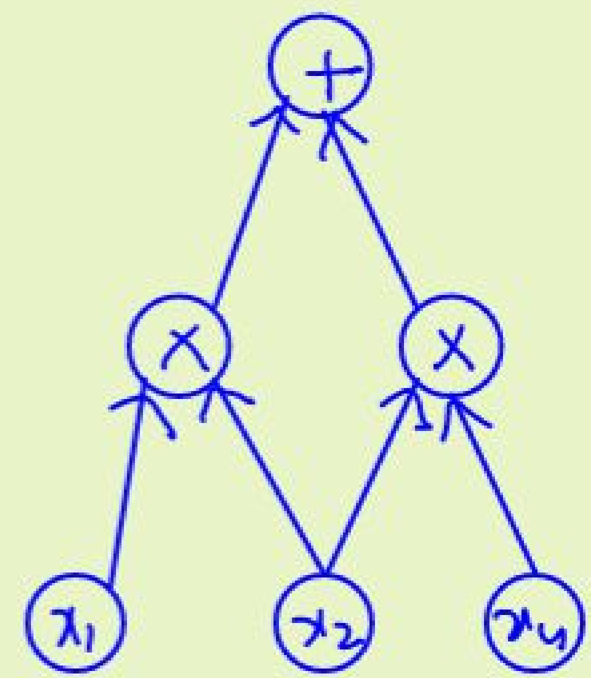


Algebraic formulas



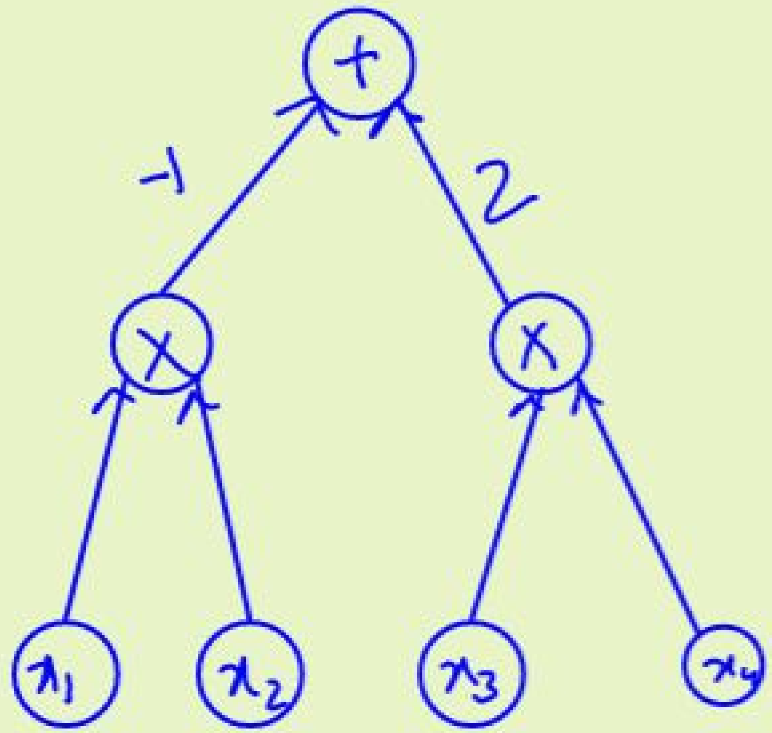
$$\sum_{p} \prod_{e \in p} w_e$$

Algebraic Branching Programs

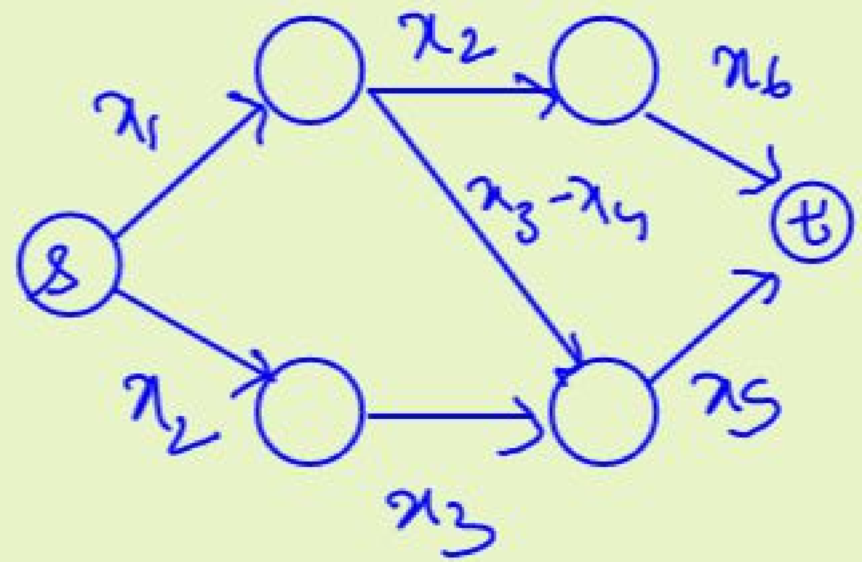


Algebraic Circuits

Algebraic /Arithmetic Circuit Complexity



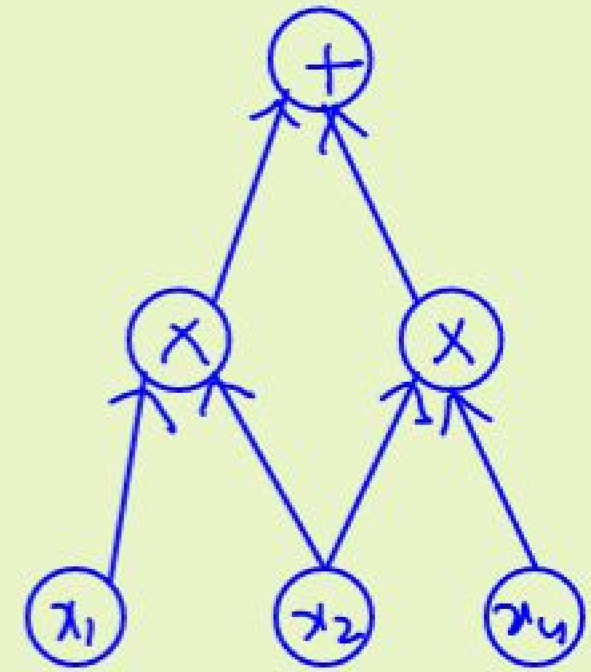
Algebraic formulas



$x_1 x_2 x_6 + x_2 x_3 x_5$

$+ x_1 (x_3 - x_4) x_5$

Algebraic Branching Programs



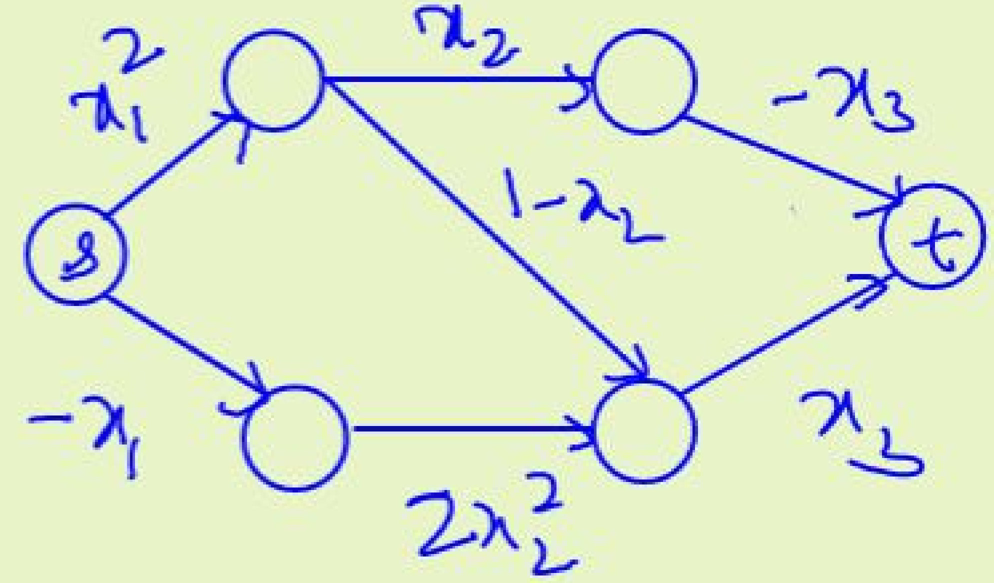
Algebraic Circuits

Algebraic /Arithmetic Circuit Complexity

Read-once Oblivious

Algebraic Branching Programs -

Each layer involves a distinct variable.



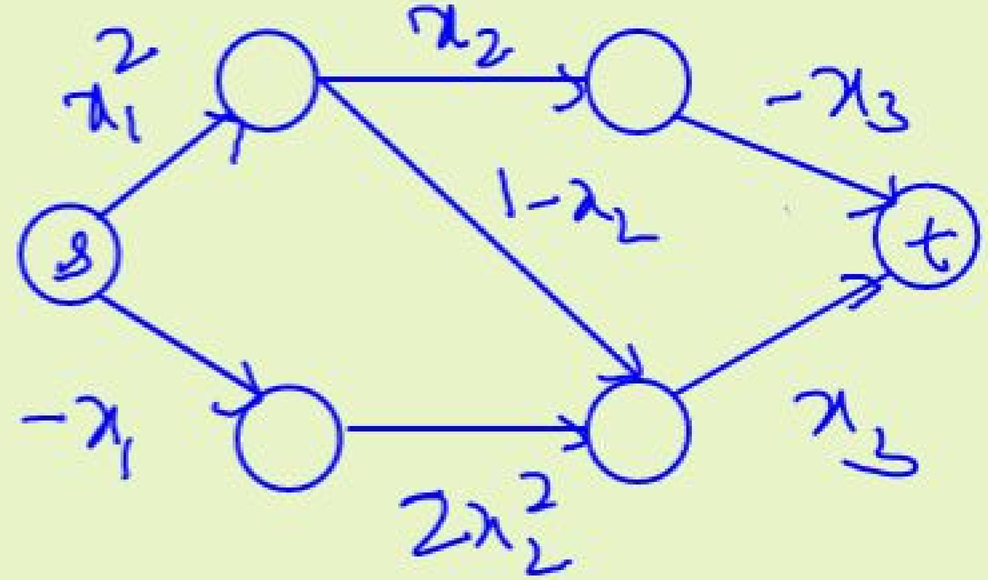
Algebraic / Arithmetic Circuit Complexity

Read-once Oblivious

Algebraic Branching Programs -

Each layer involves a distinct variable.

Weights - Univariate polys.



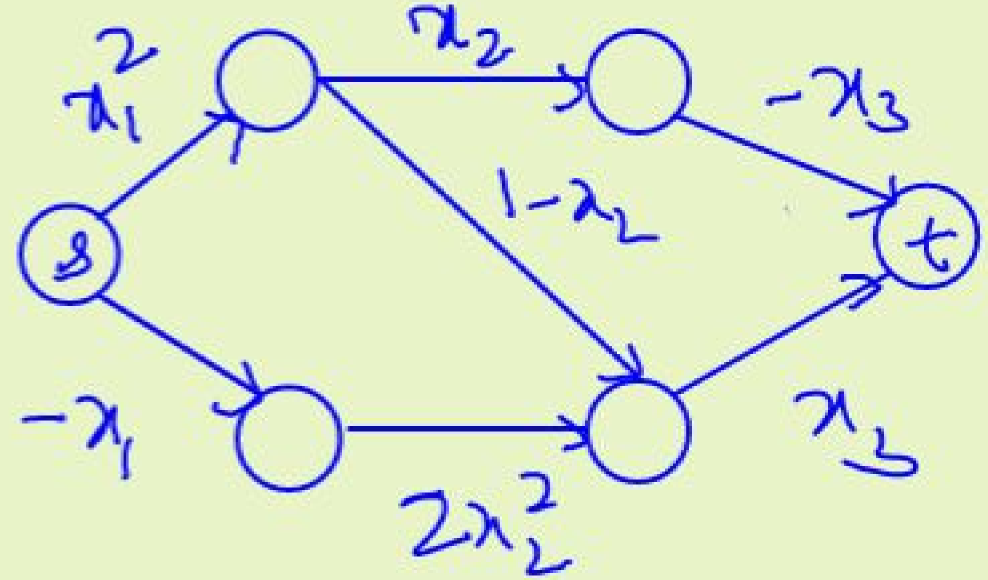
Algebraic / Arithmetic Circuit Complexity

Read-once Oblivious

Algebraic Branching Programs -

Each layer involves a distinct variable.

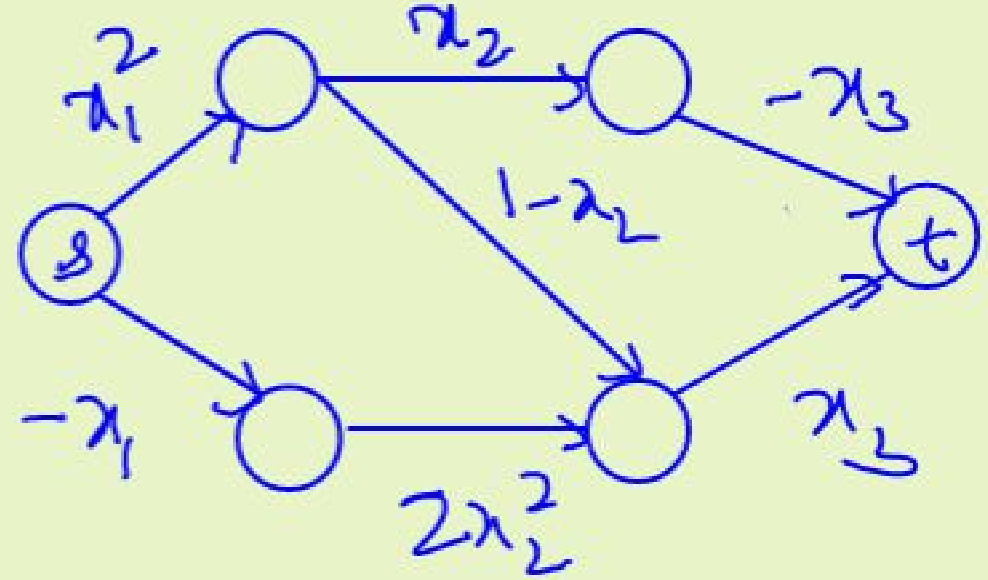
Weights - Univariate polys.



$roABP_{\pi}$: roABP in order π.

Algebraic/Arithmetic Circuit Complexity

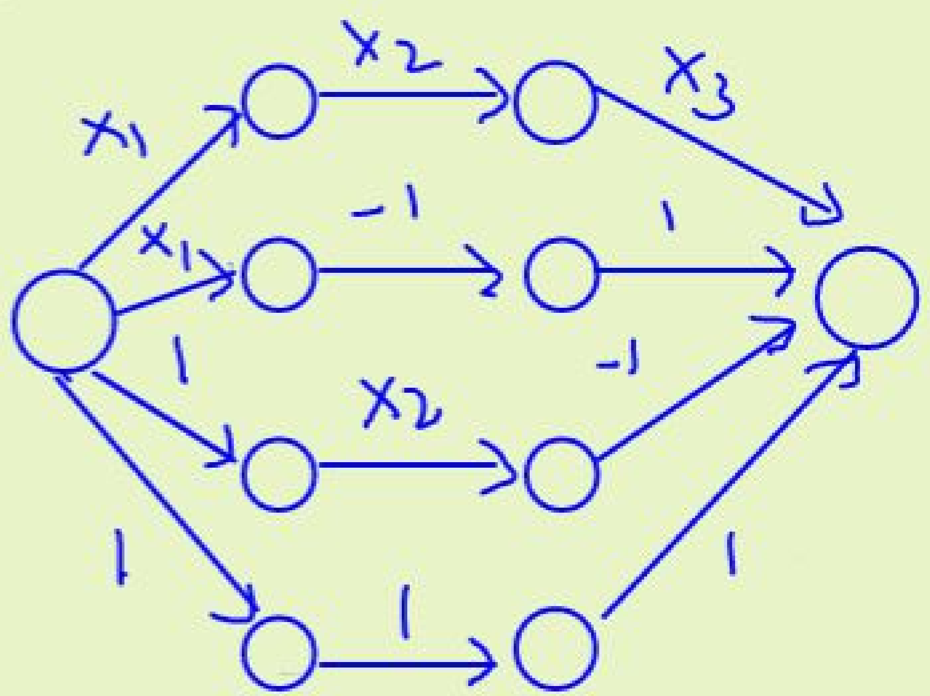
Read-once Oblivious



Algebraic Branching Programs - Each layer involves a distinct variable.

Weights - Univariate polys.

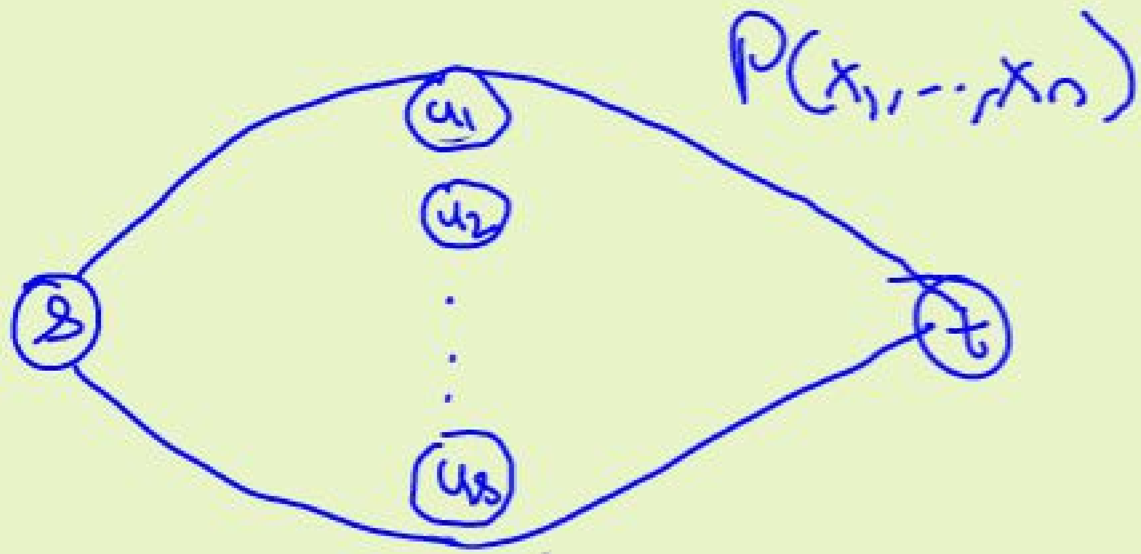
Eg: $x_1x_2x_3 - x_1 - x_2 + 1$



$roABP_\pi$: roABP in order π.

Obs: $P(x_1, \dots, x_n)$ with M monomials $\Rightarrow$ $roABP_\pi$ of size $O(Mn)$

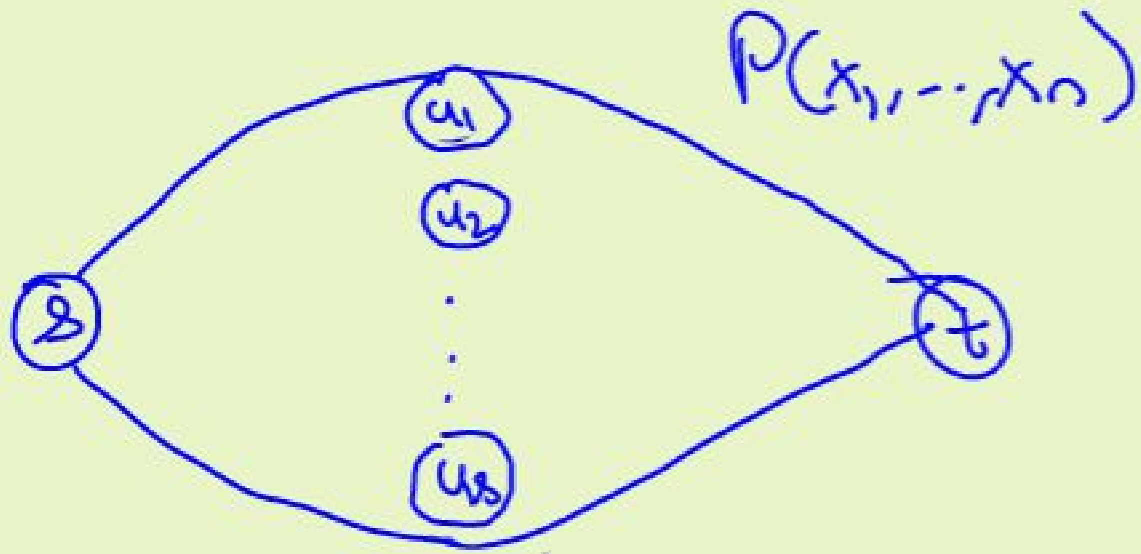
Proving roABP lower bounds via rank [Nisan'91]



$\pi: x_1 x_2 \cdots x_{n/2} \; x_{n/2+1} \cdots x_n$

$$P = \sum_{\text{paths } p} \prod_{e \in p} w_e$$

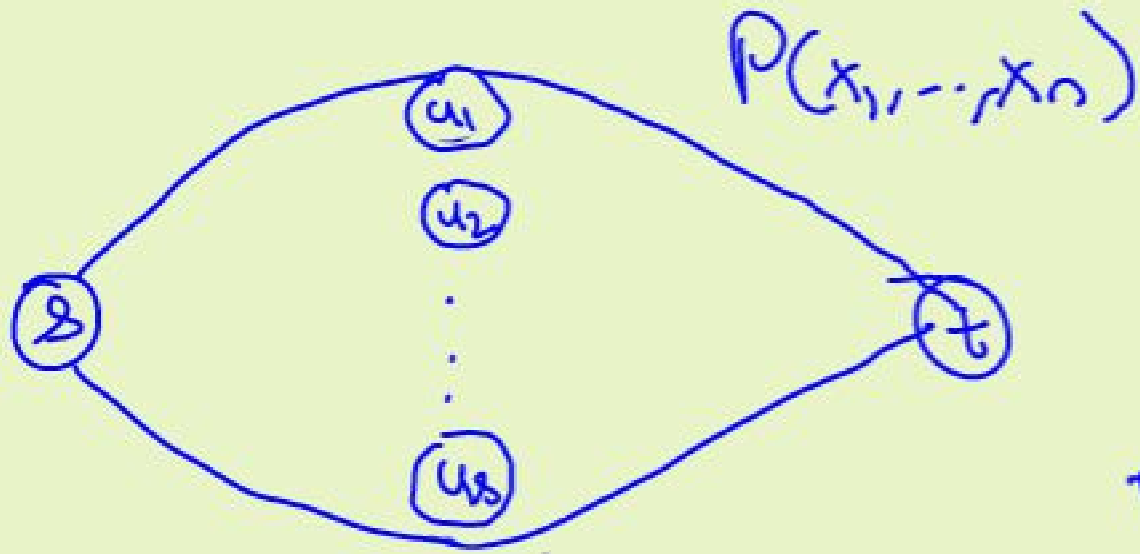
Proving roABP lower bounds via rank [Nisan'91]

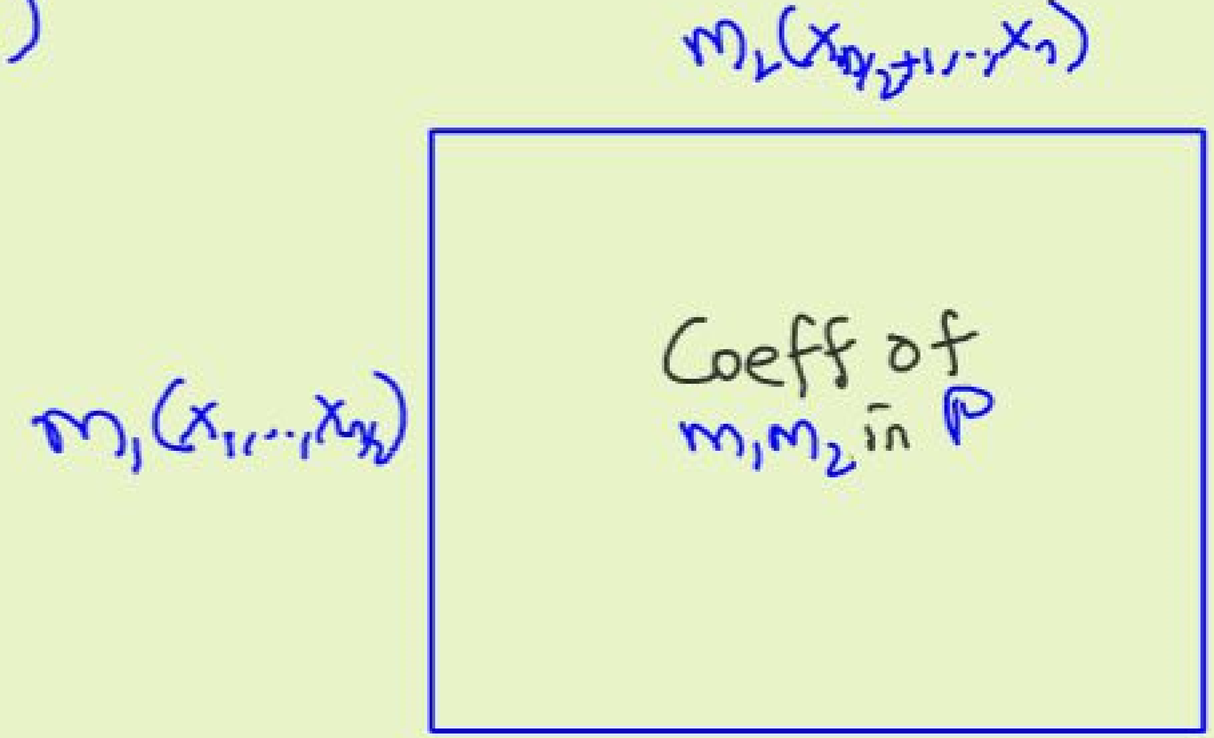


$\pi: x_1 x_2 \cdots x_{n/2} \; x_{n/2+1} \cdots x_n$

$$P = \sum_{i=1}^{s} P_{s,u_i}(x_1,\ldots,x_{n/2}) \cdot P_{u_i,t}(x_{n/2+1},\ldots,x_n)$$

Proving roABP lower bounds via rank [Nisan'91]



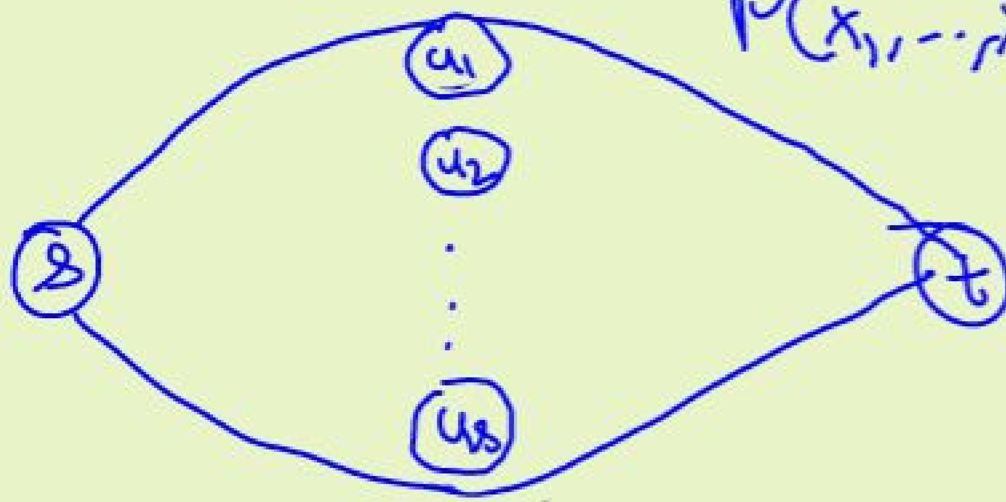


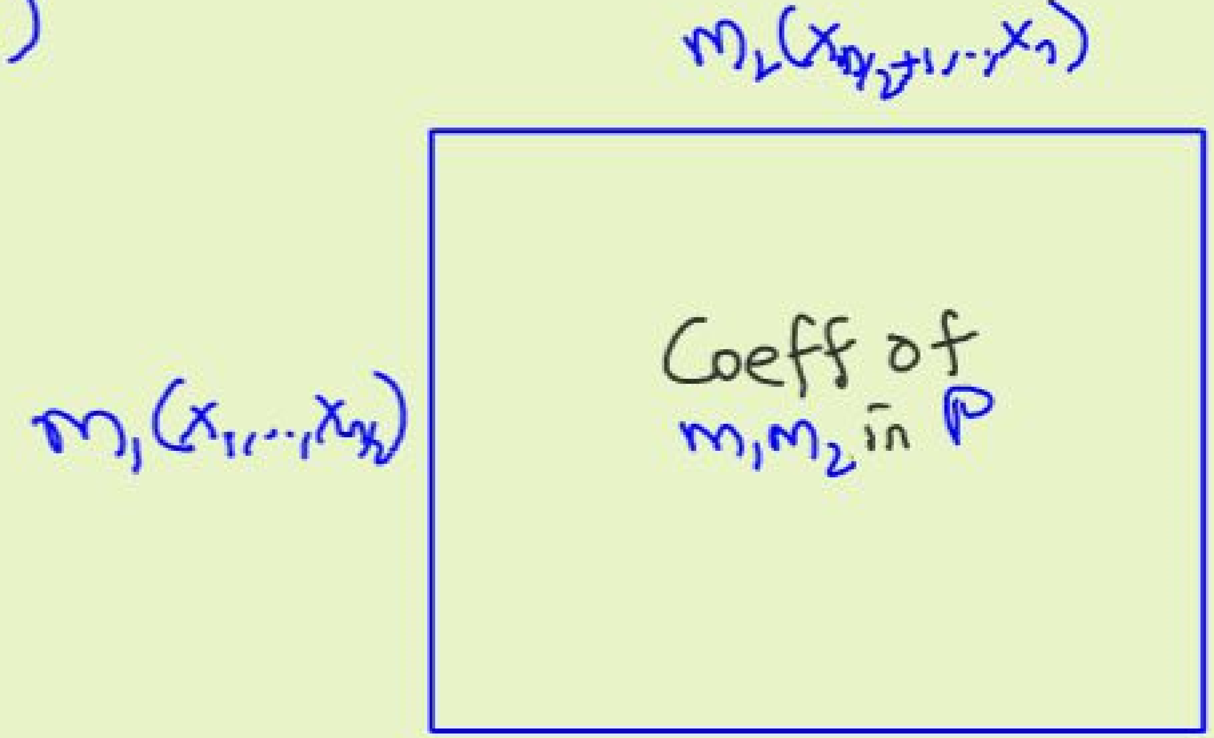
$\pi: x_1 x_2 \cdots x_{n/2} \; x_{n/2+1} \cdots x_n$

$$P = \sum_{i=1}^{s} P_{s,u_i}(x_1,\dots,x_{n/2}) \cdot P_{u_i,t}(x_{n/2+1},\dots,x_n)$$

Proving roABP lower bounds via rank [Nisan '91]

$P(x_1,\dots,x_n)$



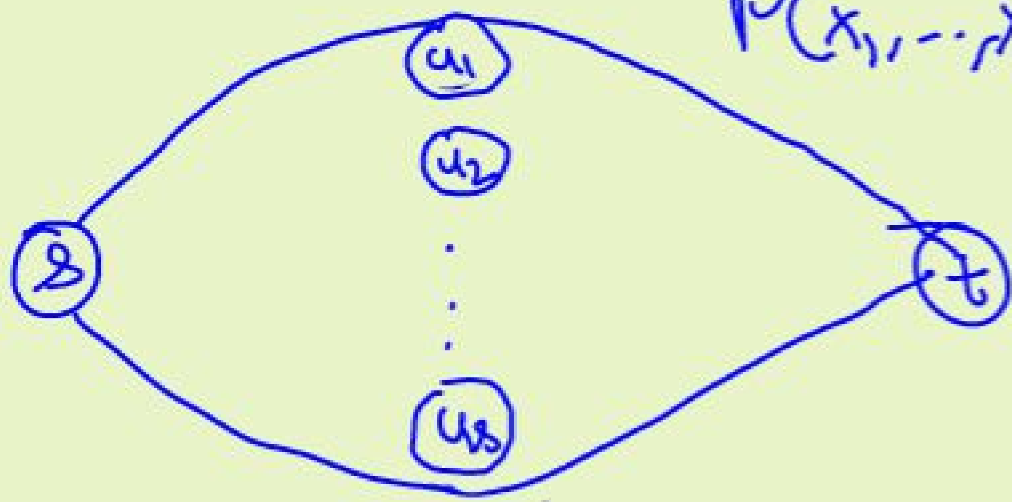


$\pi: x_1 x_2 \cdots x_{n/2}\ x_{n/2+1} \cdots x_n$

$$P = \sum_{i=1}^{s} P_{s,u_i}(x_1,\dots,x_{n/2}) \cdot P_{u_i,t}(x_{n/2+1},\dots,x_n)$$

Coeff matrix $M_{[n/2],[n]\setminus[n/2]}(P)$

Proving roABP lower bounds via rank [Nisan '91]



$P(x_1,\dots,x_n)$

$\pi: x_1 x_2 \cdots x_{n/2}\ x_{n/2+1} \cdots x_n$

$$P = \sum_{i=1}^{s} P_{s,u_i}(x_1,\dots,x_{n/2}) \cdot P_{u_i,t}(x_{n/2+1},\dots,x_n)$$

$$\begin{array}{c|c} & m_2(x_{n/2+1},\dots,x_n) \\ \hline m_1(x_1,\dots,x_{n/2}) & \boxed{\text{Coeff of } m_1 m_2 \text{ in } P} \end{array}$$

Coeff. matrix $M_{[n/2],[n]\setminus[n/2]}(P)$

Eg: $x_1 x_2 x_3 - x_1 - x_2 + 1$

$$\begin{array}{c} \\ 1 \\ x_1 \end{array}\begin{array}{c} \begin{array}{cccc} 1 & x_2 & x_3 & x_2x_3 \end{array} \\ \begin{pmatrix} 1 & -1 & 0 & 0 \\ -1 & 0 & 0 & 1 \end{pmatrix} \end{array}.$$

Proving roABP lower bounds via rank [Nisan'91]

Clm: $P = \sum_{i=1}^{s} P_i(x_1,\dots,x_{n/2}) \cdot Q_i(x_{n/2+1},\dots,x_n) \Rightarrow rk(M(P)) \leq s$

Proving roABP lower bounds via rank [Nisan'91]

<u>Clm</u>: $P = \sum_{i=1}^{s} P_i(x_1, \ldots, x_{n/2}) \cdot Q_i(x_{n/2+1}, \ldots, x_n) \Rightarrow rk(M(P)) \leq s$

<u>Pf</u>: $M(P) = \sum_{i=1}^{s} M(P_i \cdot Q_i)$

Proving roABP lower bounds via rank [Nisan'91]

Clm: $P = \sum_{i=1}^{s} P_i(x_1,\dots,x_{n/2}) \cdot Q_i(x_{n/2+1},\dots,x_n) \Rightarrow rk(M(P)) \le s$

Pf: $M(P) = \sum_{i=1}^{s} M(P_i \cdot Q_i)$

$$\begin{array}{cc} & m_2 \\ m_1 & \left(\begin{array}{c} \\ \mathrm{coeff}_{P_i}(m_1) \cdot \\ \mathrm{coeff}_{Q_i}(m_2) \\ \\ \end{array} \right) \end{array}$$

Proving roABP lower bounds via rank [Nisan'91]

<u>Clm</u>: $P = \sum_{i=1}^{s} P_i(x_1,\dots,x_{n/2}) \cdot Q_i(x_{n/2+1},\dots,x_n) \Rightarrow rk(M(P)) \leq s$

<u>Pf</u>: $M(P) = \sum_{i=1}^{s} M(P_i \cdot Q_i)$

$$\begin{array}{cc} & m_2 \\ m_1 & \begin{pmatrix} \\ \text{coeff}_{P_i}(m_1) \cdot \\ \text{coeff}_{Q_i}(m_2) \\ \\ \end{pmatrix} \end{array} \Rightarrow \text{rank } 1$$

Proving roABP lower bounds via rank [Nisan'91]

Clm: $P = \sum_{i=1}^{s} P_i(x_1,\dots,x_{n/2}) \cdot Q_i(x_{n/2+1},\dots,x_n) \Rightarrow rk(M(P)) \le s$

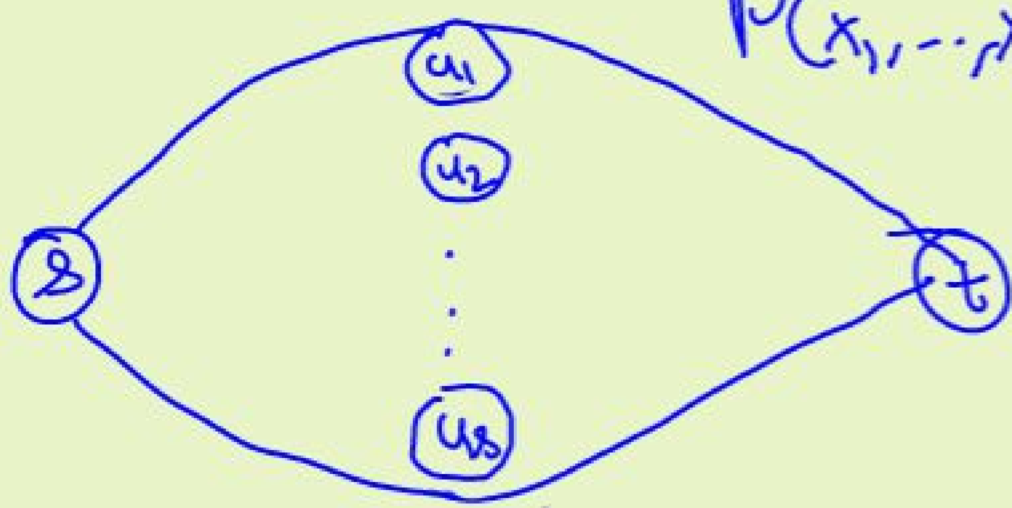
Pf: $M(P) = \sum_{i=1}^{s} M(P_i \cdot Q_i) \Rightarrow rk(M(P)) \le s$

subadditivity of rank

$$\begin{array}{cc} & m_2 \\ m_1 & \left(\begin{array}{c} \mathrm{coeff}_{P_i}(m_1) \cdot \\ \mathrm{coeff}_{Q_i}(m_2) \end{array} \right) \end{array} \Rightarrow \text{rank } 1$$

Proving roABP lower bounds via rank [Nisan'91]

$P(x_1,\dots,x_n)$

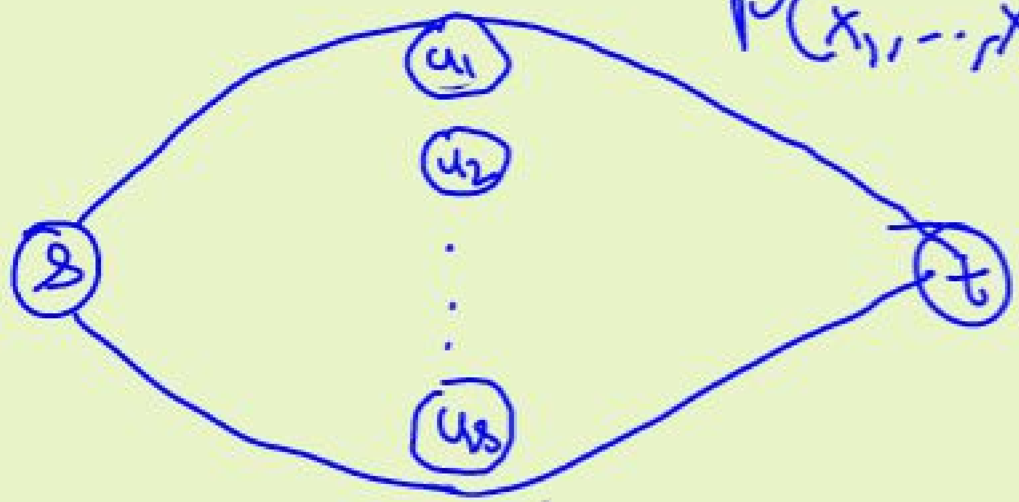


$\pi: x_1 x_2 \cdots x_{n/2}\ x_{n/2+1} \cdots x_n$

$$P = \sum_{i=1}^{s} P_{s,u_i}(x_1,\dots,x_{n/2}) \cdot P_{u_i,t}(x_{n/2+1},\dots,x_n)$$

$$\Rightarrow \operatorname{rk}\left(M_{[n/2],[n]\setminus[n/2]}(P)\right) \leq s$$

Proving roABP lower bounds via rank [Nisan'91]



$P(x_1, \ldots, x_n)$

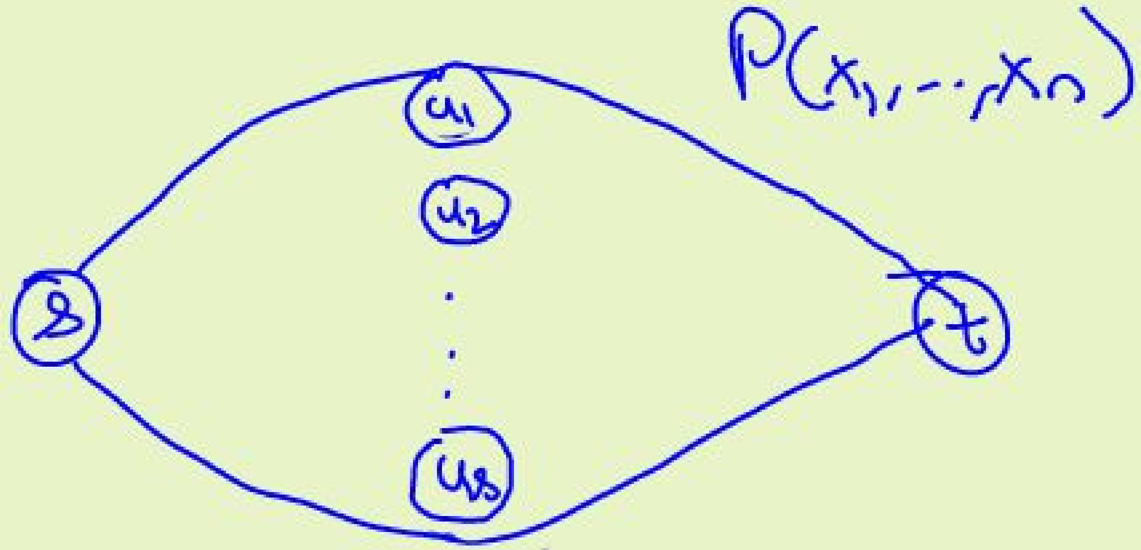
$$P(x_1, \ldots, x_n) := (x_1 + x_{n/2+1}) \cdot (x_2 + x_{n/2+2}) \cdots (x_{n/2} + x_n)$$

π: $x_1 x_2 \cdots x_{n/2} \; x_{n/2+1} \cdots x_n$

$$P = \sum_{i=1}^{s} P_{s,u_i}(x_1, \ldots, x_{n/2}) \cdot P_{u_i,t}(x_{n/2+1}, \ldots, x_n)$$

$$\Rightarrow \operatorname{rk}\left(M_{[n/2],[n]\setminus[n/2]}(P)\right) \leq s$$

Proving roABP lower bounds via rank [Nisan '91]



$P(x_1,\ldots,x_n) :=$

$$(x_1+x_{n/2+1})\cdot(x_2+x_{n/2+2})\cdots(x_{n/2}+x_n)$$

π: $x_1 x_2 \cdots x_{n/2}\ x_{n/2+1} \cdots x_n$

$$P = \sum_{i=1}^{s} P_{s,u_i}(x_1,\ldots,x_{n/2})\cdot P_{u_i,t}(x_{n/2+1},\ldots,x_n) \qquad M^{(P)}_{[n/2],[n]\setminus[n/2]} = \begin{pmatrix} 0 & & 1 \\ & \iddots & \\ 1 & & 0 \end{pmatrix}$$

$$\Rightarrow \mathrm{rk}\left(M^{(P)}_{[n/2],[n]\setminus[n/2]}\right) \leq s$$

$$\Rightarrow s \geq 2^{n/2}$$

Unknown Order

→ $P_\pi := (x_{\pi(1)} + x_{\pi(n/2+1)}) \cdots (x_{\pi(n/2)} + x_{\pi(n)})$ hard for roABP$_\pi$

Unknown Order

$\rightarrow P_\pi := (x_{\pi(1)} + x_{\pi(n/2+1)}) \cdots (x_{\pi(n/2)} + x_{\pi(n)})$ hard for roABP_π

$\underline{\underline{\text{Clm}}}$ $P_{all}(x, z) := \sum_{\sigma \in S_n} \prod_i z_{i,\sigma(i)} \cdot P_\sigma$ hard for all $\pi \in S_n$.

Unknown Order

$\to P_\pi := (x_{\pi(1)} + x_{\pi(n/2+1)}) \cdots (x_{\pi(n/2)} + x_{\pi(n)})$ hard for roABP$_\pi$

<u>Clm</u> $P_{all}(x,z) := \sum_{\sigma \in S_n} \prod_i z_{i,\sigma(i)} \cdot P_\sigma$ hard for all $\pi \in S_n$.

Pf: roABP A' for P_{all} in order $\pi' \in S_{n+n^2}$.

$\pi = \pi'|_x$. Set $z_{i,\pi(i)} = 1\ \forall i$ & other $z_{i,j} = 0$.

Unknown Order

$\to P_\pi := (x_{\pi(1)} + x_{\pi(n/2+1)}) \cdots (x_{\pi(n/2)} + x_{\pi(n)})$ hard for roABP$_\pi$

Clm $P_{all}(x,z) := \sum_{\sigma \in S_n} \prod_i z_{i,\sigma(i)} \cdot P_\sigma$ hard

for all $\pi \in S_n$.

Pf: roABP A' for P_{all} in order $\pi' \in S_{n+n^2}$.

$\pi = \pi'|_x$. Set $z_{i,\pi(i)} = 1 \ \forall i$ & other $z_{i,j} = 0$.

$A' \rightsquigarrow A$ for P_π

size s order π' size s order π

Unknown Order

$\rightarrow P_\pi := (x_{\pi(1)} + x_{\pi(n/2+1)}) \cdots (x_{\pi(n/2)} + x_{\pi(n)})$ hard for roABP_π

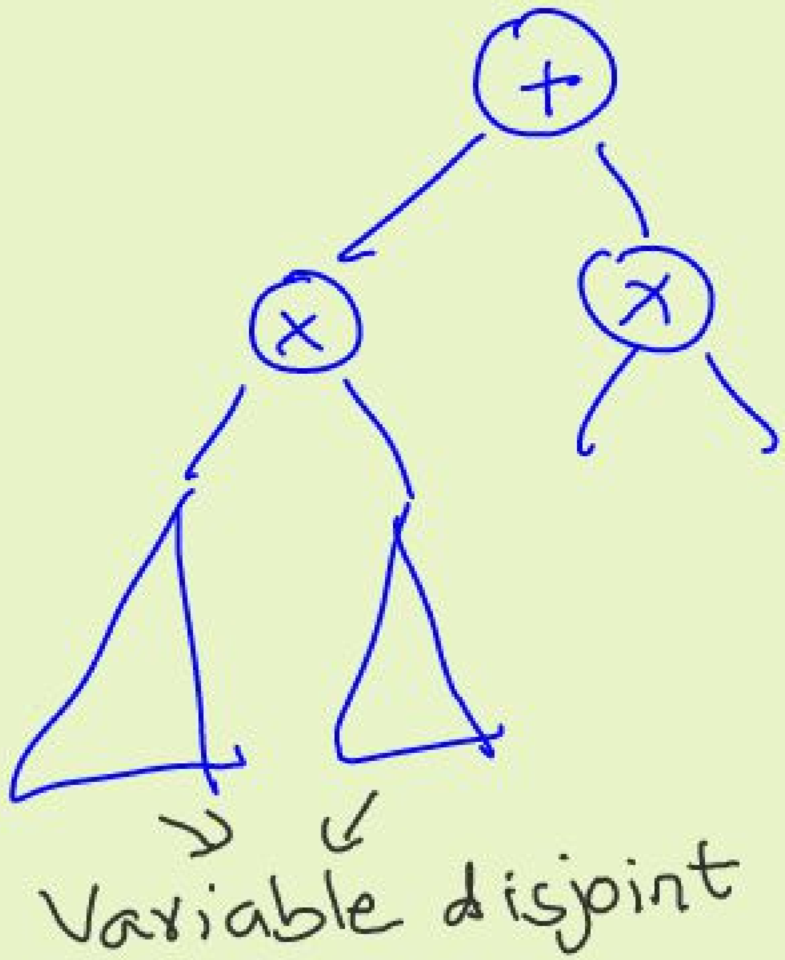
Clm $P_{all}(x,z) := \sum_{\sigma \in S_n} \prod_i z_{i,\sigma(i)} \cdot P_\sigma$ hard for all $\pi \in S_n$.

Pf: roABP A' for P_{all} in order $\pi' \in S_{n+n^2}$.

$\pi = \pi'|_x$. Set $z_{i,\pi(i)} = 1 \ \forall i$ & other $z_{i,j} = 0$.

$\underset{\substack{\text{size } s \\ \text{order } \pi'}}{A'} \rightsquigarrow \underset{\substack{\text{size } s \\ \text{order } \pi}}{A}$ for $P_\pi \implies s \geq 2^{n/2}$.

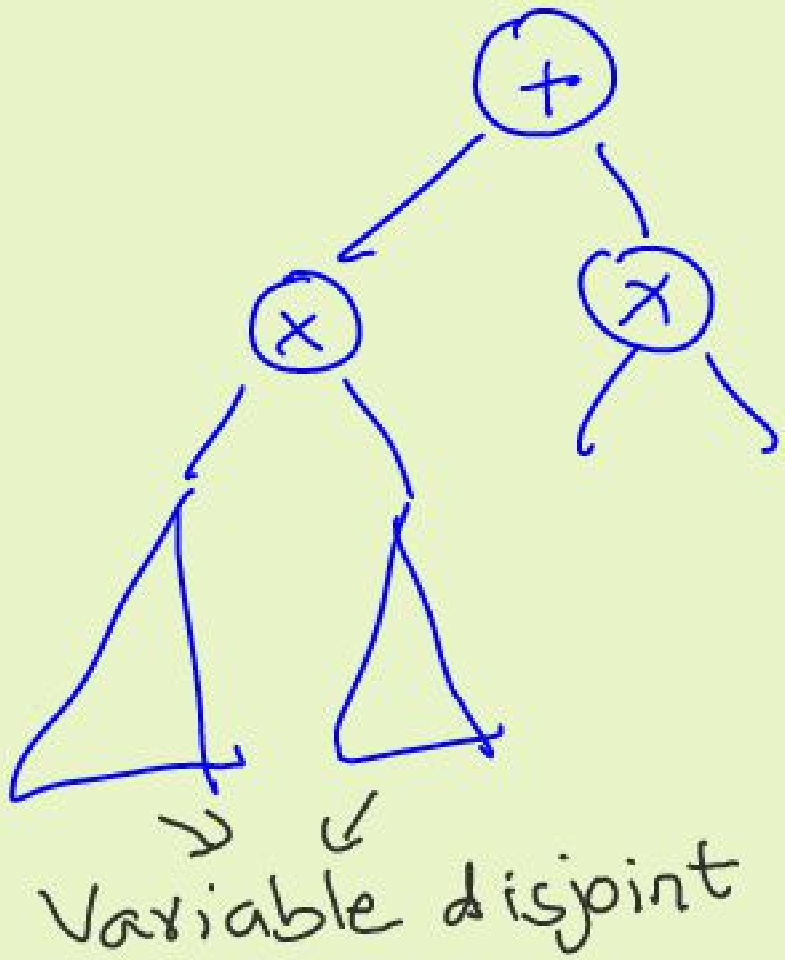
Multilinear formulas



Syntactically multilinear.

Can only compute multilinear polynomials

Multilinear formulas

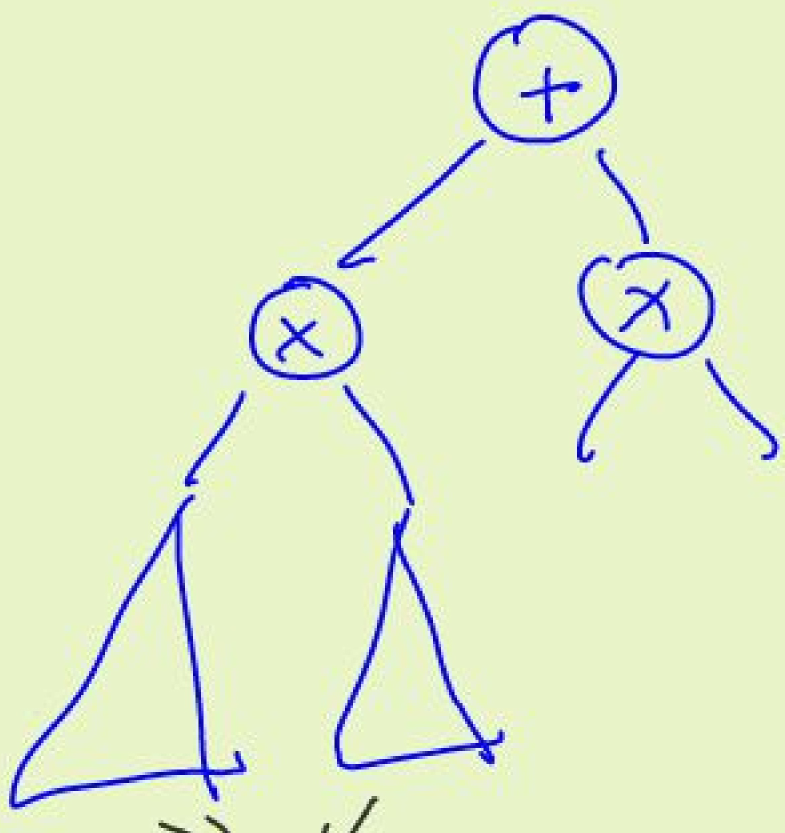


Syntactically multilinear.

Can only compute multilinear polynomials

<u>Thm</u> [Raz'04]: Superpoly. lower bounds.

Multilinear formulas



Variable disjoint

Syntactically multilinear.

Can only compute multilinear polynomials

<u>Thm</u> [Raz '04]: Superpoly. lower bounds.

Rank <u>Lemma</u>: $F(x_1, \ldots, x_n)$ multilinear formula size $n^{O(1)}$.

$S \in_R \binom{[n]}{n/2}$ $\Pr_S[\mathrm{rk}(M_{S,\bar{S}}(F)) < \text{full}] = 1 - o(1)$

Proof of depth-3 case

Rank Lemma: $F(x_1, \dots, x_n)$ multilinear formula size $n^{O(1)}$.
$S \in_R \binom{[n]}{n/2}$ $\Pr[\mathrm{rk}(M_{S,\bar{S}}(F)) < \text{full}] = 1 - o(1)$

Proof of depth-3 case

Rank Lemma: $F(x_1, \ldots, x_n)$ multilinear formula size $n^{O(1)}$.
$S \in_R \binom{[n]}{n/2}$ $\Pr[\mathrm{rk}(M_{S,\bar{S}}(F)) < \text{full}] = 1 - o(1)$

$$F = \sum_{i=1}^{s} L_{i,1}(X_{i,1}) \cdots L_{i,t}(X_{i,t})$$

plus disjoint

Proof of depth-3 case

Rank Lemma: $F(x_1, \dots, x_n)$ multilinear formula size $n^{O(1)}$.
$S \in_R \binom{[n]}{n/2}$ $\Pr[rk(M_{S,\bar{S}}(F)) < \text{full}] = 1 - o(1)$

$$F = \sum_{i=1}^{s} L_{i,1}(X_{i,1}) \cdots L_{i,t}(X_{i,t})$$

plus disjoint

$$M_{S,\bar{S}}(F) = \sum_{i=1}^{s} M_{S,\bar{S}}(L_{i,1} \cdots L_{i,t})$$

$$\Rightarrow rk(M_{S,\bar{S}}(F)) \leq \sum_{i=1}^{s} rk(M_{S,\bar{S}}(L_{i,1} \cdots L_{i,t}))$$

Proof of depth-3 case

Rank Lemma: $F(x_1, \ldots, x_n)$ multilinear formula size $n^{O(1)}$.

$S \in_R \binom{[n]}{n/2}$ $\Pr[rk(M_{S,\bar{S}}(F)) < full] = 1 - o(1)$

$$F = \sum_{i=1}^{s} L_{i,1}(x_{i,1}) \cdots L_{i,t}(x_{i,t})$$

plus disjoint

$$M_{S,\bar{S}}(F) = \sum_{i=1}^{s} M_{S,\bar{S}}(L_{i,1} \cdots L_{i,t})$$

$$\Rightarrow rk(M_{S,\bar{S}}(F)) \leq \sum_{i=1}^{s} rk(M_{S,\bar{S}}(L_{i,1} \cdots L_{i,t}))$$

Suff: $\Pr_S\left[rk(M_{S,\bar{S}}(L_1 \cdots L_t)) \geq \frac{2^{n/2}}{2^{\Omega(n)}}\right] \leq \frac{1}{2^{\Omega(n)}}$

Product of linear polys

$$\Pr_S\left[rk(M_{S,\bar{S}}(L_1 \cdots L_t)) \geq \frac{2^{n/2}}{2^{\Omega(n)}} \right] \leq \frac{1}{2^{\Omega(n)}}$$

$$L = L_1(X_1) \cdots L_t(X_t)$$

Product of linear polys

$$\Pr_S\left[rk(M_{S,\bar{S}}(L_1\cdots L_t)) \geq \frac{2^{n/2}}{2^{\Omega(n)}}\right] \leq \frac{1}{2^{\Omega(n)}}$$

$L = L_1(X_1)\cdots L_t(X_t)$ $\qquad S_i = X_i \cap S$

$$M_{S,\bar{S}}(L) = M_{S_1,\bar{S}_1}(L_1) \otimes \cdots \otimes M_{S_t,\bar{S}_t}(L_t)$$

Product of linear polys

$$\Pr_S\left[rk(M_{S,\bar S}(L_1 \cdots L_t)) \geq \frac{2^{n/2}}{2^{\Omega(n)}} \right] \leq \frac{1}{2^{\Omega(n)}}$$

$$L = L_1(X_1) \cdots L_t(X_t) \qquad S_i = X_i \cap S$$

$$M_{S,\bar S}(L) = M_{S_1,\bar S_1}(L_1) \otimes \cdots \otimes M_{S_t,\bar S_t}(L_t)$$

$$rk(M_{S,\bar S}(L)) = \prod_{i \in [t]} rk(M_{S_i,\bar S_i}(L_i)) \leq 2^{n/2} = 2^{\sum_i \frac{|X_i|}{2}}$$

Obs $|S_i| \neq |\bar S_i| \Rightarrow rk(M_{S_i,\bar S_i}(L_i)) \leq \min\{2^{|S_i|}, 2^{|\bar S_i|}\}$

$$< 2^{\frac{|X_i|}{2} - 1}$$

Product of linear polys

$\Pr_S \left[rk(M_{S,\bar{S}}(L_1 \cdots L_t)) \geq \frac{2^{n/2}}{2^{\Omega(n)}} \right] \leq \frac{1}{2^{\Omega(n)}}$

$L = L_1(X_1) \cdots L_t(X_t)$ $\qquad S_i = X_i \cap S$

$M_{S,\bar{S}}(L) = M_{S_1,\bar{S}_1}(L_1) \otimes \cdots \otimes M_{S_t,\bar{S}_t}(L_t)$

$rk(M_{S,\bar{S}}(L)) = \prod_{i \in [t]} rk(M_{S_i,\bar{S}_i}(L_i)) \leq 2^{n/2} = 2^{\sum_i \frac{|X_i|}{2}}$

Obs $\underbrace{|S_i| \neq |\bar{S}_i|}_{\text{discrepancy}} \Rightarrow rk(M_{S_i,\bar{S}_i}(L_i)) \leq \min\{2^{|S_i|}, 2^{|\bar{S}_i|}\}$

$< 2^{\frac{|X_i|}{2} - 1}$

Product of linear polys

$$\Pr_S\left[rk(M_{S,\bar{S}}(L_1 \cdots L_t)) \geq \frac{2^{n/2}}{2^{\Omega(n)}} \right] \leq \frac{1}{2^{\Omega(n)}}$$

$$L = L_1(X_1) \cdots L_t(X_t) \qquad S_i = X_i \cap S$$

$$M_{S,\bar{S}}(L) = M_{S_1,\bar{S}_1}(L_1) \otimes \cdots \otimes M_{S_t,\bar{S}_t}(L_t)$$

$$rk(M_{S,\bar{S}}(L)) = \prod_{i \in [t]} rk(M_{S_i,\bar{S}_i}(L_i)) \leq 2^{n/2} = 2^{\sum_i \frac{|X_i|}{2}}$$

Obs $\underbrace{|S_i| \neq |\bar{S}_i|}_{\text{discrepancy}} \Rightarrow rk(M_{S_i,\bar{S}_i}(L_i)) \leq \min\{2^{|S_i|}, 2^{|\bar{S}_i|}\}$

$$< 2^{\frac{|X_i|}{2} - 1}$$

$$\Pr\left[\#\{ i \mid |S_i| \neq |\bar{S}_i| \} < \frac{t}{10} \right] \leq 2^{-\Omega(t)}$$

Done for $t = \Omega(n)$. Other case easy [ex.]

General multilinear formulas

Product lemma [Shpilka-Yehudayoff '10] :

F multilinear formula of size s

$$F = \sum_{i=1}^{s} F_{i,1}(X_{i,1}) \cdots F_{i,\ell}(X_{i,\ell})$$

p/w disjoint

Take-home messages

→ Co-efficient matrix

→ Discrepancy as a means of bounding coefficient matrix rank.