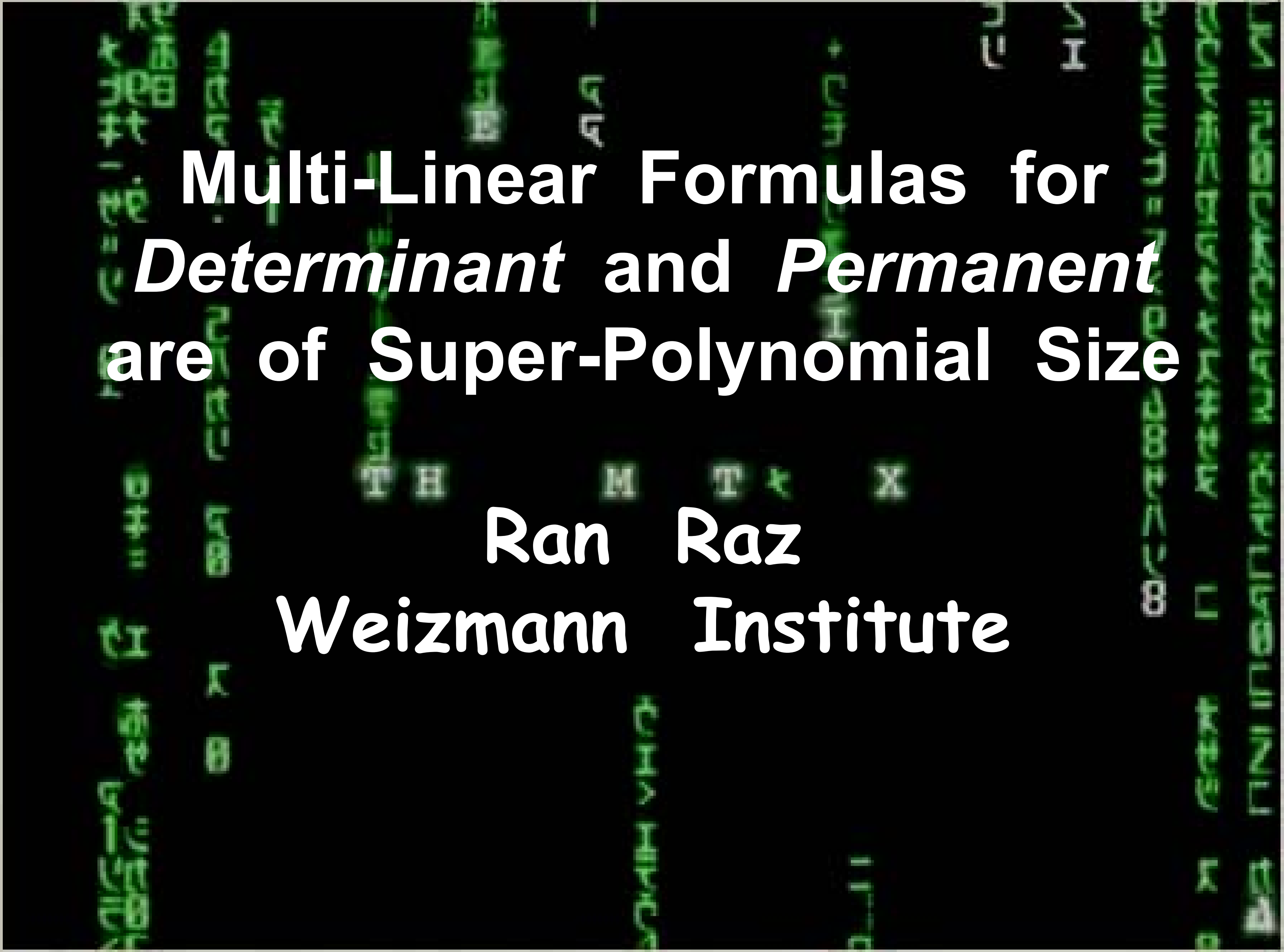


Multi-Linear Formulas for *Determinant* and *Permanent* are of Super-Polynomial Size

Ran Raz
Weizmann Institute

Determinant:

$$\sum_{\sigma \in \mathbf{S_n}} \mathsf{sgn}(\sigma) \mathbf{X}_{\mathbf{1},\sigma(\mathbf{1})} \cdots \mathbf{X}_{\mathbf{n},\sigma(\mathbf{n})}$$

Permanent:

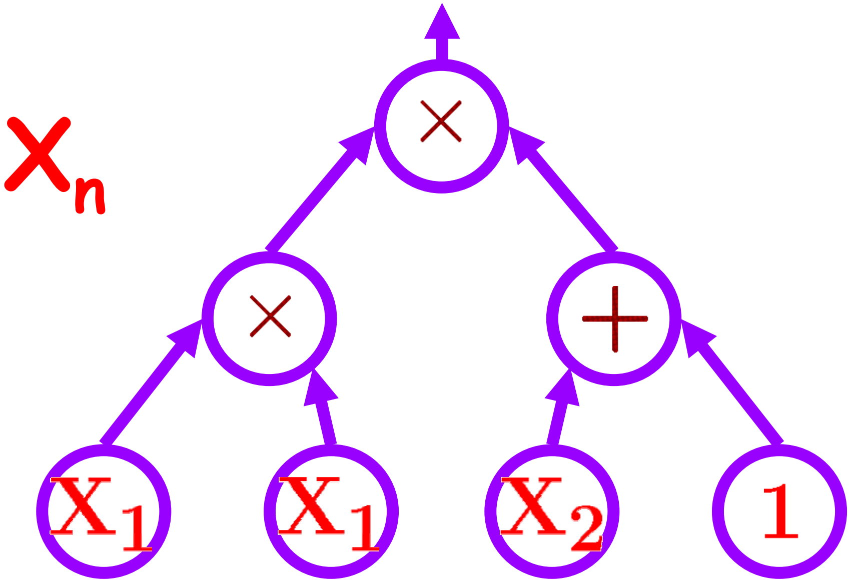
$$\sum_{\sigma \in \mathbf{S_n}} \mathbf{X}_{\mathbf{1},\sigma(\mathbf{1})} \cdots \mathbf{X}_{\mathbf{n},\sigma(\mathbf{n})}$$

Arithmetic Formulas:

Field: $\mathbb{F}$

Variables: $X_1, \ldots, X_n$

Gates: $+$, $\times$



Every gate in the formula computes a polynomial in $\mathbb{F}[X_1, \ldots, X_n]$

Example: $(X_1$ □ $X_1)$ □ $(X_2 + 1)$

Smallest Arithmetic Formula:

Determinant [Ber 84]: $n^{O(\log n)}$

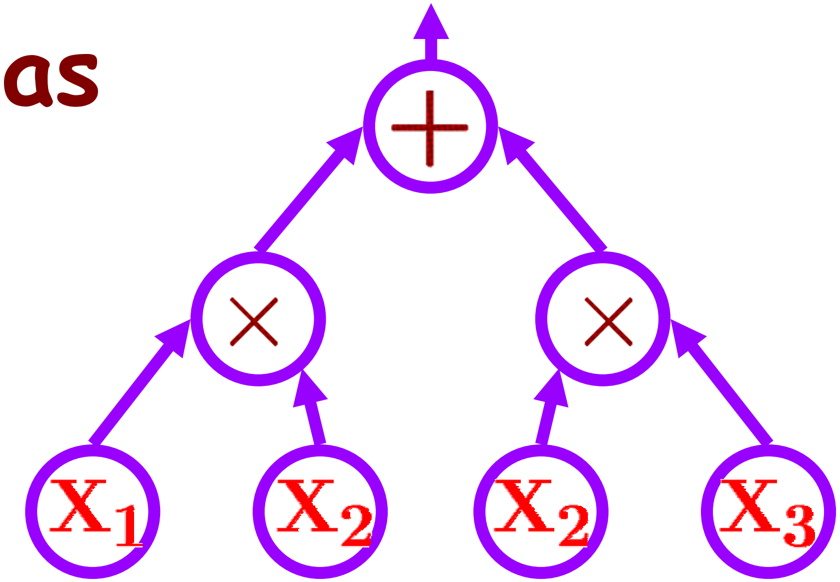
Permanent [Rys 63]: $O(n^2 \cdot 2^n)$

Are there poly size formulas ?

Super polynomial lower bounds are not known for any explicit function (outstanding open problem)

Multilinear Formulas

[NW]:



Every gate in the formula computes a multilinear polynomial

Example: $(X_1 \square X_2) + (X_2 \square X_3)$

(no high powers of variables)

Motivation:

1) For many functions, non-multilinear formulas are very counter-intuitive
2) Many formulas for Determinant and Permanent are multilinear (Ryser)
3) Multilinear polynomials: interesting subclass of polynomials
4) Multilinear formulas: strong subclass of formulas (contains other classes)

Multilinear Formulas and Skepticism of Quantum Computing [Aaronson]:

$\Big(\Big|$ $\Big\rangle - \Big|$ $\Big\rangle\Big)/\sqrt{2}$

Previous Work:

[NW 95]: Lower bounds for a subclass of constant depth multilinear formulas

[Nis, NW, RS]: Lower bounds for other subclasses of multilinear formulas

[Sch 76, SS 77, Val 83]: Lower bounds for monotone arithmetic formulas

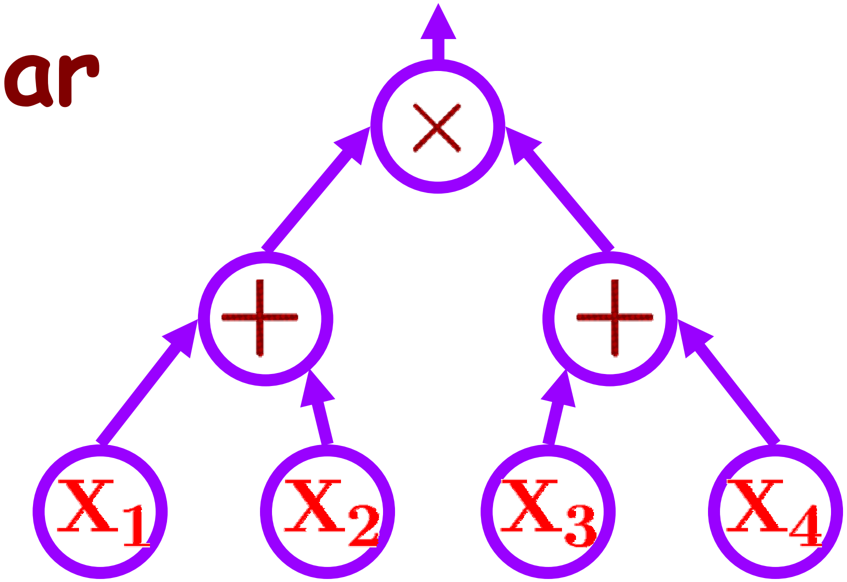
For general multilinear formulas:
no lower bound, even for constant depth

Our Result:

Any multilinear formula for the Determinant or the Permanent is of size:

$$n^{\Omega(\log n)}$$

Syntactic Multilinear Formulas:



No variable appears in both sons of any product gate

Proposition:

Multilinear formulas and syntactic multilinear formulas are equivalent

Partial Derivatives Matrix [Nis]:

f = a multilinear polynomial over $\{y_1,...,y_m\}$ □ $\{z_1,...,z_m\}$

P = set of multilinear monomials in $\{y_1,...,y_m\}$. $|P| = 2^m$

Q = set of multilinear monomials in $\{z_1,...,z_m\}$. $|Q| = 2^m$

Partial Derivatives Matrix [Nis]:

f = a multilinear polynomial over
$\{y_1,\dots,y_m\}$ □ $\{z_1,\dots,z_m\}$

P = set of multilinear monomials in
$\{y_1,\dots,y_m\}$. $|P| = 2^m$

Q = set of multilinear monomials in
$\{z_1,\dots,z_m\}$. $|Q| = 2^m$

$M = M_f =$ 2^m dimensional matrix:

For every p □ P, q □ Q,

$M_f(p,q)$ = coefficient of pq in f

Example:

$$f(y_1,y_2,z_1,z_2) = 1 + y_1y_2 - y_1z_1z_2$$

$$M_f = \begin{array}{cccc|c} 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & -1 & y_1 \\ 0 & 0 & 0 & 0 & y_2 \\ 1 & 0 & 0 & 0 & y_1y_2 \\ \hline 1 & z_1 & z_2 & z_1z_2 & \end{array}$$

Partial Derivatives Method [N,NW]

[Nis]: If f is computed by a noncommutative formula of size s then $\mathrm{Rank}(M_f) = \mathrm{poly}(s)$

[NW,RS]: The same for other classes of formulas

Is the same true for multilinear formulas ?

Counter Example:

$$f = \prod_{i=1}^{m} (y_i + z_i)$$

M_f is a permutation matrix

Rank(M_f) = 2^m

Basic Facts:

1) If f depends on only k variables in $\{y_1, \ldots, y_m\}$ then $\mathrm{Rank}(M_f)$ □ 2^k

2) If $f=g+h$ then
$\mathrm{Rank}(M_f)$ □ $\mathrm{Rank}(M_g) + \mathrm{Rank}(M_h)$

3) If $f=g$□h then
$\mathrm{Rank}(M_f) = \mathrm{Rank}(M_g)$ □ $\mathrm{Rank}(M_h)$

Notations:

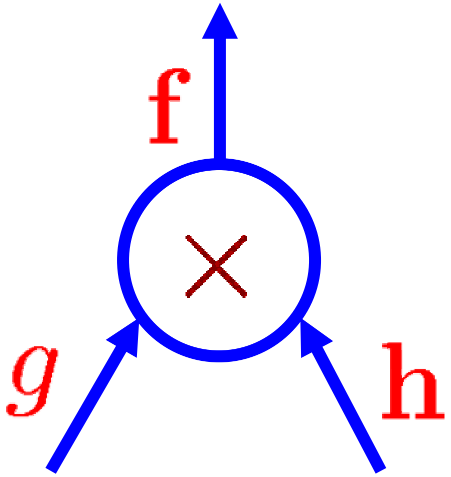
Y_f = variables in $\{y_1,...,y_m\}$ that f depends on

Z_f = variables in $\{z_1,...,z_m\}$ that f depends on

f is k-unbalanced if $||Y_f|-|Z_f||$ □ k

A gate v is k-unbalanced if it computes a k-unbalanced function f

Crucial Observation:



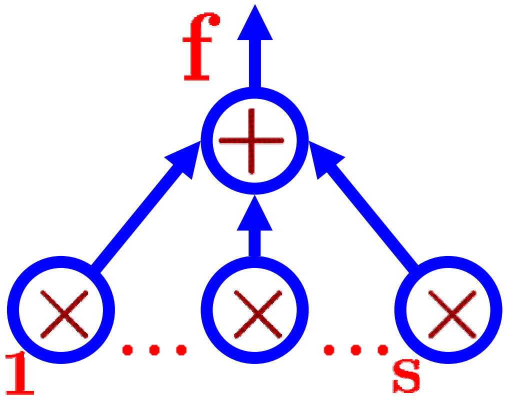
If f=g□h and either g or h are k-unbalanced then Rank(M_f) □ 2^{m-k}

Proof:

Either $|Y_g| + |Z_h|$ □ $m-k$

or $|Z_g| + |Y_h|$ □ $m-k$

Corollary:



s = number of top product gates

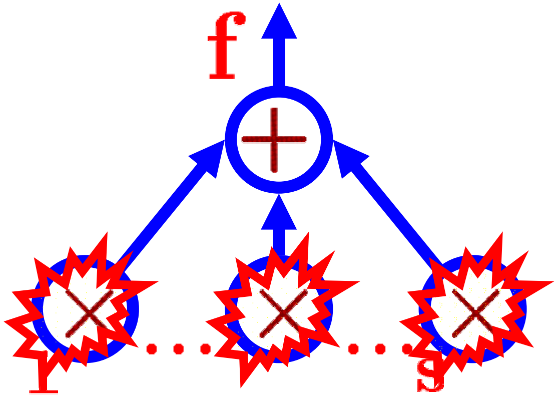
If every top product gate has a k-unbalanced son then

Rank(M_f) □ s□2^{m-k}

Random Partition:

Partition (at random) $\{x_1,\ldots,x_{2m}\}$ □ □□$\{y_1,\ldots,y_m\}$ □ $\{z_1,\ldots,z_m\}$ and hope to unbalance all top products

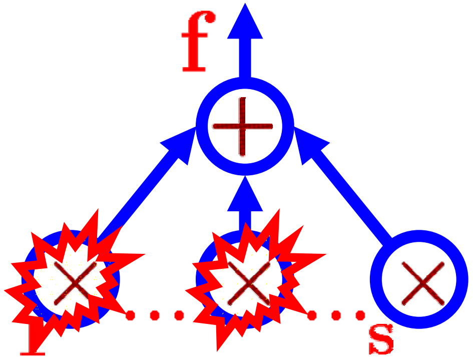
If v depends on □ m variables then (w.h.p.) v becomes m^{ε}-unbalanced



Random Partition:

Partition (at random) $\{x_1,\ldots,x_{2m}\}$
□ □□$\{y_1,\ldots,y_m\}$ □ $\{z_1,\ldots,z_m\}$ and
hope to unbalance all top products

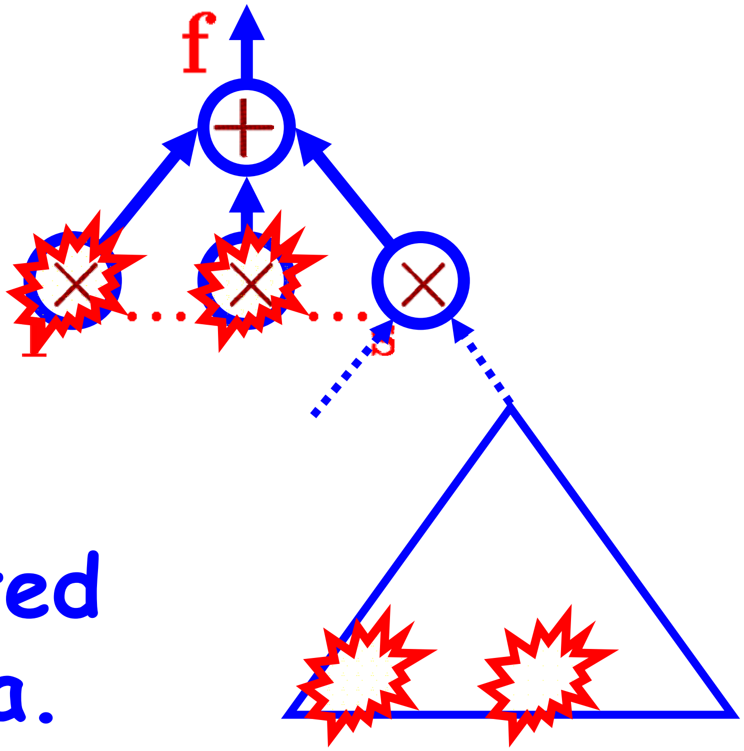
If v depends on □ m variables then
(w.h.p.) v becomes m^{ε}-unbalanced



Problem: With probability □ $m^{-1/2}$,
v is completely balanced.
If there are > $m^{1/2}$ top products,
some of them have balanced sons

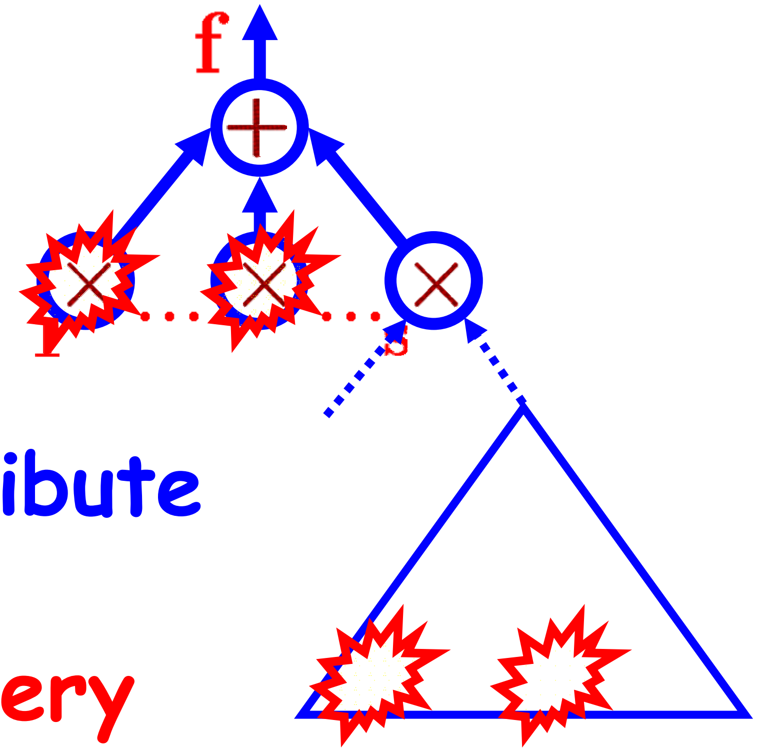
That's the most stupid idea I ever heard

Recursion:



A gate that remained balanced is still computed by a multilinear formula. Maybe some of its sons are unbalanced...

Intuition:



Unbalanced gates contribute little to the final rank.

Enough to show that every path from a leaf to the root contains an unbalanced gate

Notations:

Ψ = a multilinear formula (fanin 2)

$|\Psi|$ = size of Ψ

A path from a leaf to the root is central if the degrees along it increase by factors of at most 2

Ψ is k-weak if every central path contains a k-unbalanced gate

Notations:

Ψ = a multilinear formula (fanin 2)

$|\Psi|$ = size of Ψ

A path from a leaf to the root is central if the degrees along it increase by factors of at most 2

Ψ is k-weak if every central path contains a k-unbalanced gate

Lemma 1: If Ψ is k-weak then

$$\mathrm{Rank}(\mathbf{M}_{\Psi}) \leq |\Psi| \cdot 2^{\mathrm{m}-(\mathbf{k}/2)}$$

Lemma 2:

Assume $|\Psi| < m^{(\log m)/100}$

Partition (at random) $\{X_1,\ldots,X_{2m}\}$ □ □□$\{y_1,\ldots,y_m\}$ □ $\{z_1,\ldots,z_m\}$. Then (w.h.p.): Ψ is k-weak for $k=m^{\varepsilon}$

Intuition:

A central path contains $\Omega(\log m)$ gates.

A gate is not k-unbalanced with prob $m^{-\delta}$

Hence, a central path does not contain a k-unbalanced gate with prob $< m^{-\Omega(\log m)}$

Lemma 1: If Ψ is k-weak then

$$\mathrm{Rank}(M_\Psi) \leq |\Psi| \cdot 2^{m-(k/2)}$$

Lemma 2: Assume $|\Psi| < m^{(\log m)/100}$. Partition

$\{x_1,\dots,x_{2m}\}$ □ □□$\{y_1,\dots,y_m\}$ □ $\{z_1,\dots,z_m\}$

then (w.h.p.) Ψ is m^{ε}-weak

Corollary: If for every partition Rank(M_f) □ 2^m then any multilinear formula Ψ for f is of size $m^{\Omega(\log m)}$

Is this true for Determinant or Permanent ?

Not even close...

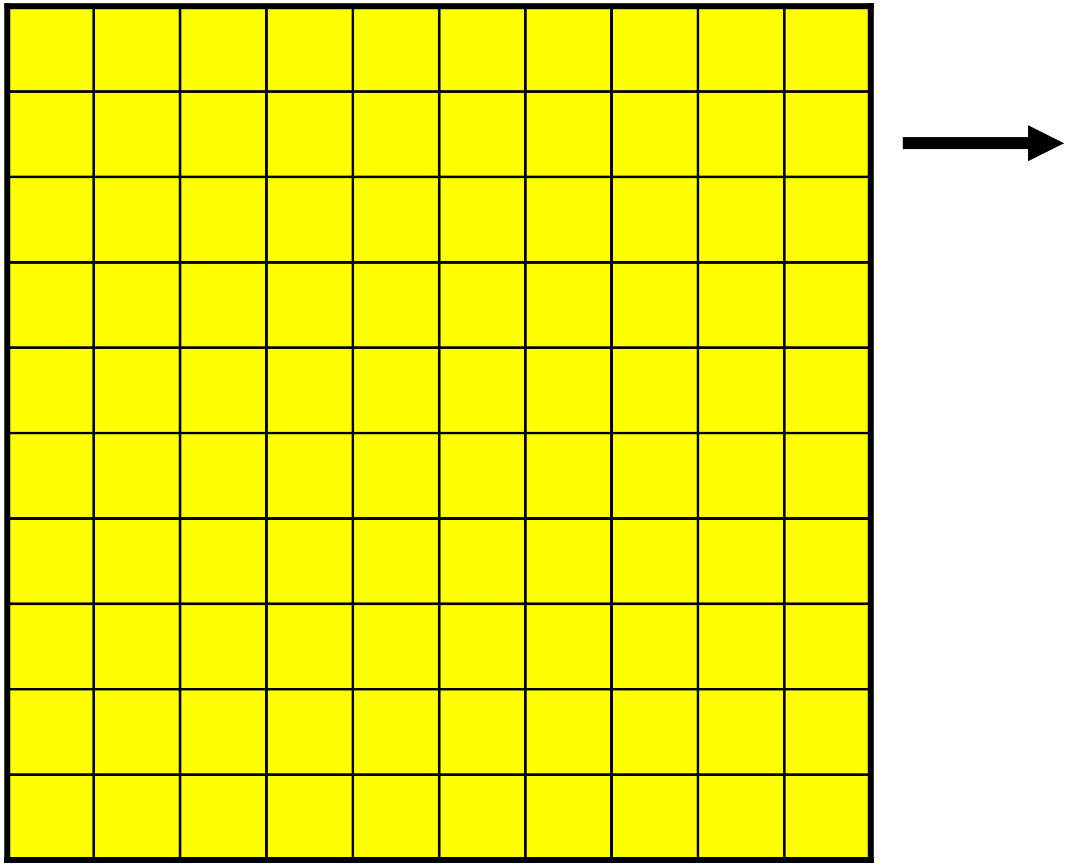
Determinant and Permanent have n^2 inputs. Rank(M_f) is at most 2^n ...

(for any partition)

Determinant and Permanent:

We will map $\{X_{i,j}\}$ □ □□

$\{y_1,...,y_m\}$ □ $\{z_1,...,z_m\}$ □ □$\{0,1\}$

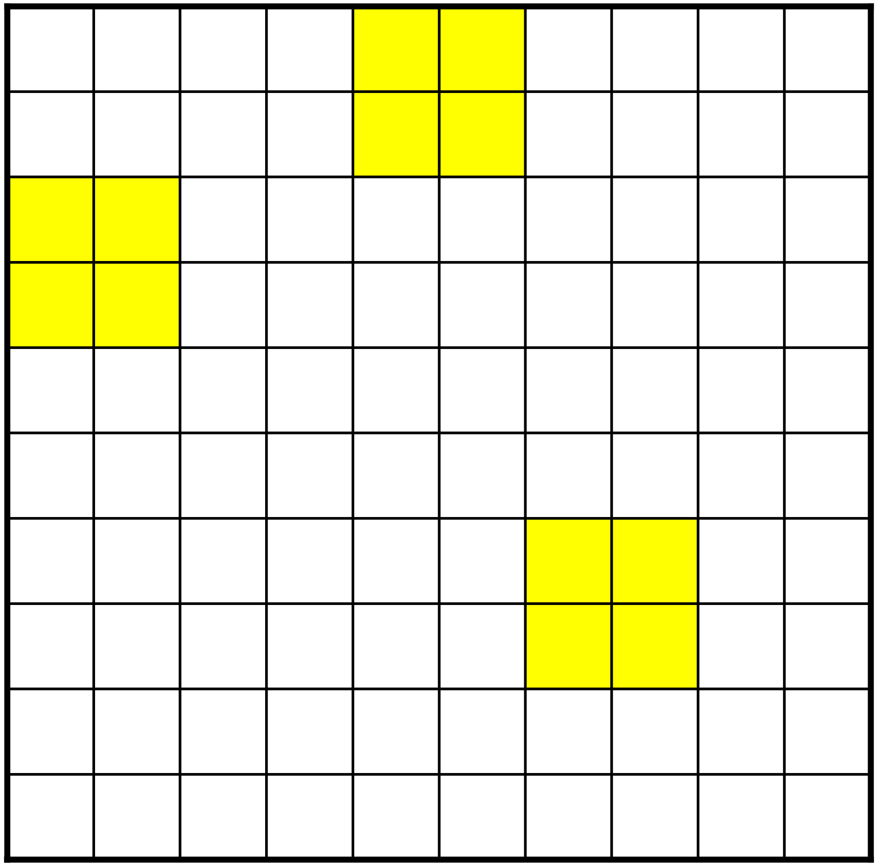


$\{y_1,...,y_m\}$ □

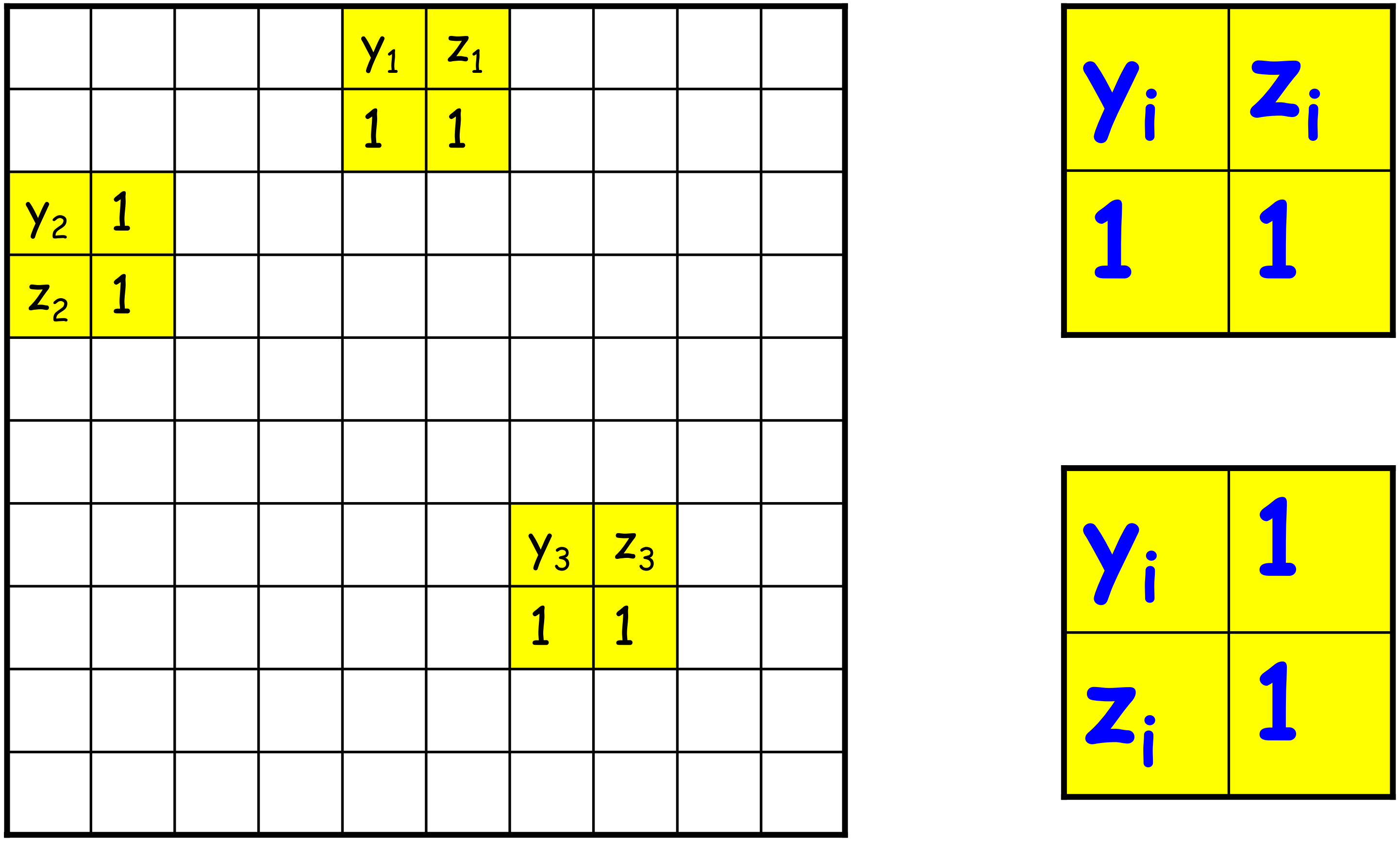
$\{z_1,...,z_m\}$ □ □□□□□

$\{0,1\}$

$(m=n^{\varepsilon})$



Step 1: Choose **m** submatrices of size 2□2 (with different rows and columns).



Step 2: Map submatrix i to either

$$\begin{array}{|c|c|}\hline y_i & z_i \\ \hline 1 & 1 \\ \hline\end{array} \quad \text{or} \quad \begin{array}{|c|c|}\hline y_i & 1 \\ \hline z_i & 1 \\ \hline\end{array}$$

				y_1	z_1				
				1	1				
y_2	1								
z_2	1								
								🟥	
		🟥							
						y_3	z_3		
						1	1		
			🟥						
									🟥

Step 3: Choose a perfect matching of all other rows and columns.

				y_1	z_1				
				1	1				
y_2	1								
z_2	1								
								1	
		1							
						y_3	z_3		
						1	1		
			1						
									1

Step 4: Map the perfect matching to 1 and all other entries to 0.

Lemma:

Assume $|\Psi| < n^{(\log n)/100}$

Map (as above) $\{X_{i,j}\}$ □ □□

$\{y_1,...,y_m\}$ □ $\{z_1,...,z_m\}$ □ □$\{0,1\}$. Then

(w.h.p.): Ψ is k-weak for $k=n^{\varepsilon}$

Corollary: After the mapping,

Rank(M_{Ψ}) < 2^m (w.h.p.)

But Ψ computes the permanent of:

				y_1	z_1				
				1	1				
y_2	1								
z_2	1								
								1	
		1							
						y_3	z_3		
						1	1		
			1						
									1

= **the permanent of:**

y_1	z_1								
1	1								
		y_2	1						
		z_2	1						
				y_3	z_3				
				1	1				
						1			
							1		
								1	
									1

$$= \prod_{i=1}^{m} (y_i + z_i)$$

Thus:

$\mathrm{Rank}(M_{\Psi}) = 2^m$

(contradiction...)

The proof for the determinant is the same, except that we get the polynomial

$$\prod_{i=1}^{m} (y_i - z_i)$$

Additional Research:

[R] Exponential lower bounds for constant depth multilinear formulas

[Aar] Applications to quantum circuits

Open:

1) Lower bounds for multilinear proof systems
2) Separation of multilinear and non-multilinear formula size
3) Polynomial Identity Testing for multilinear formulas

The End