Lower bounds for shallow arithmetic circuits

Ramprasad Saptharishi
Tel Aviv University

Indian Institute of Technology Bombay,
November 2015

Complexity:

Can certain tasks

be computed

under certain resource constraints?

Time Complexity:

Can certain tasks

be computed

by polynomial time algorithms?

Space
Complexity:

Can certain tasks

be computed

by algorithms using just LOG-space?

Communication Complexity:

Can a boolean function $f(\mathbf{x}, \mathbf{y})$

be jointly computed

using very few bits of communication?

Circuit
Complexity:

Can a boolean function $f(\mathbf{x})$

be computed

by polynomial sized boolean circuits?
(made of AND, OR and NOT gates)

Arithmetic Circuit Complexity:

Can a polynomial $f(\mathbf{x})$

be computed

by polynomial sized arithmetic circuits?

(made of $+$ and $\times$ gates)

Arithmetic Circuit
Complexity:

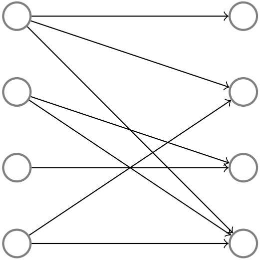
Can a polynomial $f(\mathbf{x})$

be computed

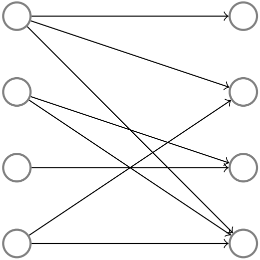
by polynomial sized arithmetic circuits?
(made of $+$ and $\times$ gates)

Focus of this talk

An application

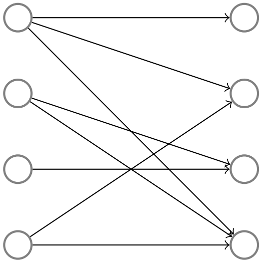


An application



Does there exist a perfect matching?

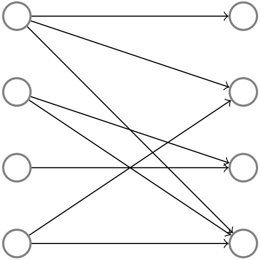
An application



Does there exist a perfect matching?

Want *efficient parallel* algorithms.

An application



Does there exist a perfect matching?

Want *efficient parallel* algorithms.

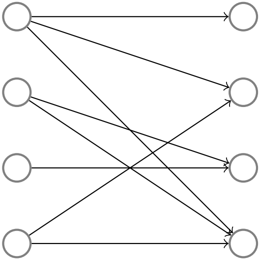
Tutte's Theorem

The graph has a perfect matching *if and only if*

$$\begin{vmatrix} x_{11} & x_{12} & 0 & x_{14} \\ 0 & 0 & x_{23} & x_{24} \\ 0 & 0 & x_{33} & 0 \\ 0 & x_{42} & 0 & x_{44} \end{vmatrix} \neq 0$$

as a formal polynomial.

An application



Does there exist a perfect matching?

Want *efficient parallel* algorithms.

Question: Can we test non-zeroness of “efficient polynomials”?

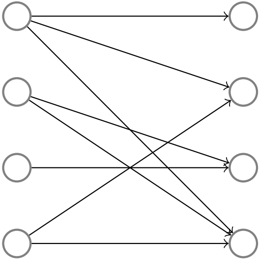
Tutte's Theorem

The graph has a perfect matching *if and only if*

$$\begin{vmatrix} x_{11} & x_{12} & 0 & x_{14} \\ 0 & 0 & x_{23} & x_{24} \\ 0 & 0 & x_{33} & 0 \\ 0 & x_{42} & 0 & x_{44} \end{vmatrix} \neq 0$$

as a formal polynomial.

An application



Does there exist a perfect matching?

Want *efficient parallel* algorithms.

Question: Can we test non-zeroness of "efficient polynomials"?

Firstly, what *are* efficient polynomials?

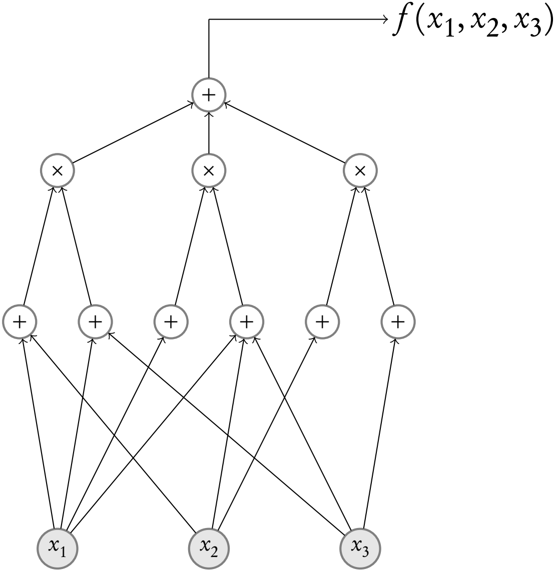
Tutte's Theorem

The graph has a perfect matching *if and only if*

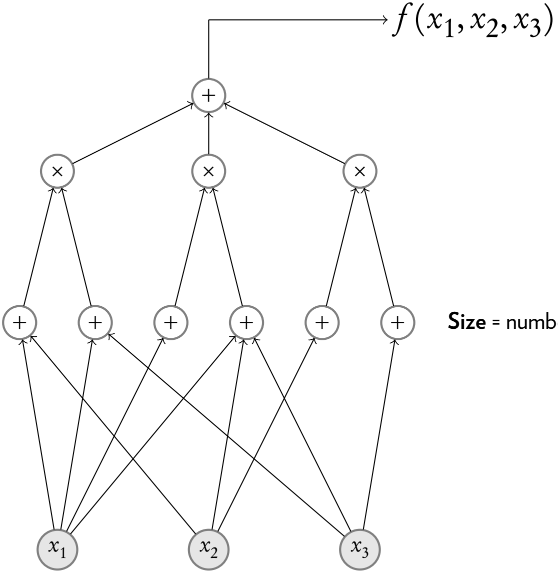
$$\begin{vmatrix} x_{11} & x_{12} & 0 & x_{14} \\ 0 & 0 & x_{23} & x_{24} \\ 0 & 0 & x_{33} & 0 \\ 0 & x_{42} & 0 & x_{44} \end{vmatrix} \neq 0$$

as a formal polynomial.

Arithmetic Circuits

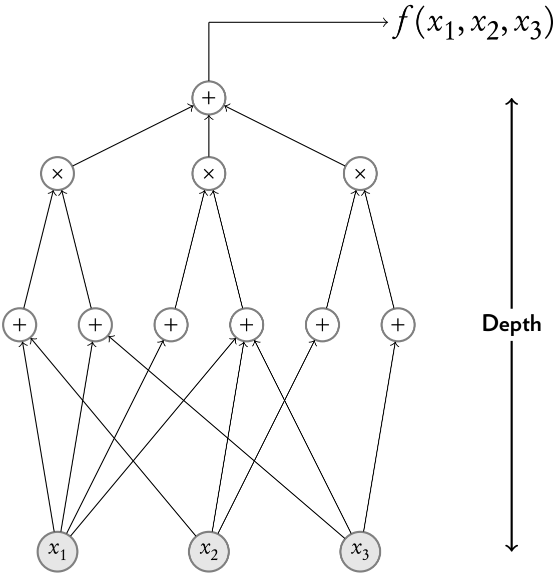


Arithmetic Circuits

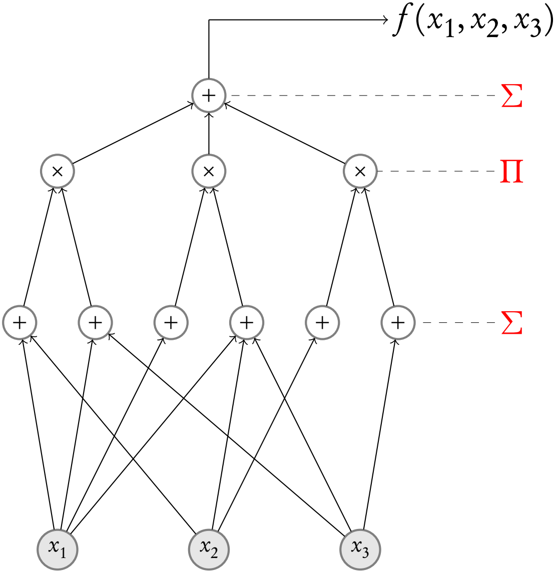


Size = number of gates

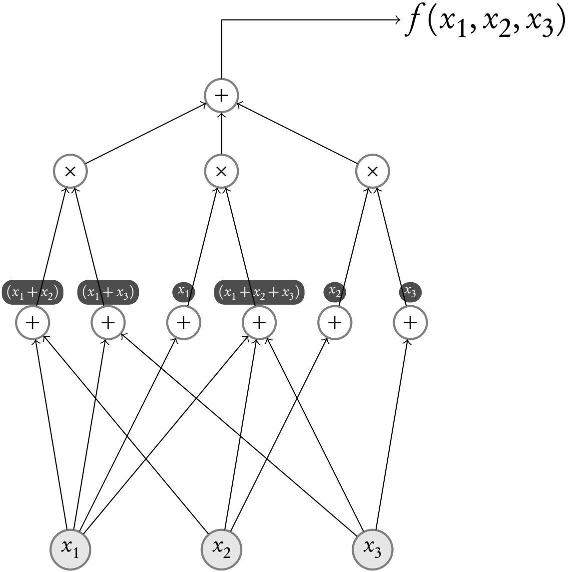
Arithmetic Circuits



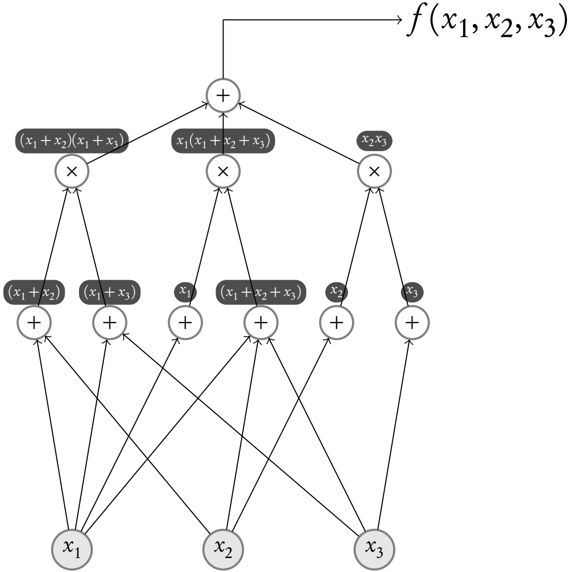
Arithmetic Circuits



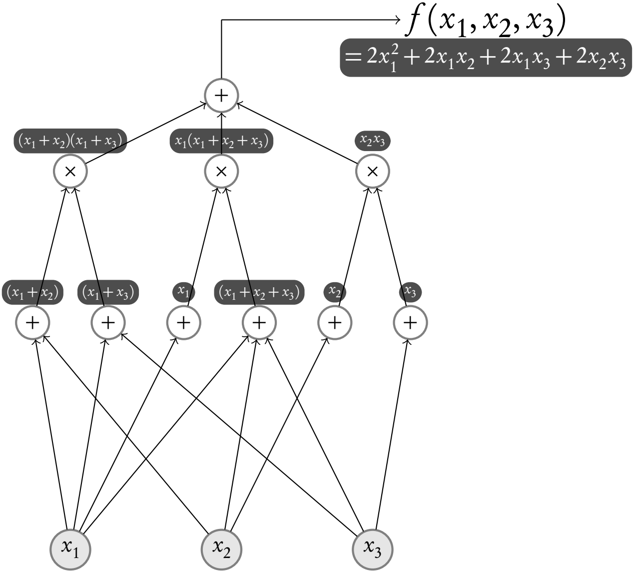
Arithmetic Circuits



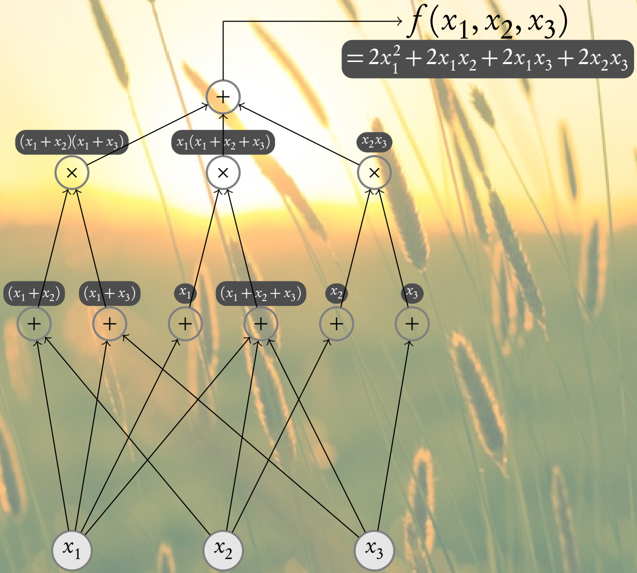
Arithmetic Circuits



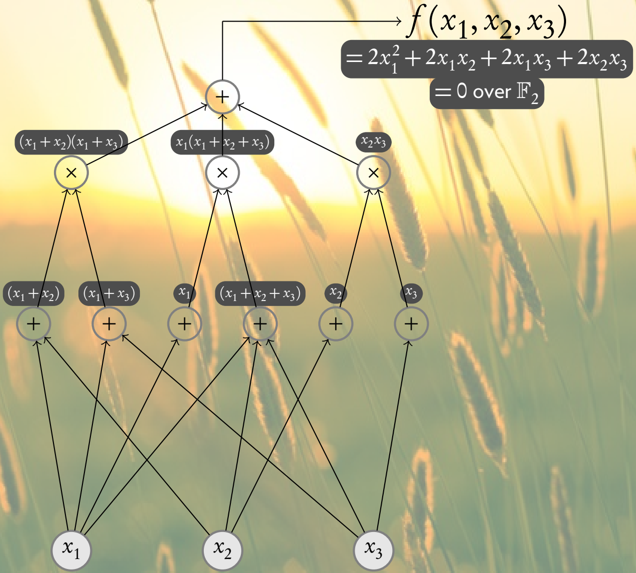
Arithmetic Circuits



Arithmetic Circuits



Arithmetic Circuits



Algebraic analogue of P

Definition (Valiant's P, or efficient computation)

Polynomials $f(x_1, \ldots, x_n)$ that can be computed by $\mathrm{poly}(n)$-sized arithmetic circuits?

Algebraic analogue of P

Definition (Valiant's P, or efficient computation)

Polynomials $f(x_1, \ldots, x_n)$, of degree $d = \mathrm{poly}(n)$, that can be computed by $\mathrm{poly}(n)$-sized arithmetic circuits.

Algebraic analogue of P

Definition (Valiant's P, or efficient computation)

Polynomials $f(x_1, \ldots, x_n)$, of degree $d = \text{poly}(n)$, that can be computed by $\text{poly}(n)$-sized arithmetic circuits.

Examples:

$$\text{[Ben-Or]} \quad \text{ESym}_d(x_1, \cdots, x_n) = \sum_{S \subseteq [n], |S| = d} \prod_{i \in S} x_i$$

$$\text{[Berkowitz,Mahajan-Vinay]} \quad \text{Det}_n = \begin{vmatrix} x_{11} & \cdots & x_{n1} \\ \vdots & \ddots & \vdots \\ x_{n1} & \cdots & x_{nn} \end{vmatrix}$$

Algebraic analogue of P

Definition (Valiant's P, or efficient computation)

Polynomials $f(x_1, \ldots, x_n)$, of degree $d = \mathrm{poly}(n)$, that can be computed by $\mathrm{poly}(n)$-sized arithmetic circuits.

Examples:

$$\text{[Ben-Or]} \quad \mathrm{ESym}_d(x_1, \cdots, x_n) = \sum_{S \subseteq [n], |S| = d} \prod_{i \in S} x_i$$

$$\text{[Berkowitz,Mahajan-Vinay]} \quad \mathrm{Det}_n = \begin{vmatrix} x_{11} & \cdots & x_{n1} \\ \vdots & \ddots & \vdots \\ x_{n1} & \cdots & x_{nn} \end{vmatrix}$$

Fact: [Valiant] Det_n is complete* for VP.

Definition (Valiant's NP, or "explicit polynomials")

"Anything that can be succinctly described"

Examples:

$$\begin{aligned} \text{Perm}_n &= \operatorname{perm}\begin{bmatrix} x_{11} & \cdots & x_{n1} \\ \vdots & \ddots & \vdots \\ x_{n1} & \cdots & x_{nn} \end{bmatrix} \\ &= \sum_{\pi \in S_n} \prod_{i=1}^{n} x_{i\,\pi(i)} \end{aligned}$$

Algebraic analogue of NP

Definition (Valiant's NP, or "explicit polynomials")

"Anything that can be succinctly described"

- Given a monomial, the coefficient can be described easily.

Examples:

$$\text{Perm}_n = \text{perm}\begin{bmatrix} x_{11} & \cdots & x_{n1} \\ \vdots & \ddots & \vdots \\ x_{n1} & \cdots & x_{nn} \end{bmatrix}$$

Algebraic analogue of NP

Definition (Valiant's NP, or "explicit polynomials")

"Anything that can be succinctly described"

- Given a monomial, the coefficient can be described easily.

Examples:

$$\mathrm{Perm}_n \quad = \quad \mathrm{perm}\begin{bmatrix} \ell_{11} & \cdots & \ell_{n1} \\ \vdots & \ddots & \vdots \\ \ell_{n1} & \cdots & \ell_{nn} \end{bmatrix}$$

Algebraic analogue of NP

Definition (Valiant's NP, or "explicit polynomials")

"Anything that can be succinctly described"

- Given a monomial, the coefficient can be described easily.
- An exponential sum of a VP polynomial $g(\mathbf{x}, \mathbf{y})$:

$$f(\mathbf{x}) = \sum_{\mathbf{y} \in \{0,1\}^m} g(\mathbf{x}, \mathbf{y})$$

Algebraic analogue of NP

Definition (Valiant's NP, or "explicit polynomials")

"Anything that can be succinctly described"

- Given a monomial, the coefficient can be described easily.
- An exponential sum of a VP polynomial $g(\mathbf{x}, \mathbf{y})$:

$$f(\mathbf{x}) = \sum_{\mathbf{y} \in \{0,1\}^m} g(\mathbf{x}, \mathbf{y})$$

Fact: [Valiant] Perm_n is complete for VNP.

Algebraic analogue of NP

Definition (Valiant's NP, or "explicit polynomials")

"Anything that can be succinctly described"

- Given a monomial, the coefficient can be described easily.
- An exponential sum of a VP polynomial $g(\mathbf{x}, \mathbf{y})$:

$$f(\mathbf{x}) = \sum_{\mathbf{y} \in \{0,1\}^m} g(\mathbf{x}, \mathbf{y})$$

Fact: [Valiant] Perm_n is complete for VNP.

VP vs VNP

Algebraic analogue of NP

Definition (Valiant's NP, or "explicit polynomials")

"Anything that can be succinctly described"

- Given a monomial, the coefficient can be described easily.
- An exponential sum of a VP polynomial $g(\mathbf{x}, \mathbf{y})$:

$$f(\mathbf{x}) \quad = \quad \sum_{\mathbf{y} \in \{0,1\}^m} g(\mathbf{x}, \mathbf{y})$$

Fact: [Valiant] Perm_n is complete for VNP.

$$\boxed{\text{VP} \quad \text{vs} \quad \text{VNP} \quad \overset{\sim}{\Longleftrightarrow} \quad \text{Det} \quad \text{vs} \quad \text{Perm}}$$

Why?

Why?

Algo Good lower bounds imply good upper bounds for polynomial identity testing. Deterministic algorithms for polynomial identity testing has many applications.

Why?

Algo Good lower bounds imply good upper bounds for polynomial identity testing. Deterministic algorithms for polynomial identity testing has many applications.

Compl. $VP \neq VNP$ is easier to prove than $P \neq NP$.

Why?

Algo Good lower bounds imply good upper bounds for polynomial identity testing. Deterministic algorithms for polynomial identity testing has many applications.

Compl. $\mathrm{VP} \neq \mathrm{VNP}$ is easier to prove than $\mathrm{P} \neq \mathrm{NP}$.

Math. The “Det vs Perm” is a very elegant mathematical question.

Why?

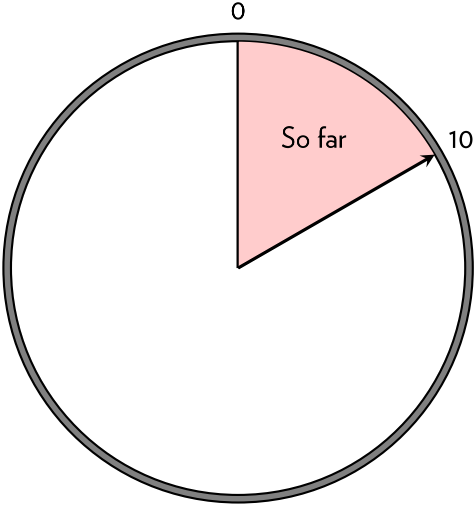
Algo Good lower bounds imply good upper bounds for polynomial identity testing. Deterministic algorithms for polynomial identity testing has many applications.

Compl. VP $\neq$ VNP is easier to prove than P $\neq$ NP.

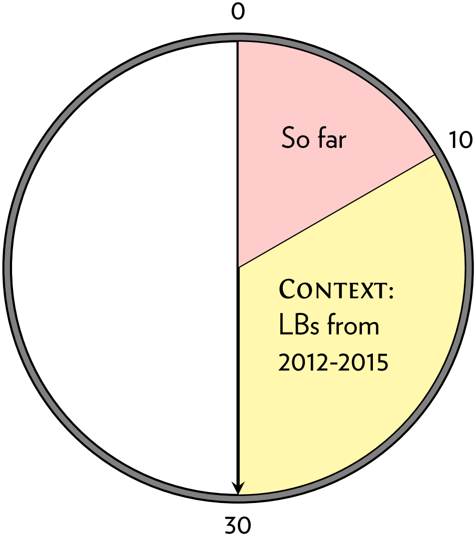
Math. The "Det vs Perm" is a very elegant mathematical question.

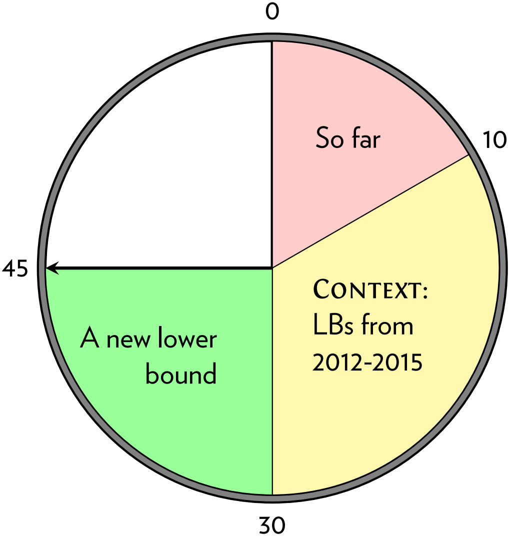
Fame *"The determinant of this conjecture would become permanently famous."*
– Neeraj Kayal

Outline

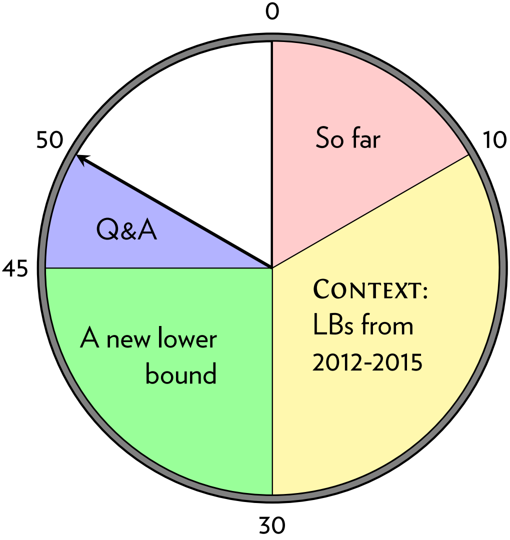


Outline

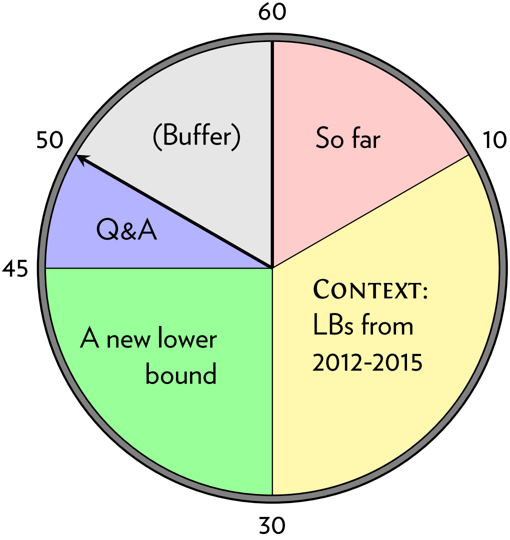



0
So far
10
45
Context:
LBs from
2012-2015
A new lower
bound
30

Outline


0
So far
10
Context:
LBs from
2012-2015
30
A new lower
bound
45
Q&A
50

Outline


60
So far
10
CONTEXT:
LBs from
2012-2015
30
A new lower
bound
45
Q&A
50
(Buffer)

Outline

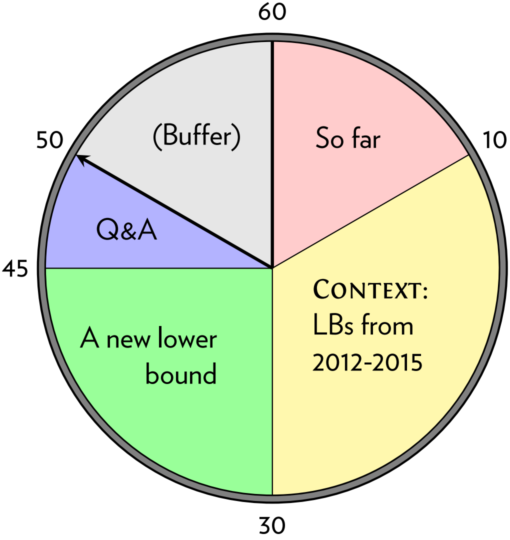


Diagram not to scale

Proof strategies to separate VP and VNP

- **Polynomial identity testing:**
  [Heintz-Schnorr, Kabanets-Impagliazzo, Agrawal]: Strong enough PITs imply lower bounds.

Proof strategies to separate VP and VNP

- **Polynomial identity testing:**
  [Heintz-Schnorr, Kabanets-Impagliazzo, Agrawal]: Strong enough PITs imply lower bounds.

- **Geometric Complexity Theory:**
  [Mulmuley-Sohoni]: The "symmetries" of determinant and permanent are very different. Formalize this via representation theory.

Proof strategies to separate VP and VNP

- **POLYNOMIAL IDENTITY TESTING:**
  [Heintz-Schnorr, Kabanets-Impagliazzo, Agrawal]: Strong enough PITs imply lower bounds.

- **GEOMETRIC COMPLEXITY THEORY:**
  [Mulmuley-Sohoni]: The "symmetries" of determinant and permanent are very different. Formalize this via representation theory.

- **REAL τ-CONJECTURE:**
  [Shub-Smale]: "Simple" polynomials cannot have too many real roots. E.g. If f and g are univariates with s monomials, how many real roots can $fg + 1$ have?

Proof strategies to separate VP and VNP

- **Polynomial identity testing:**
  [Heintz-Schnorr, Kabanets-Impagliazzo, Agrawal]: Strong enough PITs imply lower bounds.

- **Geometric Complexity Theory:**
  [Mulmuley-Sohoni]: The "symmetries" of determinant and permanent are very different. Formalize this via representation theory.

- **Real τ-conjecture:**
  [Shub-Smale]: "Simple" polynomials cannot have too many real roots. E.g. If f and g are univariates with s monomials, how many real roots can $fg + 1$ have?

- **Direct attacks.**

Proof strategies to separate VP and VNP

- **Polynomial identity testing:**
  [Heintz-Schnorr, Kabanets-Impagliazzo, Agrawal]: Strong enough PITs imply lower bounds.

- **Geometric Complexity Theory:**
  [Mulmuley-Sohoni]: The "symmetries" of determinant and permanent are very different. Formalize this via representation theory.

- **Real τ-conjecture:**
  [Shub-Smale]: "Simple" polynomials cannot have too many real roots. E.g. If f and g are univariates with s monomials, how many real roots can $fg+1$ have?

- **Direct attacks.** (This talk.)

How does one begin?

How does one begin?

- [Baur-Strassen 83]: An $\Omega(n \log d)$ lower bound for an explicit polynomial computed by an arithmetic circuit.
- [Kalorkoti 85]: An $\Omega(n^2)$ lower bound for an explicit polynomial computed by an arithmetic formulas.

How does one begin?

- [Baur-Strassen 83]: An $\Omega(n \log d)$ lower bound for an explicit polynomial computed by an arithmetic circuit.
- [Kalorkoti 85]: An $\Omega(n^2)$ lower bound for an explicit polynomial computed by an arithmetic formulas.

"If you can't solve a problem, there is a simpler problem that you can't solve. Find it" – *George Pólya*

How does one begin?

- [Baur-Strassen 83]: An $\Omega(n \log d)$ lower bound for an explicit polynomial computed by an arithmetic circuit.
- [Kalorkoti 85]: An $\Omega(n^2)$ lower bound for an explicit polynomial computed by an arithmetic formulas.

"If you can't solve a problem, there is a simpler problem that you can't solve. Find it" – *George Pólya*

How does one begin?

- [Baur-Strassen 83]: An $\Omega(n \log d)$ lower bound for an explicit polynomial computed by an arithmetic circuit.
- [Kalorkoti 85]: An $\Omega(n^2)$ lower bound for an explicit polynomial computed by an arithmetic formulas.

"If you can't solve a problem, there is a simpler problem that you can't solve. Find it" *– George Pólya*

... lower bounds for small-depth circuits.

$\Sigma\Pi$ circuits

$\Sigma\Pi$ circuits

- **DEPTH-2 CIRCUITS:**
  Sum of few monomials

$\Sigma\Pi$ circuits

- **Depth-2 circuits:**
  Sum of few monomials a.k.a. *sparse* polynomials

$\Sigma\Pi\Sigma$ circuits

- **Depth-2 circuits:**
  Sum of few monomials a.k.a. *sparse* polynomials

- **Depth-3 circuits:**

$\Sigma\Pi\Sigma$ circuits

- **DEPTH-2 CIRCUITS:**
  Sum of few monomials a.k.a. *sparse* polynomials

- **DEPTH-3 CIRCUITS:**
  Sum of products of linear polynomials.

$\Sigma\Pi\Sigma\Pi$ circuits

- **DEPTH-2 CIRCUITS:**
  Sum of few monomials a.k.a. *sparse* polynomials
- **DEPTH-3 CIRCUITS:**
  Sum of products of linear polynomials.
- **DEPTH-4 CIRCUITS:**

$\Sigma\Pi\Sigma\Pi$ circuits

- **DEPTH-2 CIRCUITS:**
  Sum of few monomials a.k.a. *sparse* polynomials
- **DEPTH-3 CIRCUITS:**
  Sum of products of linear polynomials.
- **DEPTH-4 CIRCUITS:**
  Sum of products of sparse polynomials.

$\Sigma\Pi\Sigma\Pi$ circuits

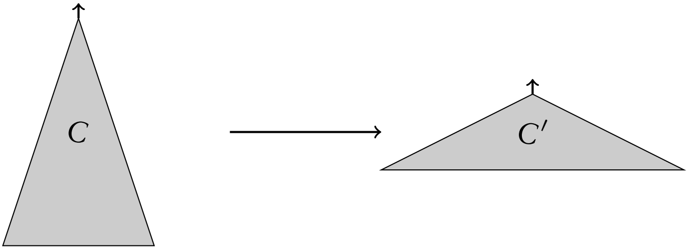
- **Depth-2 circuits:**
  Sum of few monomials a.k.a. *sparse* polynomials
- **Depth-3 circuits:**
  Sum of products of linear polynomials.
- **Depth-4 circuits:**
  Sum of products of sparse polynomials.

How powerful are such shallow circuits?

Depth reduction

Generic depth reduction

Can be computed by		Can be computed by
arithmetic circuits	⟶	“shallow” circuits
of “small” size		of “smallish” size



Depth reduction

Theorem ([Valiant-Skyum-Berkowitz-Rackoff-83])

Can be computed by		*Can be computed by*
arithmetic circuits	$\longrightarrow$	*log-depth circuits*
of $\mathrm{poly}(n,d)$ *size*		*of* $\mathrm{poly}(n,d)$ *size*

Reduction to depth-4

Theorem ([Agrawal-Vinay-08, Koiran-12, Tavenas-13])

Can be computed by		*Can be computed by*
arithmetic circuits	$\longrightarrow$	*depth-4 circuits*
of "small" size		*of "not-too-large" size*

Reduction to depth-4

Theorem ([Agrawal-Vinay-08, Koiran-12, Tavenas-13])

Can be computed by		Can be computed by
arithmetic circuits	⟶	depth-4 circuits
of $\mathrm{poly}(n,d)$ size		of $n^{O(\sqrt{d})}$ size

Reduction to depth-4

Theorem ([Agrawal-Vinay-08, Koiran-12, Tavenas-13])

Can be computed by		Can be computed by
arithmetic circuits	$\longrightarrow$	*depth-4 circuits**
of $\mathrm{poly}(n,d)$ *size*		*of* $n^{O(\sqrt{d})}$ *size*

Reduction to depth-4

Theorem ([Agrawal-Vinay-08, Koiran-12, Tavenas-13])

Can be computed by		Can be computed by
arithmetic circuits	$\longrightarrow$	depth-4 circuits*
of $\mathrm{poly}(n,d)$ size		of $n^{O(\sqrt{d})}$ size

Depth-4 circuits* : $\sum \prod^{\sqrt{d}} \sum \prod^{\sqrt{d}}$ circuits

Reduction to depth-4

Theorem ([Agrawal-Vinay-08, Koiran-12, Tavenas-13])

Can be computed by		*Can be computed by*
arithmetic circuits	$\longrightarrow$	$\Sigma\Pi^{\sqrt{d}}\Sigma\Pi^{\sqrt{d}}$ *circuits*
of $\mathrm{poly}(n, d)$ *size*		*of* $n^{O(\sqrt{d})}$ *size*

Reduction to depth-4

Theorem ([Agrawal-Vinay-08, Koiran-12, Tavenas-13])

Can be computed by		Can be computed by
arithmetic circuits	$\longrightarrow$	$\Sigma\Pi^{\sqrt{d}}\Sigma\Pi^{\sqrt{d}}$ circuits
of $\mathrm{poly}(n,d)$ size		of $n^{O(\sqrt{d})}$ size

(Or)

Cannot be computed by		Cannot be computed by
arithmetic circuits	$\longleftarrow$	$\Sigma\Pi^{\sqrt{d}}\Sigma\Pi^{\sqrt{d}}$ circuits
of $\mathrm{poly}(n,d)$ size		of $n^{O(\sqrt{d})}$ size

Chasm at depth-4

Theorem ([Agrawal-Vinay-08, Koiran-12, Tavenas-13])

Can be computed by		*Can be computed by*
arithmetic circuits	$\longrightarrow$	$\Sigma\Pi^{\sqrt{d}}\Sigma\Pi^{\sqrt{d}}$ *circuits*
of $\mathrm{poly}(n,d)$ *size*		*of* $n^{O(\sqrt{d})}$ *size*

(Or)

Cannot be computed by		*Cannot be computed by*
arithmetic circuits	$\longleftarrow$	$\Sigma\Pi^{\sqrt{d}}\Sigma\Pi^{\sqrt{d}}$ *circuits*
of $\mathrm{poly}(n,d)$ *size*		*of* $n^{O(\sqrt{d})}$ *size*

Chasm at depth-4

Theorem ([Agrawal-Vinay-08, Koiran-12, Tavenas-13])

Can be computed by arithmetic circuits of $\text{poly}(n,d)$ size	$\longrightarrow$	Can be computed by $\Sigma\Pi^{\sqrt{d}}\Sigma\Pi^{\sqrt{d}}$ circuits of $n^{O(\sqrt{d})}$ size

(Or)

Cannot be computed by arithmetic circuits of $\text{poly}(n,d)$ size	$\longleftarrow$	**Cannot** be computed by $\Sigma\Pi^{\sqrt{d}}\Sigma\Pi^{\sqrt{d}}$ circuits of $n^{O(\sqrt{d})}$ size

The first crack in the dam...

Goal: Prove a good enough lower bound for $\sum\prod^{\sqrt{d}}\sum\prod^{\sqrt{d}}$

Goal: Prove a good enough lower bound for $\sum\prod^{\sqrt{d}}\sum\prod^{\sqrt{d}}$

Theorem ([Nisan-Wigderson-95])

An $2^{\Omega(d)}$ lower bound for $\Sigma\Pi^{d}\Sigma\Pi^{1}$ circuits.

The first crack in the dam...

Goal: Prove a good enough lower bound for $\sum\prod^{\sqrt{d}}\sum\prod^{\sqrt{d}}$

Theorem ([Nisan-Wigderson-95])

An $2^{\Omega(d)}$ lower bound for $\Sigma\Pi^{d}\Sigma\Pi^{1}$ circuits.

Theorem ([Kayal-12])

An $2^{\Omega(d)}$ lower bound for $\Sigma\Pi^{d/2}\Sigma\Pi^{2}$ circuits.

The first crack in the dam...

Goal: Prove a good enough lower bound for $\sum\prod^{\sqrt{d}}\sum\prod^{\sqrt{d}}$

Theorem ([Nisan-Wigderson-95])

An $2^{\Omega(d)}$ *lower bound for* $\Sigma\Pi^{d}\Sigma\Pi^{1}$ *circuits.*

Theorem ([Kayal-12])

An $2^{\Omega(d)}$ *lower bound for* $\Sigma\Pi^{d/2}\Sigma\Pi^{2}$ *circuits.*

Theorem ([Gupta-Kamath-Kayal-Saptharishi-12])

An $2^{\Omega(\sqrt{d})}$ *lower bound for* $\Sigma\Pi^{\sqrt{d}}\Sigma\Pi^{\sqrt{d}}$ *circuits.*

The first crack in the dam...

Goal: Prove $n^{\omega(\sqrt{d})}$ lower bound for $\sum\prod^{\sqrt{d}}\sum\prod^{\sqrt{d}}$

Theorem ([Nisan-Wigderson-95])

An $2^{\Omega(d)}$ lower bound for $\Sigma\Pi^{d}\Sigma\Pi^{1}$ circuits.

Theorem ([Kayal-12])

An $2^{\Omega(d)}$ lower bound for $\Sigma\Pi^{d/2}\Sigma\Pi^{2}$ circuits.

Theorem ([Gupta-Kamath-Kayal-Saptharishi-12])

An $2^{\Omega(\sqrt{d})}$ lower bound for $\Sigma\Pi^{\sqrt{d}}\Sigma\Pi^{\sqrt{d}}$ circuits.

... and the deluge that followed

	Lower bound	Circuit class	Polynomial
[GKK_1S_0-12]	$2^{\Omega(\sqrt{d})}$	$\Sigma\Pi^{\sqrt{d}}\Sigma\Pi^{\sqrt{d}}$	VP

G - Ankit Gupta
S_1 - Chandan Saha
S_2 - Srikanth Srinivasan
K - Pritish Kamath
F - Hervé Fournier
K_2 - Mrinal Kumar
K_1 - Neeraj Kayal
L - Nutan Limaye
S_3 - Shubhangi Saraf
S_0 - Ramprasad Saptharishi
M - Guillaume Malod

... and the deluge that followed

	Lower bound	Circuit class	Polynomial
[GKK_1S_0-12]	$2^{\Omega(\sqrt{d})}$	$\Sigma\Pi^{\sqrt{d}}\Sigma\Pi^{\sqrt{d}}$	VP
[$K_1S_1S_0$-13]	$n^{\Omega(\sqrt{d})}$	$\Sigma\Pi^{\sqrt{d}}\Sigma\Pi^{\sqrt{d}}$	VNP

G - Ankit Gupta
S_1 - Chandan Saha
S_2 - Srikanth Srinivasan
K - Pritish Kamath
F - Hervé Fournier
K_2 - Mrinal Kumar
K_1 - Neeraj Kayal
L - Nutan Limaye
S_3 - Shubhangi Saraf
S_0 - Ramprasad Saptharishi
M - Guillaume Malod

... and the deluge that followed

	Lower bound	Circuit class	Polynomial
[GKK_1S_0-12]	$2^{\Omega(\sqrt{d})}$	$\Sigma\Pi^{\sqrt{d}}\Sigma\Pi^{\sqrt{d}}$	VP
[$K_1S_1S_0$-13]	$n^{\Omega(\sqrt{d})}$	$\Sigma\Pi^{\sqrt{d}}\Sigma\Pi^{\sqrt{d}}$	VNP
[$FLMS_2$-13]	$n^{\Omega(\sqrt{d})}$	$\Sigma\Pi^{\sqrt{d}}\Sigma\Pi^{\sqrt{d}}$	VP

G - Ankit Gupta
S_1 - Chandan Saha
S_2 - Srikanth Srinivasan
K - Pritish Kamath
F - Hervé Fournier
K_2 - Mrinal Kumar
K_1 - Neeraj Kayal
L - Nutan Limaye
S_3 - Shubhangi Saraf
S_0 - Ramprasad Saptharishi
M - Guillaume Malod

... and the deluge that followed

	Lower bound	Circuit class	Polynomial
[GKK_1S_0-12]	$2^{\Omega(\sqrt{d})}$	$\Sigma\Pi^{\sqrt{d}}\Sigma\Pi^{\sqrt{d}}$	VP
[$K_1S_1S_0$-13]	$n^{\Omega(\sqrt{d})}$	$\Sigma\Pi^{\sqrt{d}}\Sigma\Pi^{\sqrt{d}}$	VNP
[$FLMS_2$-13]	$n^{\Omega(\sqrt{d})}$	$\Sigma\Pi^{\sqrt{d}}\Sigma\Pi^{\sqrt{d}}$	VP
[K_2S_3-13]	$n^{\Omega(\sqrt{d})}$	$\Sigma\Pi^{\sqrt{d}}\Sigma\Pi^{\sqrt{d}}$	hom. $\Sigma\Pi\Sigma\Pi$

G - Ankit Gupta
S_1 - Chandan Saha
S_2 - Srikanth Srinivasan
K - Pritish Kamath
F - Hervé Fournier
K_2 - Mrinal Kumar
K_1 - Neeraj Kayal
L - Nutan Limaye
S_3 - Shubhangi Saraf
S_0 - Ramprasad Saptharishi
M - Guillaume Malod

... and the deluge that followed

	Lower bound	Circuit class	Polynomial
[GKK_1S_0-12]	$2^{\Omega(\sqrt{d})}$	$\Sigma\Pi^{\sqrt{d}}\Sigma\Pi^{\sqrt{d}}$	VP
[$K_1S_1S_0$-13]	$n^{\Omega(\sqrt{d})}$	$\Sigma\Pi^{\sqrt{d}}\Sigma\Pi^{\sqrt{d}}$	VNP
[$FLMS_2$-13]	$n^{\Omega(\sqrt{d})}$	$\Sigma\Pi^{\sqrt{d}}\Sigma\Pi^{\sqrt{d}}$	VP
[K_2S_3-13]	$n^{\Omega(\sqrt{d})}$	$\Sigma\Pi^{\sqrt{d}}\Sigma\Pi^{\sqrt{d}}$	hom. $\Sigma\Pi\Sigma\Pi$
[$K_1LS_1S_2$-14]	$n^{\Omega(\sqrt{d})}$, over $\mathbb{Q}$	hom. $\Sigma\Pi\Sigma\Pi$	VNP

G - Ankit Gupta
S_1 - Chandan Saha
S_2 - Srikanth Srinivasan
K - Pritish Kamath
F - Hervé Fournier
K_2 - Mrinal Kumar
K_1 - Neeraj Kayal
L - Nutan Limaye
S_3 - Shubhangi Saraf
S_0 - Ramprasad Saptharishi
M - Guillaume Malod

... and the deluge that followed

	Lower bound	Circuit class	Polynomial
[GKK_1S_0-12]	$2^{\Omega(\sqrt{d})}$	$\Sigma\Pi^{\sqrt{d}}\Sigma\Pi^{\sqrt{d}}$	VP
[$K_1S_1S_0$-13]	$n^{\Omega(\sqrt{d})}$	$\Sigma\Pi^{\sqrt{d}}\Sigma\Pi^{\sqrt{d}}$	VNP
[$FLMS_2$-13]	$n^{\Omega(\sqrt{d})}$	$\Sigma\Pi^{\sqrt{d}}\Sigma\Pi^{\sqrt{d}}$	VP
[K_2S_3-13]	$n^{\Omega(\sqrt{d})}$	$\Sigma\Pi^{\sqrt{d}}\Sigma\Pi^{\sqrt{d}}$	hom. $\Sigma\Pi\Sigma\Pi$
[$K_1LS_1S_2$-14]	$n^{\Omega(\sqrt{d})}$, over $\mathbb{Q}$	hom. $\Sigma\Pi\Sigma\Pi$	VNP
[K_2S_3-14]	$n^{\Omega(\sqrt{d})}$	hom. $\Sigma\Pi\Sigma\Pi$	VP

G - Ankit Gupta
S_1 - Chandan Saha
S_2 - Srikanth Srinivasan
K - Pritish Kamath
F - Hervé Fournier
K_2 - Mrinal Kumar
K_1 - Neeraj Kayal
L - Nutan Limaye
S_3 - Shubhangi Saraf
S_0 - Ramprasad Saptharishi
M - Guillaume Malod

... and the deluge that followed

	Lower bound	Circuit class	Polynomial
[GKK_1S_0-12]	$2^{\Omega(\sqrt{d})}$	$\Sigma\Pi^{\sqrt{d}}\Sigma\Pi^{\sqrt{d}}$	VP
[$K_1S_1S_0$-13]	$n^{\Omega(\sqrt{d})}$	$\Sigma\Pi^{\sqrt{d}}\Sigma\Pi^{\sqrt{d}}$	VNP
[$FLMS_2$-13]	$n^{\Omega(\sqrt{d})}$	$\Sigma\Pi^{\sqrt{d}}\Sigma\Pi^{\sqrt{d}}$	VP
[K_2S_3-13]	$n^{\Omega(\sqrt{d})}$	$\Sigma\Pi^{\sqrt{d}}\Sigma\Pi^{\sqrt{d}}$	hom. $\Sigma\Pi\Sigma\Pi$
[$K_1LS_1S_2$-14]	$n^{\Omega(\sqrt{d})}$, over $\mathbb{Q}$	hom. $\Sigma\Pi\Sigma\Pi$	VNP
[K_2S_3-14]	$n^{\Omega(\sqrt{d})}$	hom. $\Sigma\Pi\Sigma\Pi$	VP

...

G - Ankit Gupta
S_1 - Chandan Saha
S_2 - Srikanth Srinivasan
K - Pritish Kamath
F - Hervé Fournier
K_2 - Mrinal Kumar
K_1 - Neeraj Kayal
L - Nutan Limaye
S_3 - Shubhangi Saraf
S_0 - Ramprasad Saptharishi
M - Guillaume Malod

... *another crack in the dam* ...

Theorem ([Agrawal-Vinay-08, Koiran-12, Tavenas-13])

Can be computed by		Can be computed by
arithmetic circuits	$\longrightarrow$	*depth-4 circuits**
of $\mathrm{poly}(n, d)$ *size*		*of* $n^{O(\sqrt{d})}$ *size*

... another crack in the dam ...

Theorem ([Gupta-Kamath-Kayal-Saptharishi-13])

Can be computed by	Over $\mathbb{Q}$	Can be computed by
arithmetic circuits	$\longrightarrow$	*depth-3 circuits**
of $\mathrm{poly}(n, d)$ *size*		*of* $n^{O(\sqrt{d})}$ *size*

... another crack in the dam ...

Theorem ([Gupta-Kamath-Kayal-Saptharishi-13])

Can be computed by	Over $\mathbb{Q}$	Can be computed by
arithmetic circuits	$\longrightarrow$	$\Sigma\Pi\Sigma^{\sqrt{d}}$ circuits
of $\mathrm{poly}(n, d)$ size		of $n^{O(\sqrt{d})}$ size

... another crack in the dam ...

Theorem ([Gupta-Kamath-Kayal-Saptharishi-13])

Can be computed by		Can be computed by
	Over $\mathbb{Q}$	
arithmetic circuits	$\longrightarrow$	$\Sigma\Pi\Sigma^{\sqrt{d}}$ circuits
of $\mathrm{poly}(n,d)$ size		of $n^{O(\sqrt{d})}$ size

Surprising because

- such a result not true over small fields [Grigoriev-Karpinski-98],
- such a result not true for $\Sigma\Pi^{d}\Sigma$ circuits,
- no $\Sigma\Pi\Sigma$ circuit for Det_d was known better than size $d! = d^{O(d)}$ over any field.

... another crack in the dam ...

Theorem ([Gupta-Kamath-Kayal-Saptharishi-13])

Can be computed by	Over $\mathbb{Q}$	Can be computed by
arithmetic circuits	$\longrightarrow$	$\Sigma\Pi\Sigma^{\sqrt{d}}$ circuits
of $\mathrm{poly}(n,d)$ size		of $n^{O(\sqrt{d})}$ size

... *another crack in the dam* ...

Theorem ([Gupta-Kamath-Kayal-Saptharishi-13])

Can be computed by		*Can be computed by*
arithmetic circuits	*Over* $\mathbb{Q}$ $\longrightarrow$	$\Sigma\Pi\Sigma^{\sqrt{d}}$ *circuits*
of $\mathrm{poly}(n,d)$ *size*		*of* $n^{O(\sqrt{d})}$ *size*

Another Goal: Prove an $n^{\omega(\sqrt{d})}$ lower bound for $\Sigma\Pi\Sigma^{\sqrt{d}}$ circuits.

... and more ...

Another Goal: Prove an $n^{\omega(\sqrt{d})}$ lower bound for $\Sigma\Pi\Sigma^{\sqrt{d}}$ circuits.

Another Goal: Prove an $n^{\omega(\sqrt{d})}$ lower bound for $\Sigma\Pi\Sigma^{\sqrt{d}}$ circuits.

	Lower bound	Circuit class	Polynomial
[K_1S_1-15]	$n^{\Omega(\sqrt{d})}$, over $\mathbb{Q}$	$\Sigma\Pi\Sigma^{\sqrt{d}}$, $\Sigma\Pi\Sigma\Pi\Sigma^{n^{1-\epsilon}}$	VNP

K_1 - Neeraj Kayal S_1 - Chandan Saha B - Suman Bera C - Amit Chakrabarti
K_2 - Mrinal Kumar S_3 - Shubhangi Saraf

... and more ...

Another Goal: Prove an $n^{\omega(\sqrt{d})}$ lower bound for $\Sigma\Pi\Sigma^{\sqrt{d}}$ circuits.

	Lower bound	Circuit class	Polynomial
[K_1S_1-15]	$n^{\Omega(\sqrt{d})}$, over $\mathbb{Q}$	$\Sigma\Pi\Sigma^{\sqrt{d}}$, $\Sigma\Pi\Sigma\Pi\Sigma^{n^{1-\epsilon}}$	VNP
[BC-15]	$n^{\Omega(\sqrt{d})}$	$\Sigma\Pi\Sigma\Pi\Sigma^{n^{0.5-\epsilon}}$	VP

K_1 - Neeraj Kayal
K_2 - Mrinal Kumar
S_1 - Chandan Saha
S_3 - Shubhangi Saraf
B - Suman Bera
C - Amit Chakrabarti

... and more ...

Another Goal: Prove an $n^{\omega(\sqrt{d})}$ lower bound for $\Sigma\Pi\Sigma^{\sqrt{d}}$ circuits.

	Lower bound	Circuit class	Polynomial
[K_1S_1-15]	$n^{\Omega(\sqrt{d})}$, over $\mathbb{Q}$	$\Sigma\Pi\Sigma^{\sqrt{d}}$, $\Sigma\Pi\Sigma\Pi\Sigma^{n^{1-\epsilon}}$	VNP
[BC-15]	$n^{\Omega(\sqrt{d})}$	$\Sigma\Pi\Sigma\Pi\Sigma^{n^{0.5-\epsilon}}$	VP
[K_2S_3-15]	$n^{\Omega(\sqrt{d})}$, over $\mathbb{Q}$	$\Sigma\Pi\circledast^{n^{1-\epsilon}}$	VNP

K_1 - Neeraj Kayal S_1 - Chandan Saha B - Suman Bera C - Amit Chakrabarti
K_2 - Mrinal Kumar S_3 - Shubhangi Saraf

... and more ...

Another Goal: Prove an $n^{\omega(\sqrt{d})}$ lower bound for $\Sigma\Pi\Sigma^{\sqrt{d}}$ circuits.

	Lower bound	Circuit class	Polynomial
[K_1S_1-15]	$n^{\Omega(\sqrt{d})}$, over $\mathbb{Q}$	$\Sigma\Pi\Sigma^{\sqrt{d}}$, $\Sigma\Pi\Sigma\Pi\Sigma^{n^{1-\epsilon}}$	VNP
[BC-15]	$n^{\Omega(\sqrt{d})}$	$\Sigma\Pi\Sigma\Pi\Sigma^{n^{0.5-\epsilon}}$	VP
[K_2S_3-15]	$n^{\Omega(\sqrt{d})}$, over $\mathbb{Q}$	$\Sigma\Pi\circledast^{n^{1-\epsilon}}$	VNP
[K_1S_1-15]	$n^{\Omega(\sqrt{d})}$, over $\mathbb{Q}$	$\Sigma\Pi\circledast^{n^{1-\epsilon}}$	VP

K_1 - Neeraj Kayal, S_1 - Chandan Saha, B - Suman Bera, C - Amit Chakrabarti

K_2 - Mrinal Kumar, S_3 - Shubhangi Saraf

Woah... that was a lot of information

Woah... that was a lot of information

- Two possible ways to prove VP $\neq$ VNP:

Prove an $n^{\omega(\sqrt{d})}$ lower bound for $\Sigma\Pi\Sigma^{\sqrt{d}}$ circuits over $\mathbb{Q}$.

Prove an $n^{\omega(\sqrt{d})}$ lower bound for $\Sigma\Pi^{\sqrt{d}}\Sigma\Pi^{\sqrt{d}}$ circuits.

Woah... that was a lot of information

- Two possible ways to prove VP $\neq$ VNP:

  Prove an $n^{\omega(\sqrt{d})}$ lower bound for $\Sigma\Pi\Sigma^{\sqrt{d}}$ circuits over $\mathbb{Q}$.

  Prove an $n^{\omega(\sqrt{d})}$ lower bound for $\Sigma\Pi^{\sqrt{d}}\Sigma\Pi^{\sqrt{d}}$ circuits.

- We already have $n^{\Omega(\sqrt{d})}$ lower bounds in both cases, in fact for slightly more general classes!

Woah... that was a lot of information

- Two possible ways to prove VP $\neq$ VNP:

  Prove an $n^{\omega(\sqrt{d})}$ lower bound for $\Sigma\Pi\Sigma^{\sqrt{d}}$ circuits over $\mathbb{Q}$.

  Prove an $n^{\omega(\sqrt{d})}$ lower bound for $\Sigma\Pi^{\sqrt{d}}\Sigma\Pi^{\sqrt{d}}$ circuits.

- We already have $n^{\Omega(\sqrt{d})}$ lower bounds in both cases, in fact for slightly more general classes!
- It is not abnormal to be super-excited by all this!

Woah... that was a lot of information

- Two possible ways to prove VP $\neq$ VNP:

  Prove an $n^{\omega(\sqrt{d})}$ lower bound for $\Sigma\Pi\Sigma^{\sqrt{d}}$ circuits over $\mathbb{Q}$.

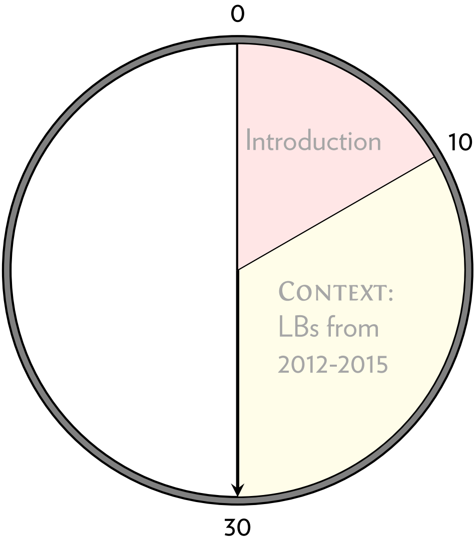
  Prove an $n^{\omega(\sqrt{d})}$ lower bound for $\Sigma\Pi^{\sqrt{d}}\Sigma\Pi^{\sqrt{d}}$ circuits.

- We already have $n^{\Omega(\sqrt{d})}$ lower bounds in both cases, in fact for slightly more general classes!

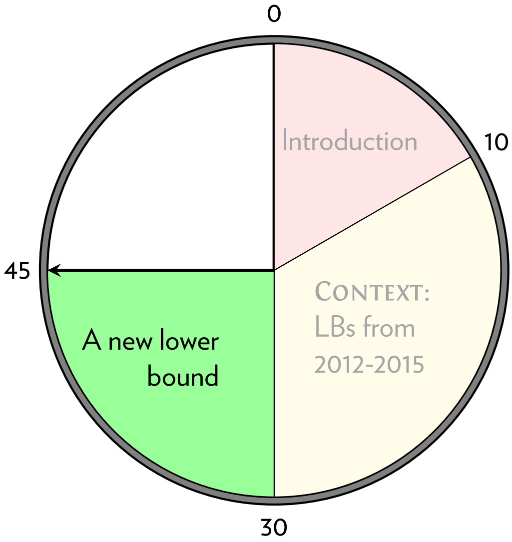
- It is not abnormal to be super-excited by all this!

Self-plug: For those who want to know more details, here is a continuously updated survey: `http://github.com/dasarpmar/lowerbounds-survey/`

Outline



Outline


0
Introduction
10
Context:
LBs from
2012-2015
45
A new lower
bound
30

Natural proof strategies

Construct a map $\Gamma : \mathbb{F}[x_1, \ldots, x_n] \to \mathbb{N}$, that assigns a number to every polynomial such that:

1. If f is computable by "small" circuits, then $\Gamma(f)$ is "small".
2. For the desired polynomial f we wish to show a lower bound, then $\Gamma(f)$ is "large".

Natural proof strategies

Construct a map $\Gamma : \mathbb{F}[x_1, \ldots, x_n] \to \mathbb{N}$, that assigns a number to every polynomial such that:
Typically $\Gamma(f)$ is the rank of some associated linear space.

1. If f is computable by "small" circuits, then $\Gamma(f)$ is "small".
2. For the desired polynomial f we wish to show a lower bound, then $\Gamma(f)$ is "large".

- [Nisan-Wigderson-95]: $\Sigma\Pi^d\Sigma$ circuits, sum of terms of the form $\ell_1 \cdots \ell_d$.

- [Nisan-Wigderson-95]: $\Sigma\Pi^d\Sigma$ circuits, sum of terms of the form $\ell_1 \cdots \ell_d$.
  Key observation: There are just 2^d linearly independent partial derivatives of $\ell_1 \cdots \ell_d$.

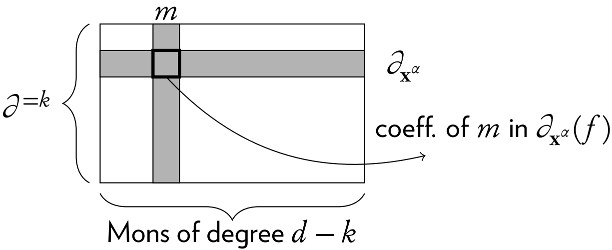
- [Nisan-Wigderson-95]: $\Sigma\Pi^d\Sigma$ circuits, sum of terms of the form $\ell_1 \cdots \ell_d$.
  Key observation: There are just 2^d linearly independent partial derivatives of $\ell_1 \cdots \ell_d$.

$$
\begin{aligned}
\partial_x(\ell_1 \cdots \ell_d) &= \partial_x(\ell_1) \cdot \ell_2 \cdots \ell_d + \cdots + \ell_1 \cdots \ell_{d-1} \cdot \partial_x(\ell_d) \\
&\in \operatorname{span}\left\{ \prod_{i \in S} \ell_i \; : \; S \subset [d] \, , \, |S| = d-1 \right\}
\end{aligned}
$$

- [Nisan-Wigderson-95]: $\Sigma\Pi^d\Sigma$ circuits, sum of terms of the form $\ell_1 \cdots \ell_d$.
  Key observation: There are just 2^d linearly independent partial derivatives of $\ell_1 \cdots \ell_d$.
  A generic polynomial is expected to have $n^{\Omega(d)}$ independent partial derivatives.

- [Nisan-Wigderson-95]: $\Sigma\Pi^d\Sigma$ circuits, sum of terms of the form $\ell_1 \cdots \ell_d$.
  Key observation: There are "few" linearly independent partial derivatives of $\ell_1 \cdots \ell_d$.

- [Nisan-Wigderson-95]: $\Sigma\Pi^d\Sigma$ circuits, sum of terms of the form $\ell_1 \cdots \ell_d$.
  Key observation: There are "few" linearly independent partial derivatives of $\ell_1 \cdots \ell_d$.



Examples

- [Nisan-Wigderson-95]: $\Sigma\Pi^d\Sigma$ circuits, sum of terms of the form $\ell_1 \cdots \ell_d$.
  Key observation: There are “few” linearly independent partial derivatives of $\ell_1 \cdots \ell_d$.
- [Gupta-Kamath-Kayal-Saptharishi-12]: $\Sigma\Pi^{\sqrt{d}}\Sigma\Pi^{\sqrt{d}}$ circuits, terms of the form $Q_1 \cdots Q_{\sqrt{d}}$.

Examples

- [Nisan-Wigderson-95]: $\Sigma\Pi^d\Sigma$ circuits, sum of terms of the form $\ell_1 \cdots \ell_d$.
  Key observation: There are "few" linearly independent partial derivatives of $\ell_1 \cdots \ell_d$.
- [Gupta-Kamath-Kayal-Saptharishi-12]: $\Sigma\Pi^{\sqrt{d}}\Sigma\Pi^{\sqrt{d}}$ circuits, terms of the form $Q_1 \cdots Q_{\sqrt{d}}$.

$$\begin{aligned} \partial_x(Q_1 \cdots Q_r) &= \partial_x(Q_1) \cdot Q_2 \cdots Q_r + \cdots + Q_1 \cdots Q_{r-1} \cdot \partial_x(Q_r) \\ &\in \operatorname{span}\left\{ \mathbf{x}^{=\sqrt{d}} \cdot \prod_{i \in S} Q_i \ : \ S \subset [r], |S| = r-1 \right\} \end{aligned}$$

- [Nisan-Wigderson-95]: $\Sigma\Pi^d\Sigma$ circuits, sum of terms of the form $\ell_1 \cdots \ell_d$.
  Key observation: There are "few" linearly independent partial derivatives of $\ell_1 \cdots \ell_d$.
- [Gupta-Kamath-Kayal-Saptharishi-12]: $\Sigma\Pi^{\sqrt{d}}\Sigma\Pi^{\sqrt{d}}$ circuits, terms of the form $Q_1 \cdots Q_{\sqrt{d}}$.

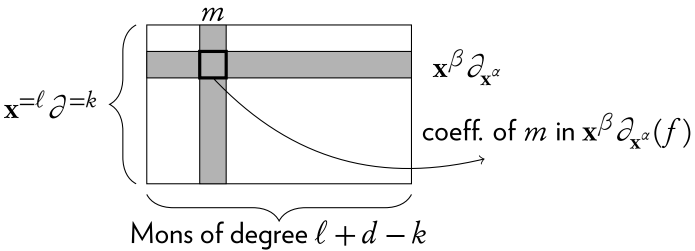
$$\begin{aligned}\partial_x(Q_1 \cdots Q_r) &= \partial_x(Q_1) \cdot Q_2 \cdots Q_r + \cdots + Q_1 \cdots Q_{r-1} \cdot \partial_x(Q_r) \\ &\in \operatorname{span}\left\{ \mathbf{x}^{=\sqrt{d}} \cdot \prod_{i \in S} Q_i \ : \ S \subset [r], |S| = r-1 \right\}\end{aligned}$$

Key observation: Many *low-degree* combinations of partial derivatives are zero if all Q_is have low degree.

Examples

- [Nisan-Wigderson-95]: $\Sigma\Pi^d\Sigma$ circuits, sum of terms of the form $\ell_1 \cdots \ell_d$.
  Key observation: There are "few" linearly independent partial derivatives of $\ell_1 \cdots \ell_d$.
- [Gupta-Kamath-Kayal-Saptharishi-12]: $\Sigma\Pi^{\sqrt{d}}\Sigma\Pi^{\sqrt{d}}$ circuits, terms of the form $Q_1 \cdots Q_{\sqrt{d}}$.
  Key observation: Many *low-degree* combinations of partial derivatives are zero if all Q_is have low degree.

- [Nisan-Wigderson-95]: $\Sigma\Pi^d\Sigma$ circuits, sum of terms of the form $\ell_1 \cdots \ell_d$.
  Key observation: There are "few" linearly independent partial derivatives of $\ell_1 \cdots \ell_d$.
- [Gupta-Kamath-Kayal-Saptharishi-12]: $\Sigma\Pi^{\sqrt{d}}\Sigma\Pi^{\sqrt{d}}$ circuits, terms of the form $Q_1 \cdots Q_{\sqrt{d}}$.
  Key observation: Many *low-degree* combinations of partial derivatives are zero if all Q_is have low degree.



- [Gupta-Kamath-Kayal-Saptharishi-12]: $\Sigma\Pi^{\sqrt{d}}\Sigma\Pi^{\sqrt{d}}$ circuits, terms of the form $Q_1 \cdots Q_{\sqrt{d}}$.
  Key observation: Many *low-degree* combinations of partial derivatives are zero if all Q_is have low degree.

Examples...

- [Gupta-Kamath-Kayal-Saptharishi-12]: $\Sigma\Pi^{\sqrt{d}}\Sigma\Pi^{\sqrt{d}}$ circuits, terms of the form $Q_1 \cdots Q_{\sqrt{d}}$.
  Key observation: Many *low-degree* combinations of partial derivatives are zero if all Q_is have low degree.

- hom. $\Sigma\Pi\Sigma\Pi$ circuits: terms like $Q_1 \cdots Q_b$ with total degree d.

Examples...

- [Gupta-Kamath-Kayal-Saptharishi-12]: $\Sigma\Pi^{\sqrt{d}}\Sigma\Pi^{\sqrt{d}}$ circuits, terms of the form $Q_1 \cdots Q_{\sqrt{d}}$.
  Key observation: Many *low-degree* combinations of partial derivatives are zero if all Q_is have low degree.

- hom. $\Sigma\Pi\Sigma\Pi$ circuits: terms like $Q_1 \cdots Q_b$ with total degree d.

- [Gupta-Kamath-Kayal-Saptharishi-12]: $\Sigma\Pi^{\sqrt{d}}\Sigma\Pi^{\sqrt{d}}$ circuits, terms of the form $Q_1 \cdots Q_{\sqrt{d}}$.
  Key observation: Many *low-degree* combinations of partial derivatives are zero if all Q_is have low degree.

- hom. $\Sigma\Pi\Sigma\Pi$ circuits: terms like $Q_1 \cdots Q_b$ with total degree d.

Low degree mons.	High degree mons.

Examples...

- [Gupta-Kamath-Kayal-Saptharishi-12]: $\Sigma\Pi^{\sqrt{d}}\Sigma\Pi^{\sqrt{d}}$ circuits, terms of the form $Q_1 \cdots Q_{\sqrt{d}}$.
  Key observation: Many *low-degree* combinations of partial derivatives are zero if all Q_is have low degree.
- hom. $\Sigma\Pi\Sigma\Pi$ circuits: terms like $Q_1 \cdots Q_b$ with total degree d.

Low degree mons.	High degree mons.
✓ [GKKS-12]	

Examples...

- [Gupta-Kamath-Kayal-Saptharishi-12]: $\Sigma\Pi^{\sqrt{d}}\Sigma\Pi^{\sqrt{d}}$ circuits, terms of the form $Q_1 \cdots Q_{\sqrt{d}}$.
  Key observation: Many *low-degree* combinations of partial derivatives are zero if all Q_is have low degree.
- hom. $\Sigma\Pi\Sigma\Pi$ circuits: terms like $Q_1 \cdots Q_b$ with total degree d.

Low degree mons.	High degree large support mons.	High degree small support mons.
✓ [GKKS-12]	Eg. $x_1 \cdots x_d$	Eg. $x_1^{d/2} x_2^{d/2}$

- [Gupta-Kamath-Kayal-Saptharishi-12]: $\Sigma\Pi^{\sqrt{d}}\Sigma\Pi^{\sqrt{d}}$ circuits, terms of the form $Q_1 \cdots Q_{\sqrt{d}}$.
  Key observation: Many *low-degree* combinations of partial derivatives are zero if all Q_is have low degree.

- hom. $\Sigma\Pi\Sigma\Pi$ circuits: terms like $Q_1 \cdots Q_b$ with total degree d.

Low degree mons.	High degree large support mons.	High degree small support mons.
✓ [GKKS-12]	Eg. $x_1 \cdots x_d$	Eg. $x_1^{d/2} x_2^{d/2}$

  - IDEA 1 - RANDOM RESTRICTIONS: Randomly set a small number of variables to zero

- [Gupta-Kamath-Kayal-Saptharishi-12]: $\Sigma\Pi^{\sqrt{d}}\Sigma\Pi^{\sqrt{d}}$ circuits, terms of the form $Q_1 \cdots Q_{\sqrt{d}}$.
  Key observation: Many *low-degree* combinations of partial derivatives are zero if all Q_is have low degree.
- hom. $\Sigma\Pi\Sigma\Pi$ circuits: terms like $Q_1 \cdots Q_b$ with total degree d.

Low degree mons.	~~High degree large support mons.~~	High degree small support mons.
✓ [GKKS-12]	~~Eg. $x_1 \cdots x_d$~~	Eg. $x_1^{d/2} x_2^{d/2}$

  - IDEA 1 - RANDOM RESTRICTIONS: Randomly set a small number of variables to zero

Examples...

- [Gupta-Kamath-Kayal-Saptharishi-12]: $\Sigma\Pi^{\sqrt{d}}\Sigma\Pi^{\sqrt{d}}$ circuits, terms of the form $Q_1 \cdots Q_{\sqrt{d}}$.
  Key observation: Many *low-degree* combinations of partial derivatives are zero if all Q_is have low degree.
- hom. $\Sigma\Pi\Sigma\Pi$ circuits: terms like $Q_1 \cdots Q_b$ with total degree d.

Low degree mons.	High degree large support mons.	High degree small support mons.
✓ [GKKS-12]	Eg. $x_1 \cdots x_d$	Eg. $x_1^{d/2} x_2^{d/2}$

- IDEA 1 - RANDOM RESTRICTIONS: Randomly set a small number of variables to zero
- IDEA 2 - MULTILINEAR PROJECTION: Discard all non-multilinear monomials

Examples...

- [Gupta-Kamath-Kayal-Saptharishi-12]: $\Sigma\Pi^{\sqrt{d}}\Sigma\Pi^{\sqrt{d}}$ circuits, terms of the form $Q_1 \cdots Q_{\sqrt{d}}$.
  Key observation: Many *low-degree* combinations of partial derivatives are zero if all Q_is have low degree.

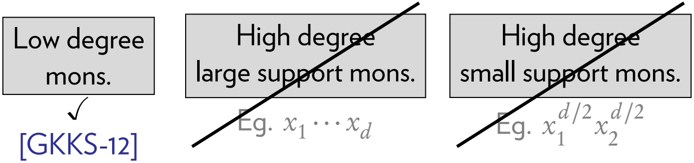
- hom. $\Sigma\Pi\Sigma\Pi$ circuits: terms like $Q_1 \cdots Q_b$ with total degree d.

Low degree mons.	~~High degree large support mons.~~	~~High degree small support mons.~~
✓ [GKKS-12]	~~Eg. $x_1 \cdots x_d$~~	~~Eg. $x_1^{d/2} x_2^{d/2}$~~

  - IDEA 1 - RANDOM RESTRICTIONS: Randomly set a small number of variables to zero
  - IDEA 2 - MULTILINEAR PROJECTION: Discard all non-multilinear monomials

- [Gupta-Kamath-Kayal-Saptharishi-12]: $\Sigma\Pi^{\sqrt{d}}\Sigma\Pi^{\sqrt{d}}$ circuits, terms of the form $Q_1 \cdots Q_{\sqrt{d}}$.
  Key observation: Many *low-degree* combinations of partial derivatives are zero if all Q_is have low degree.

- [Kayal-Limaye-Saha-Srinivasan-13], [Kumar-Saraf-13]:
  hom. $\Sigma\Pi\Sigma\Pi$ circuits: terms like $Q_1 \cdots Q_b$ with total degree d.



  - IDEA 1 - RANDOM RESTRICTIONS: Randomly set a small number of variables to zero
  - IDEA 2 - MULTILINEAR PROJECTION: Discard all non-multilinear monomials

Examples...

- [Kayal-Limaye-Saha-Srinivasan-13], [Kumar-Saraf-13]:
  hom. $\Sigma\Pi\Sigma\Pi$ circuits: terms like $Q_1 \cdots Q_b$ with total degree d.
  - IDEA 1 - RANDOM RESTRICTIONS: Randomly set a small number of variables to zero
  - IDEA 2 - MULTILINEAR PROJECTION: Discard all non-multilinear monomials

Examples...

- [Kayal-Limaye-Saha-Srinivasan-13], [Kumar-Saraf-13]:
  hom. $\Sigma\Pi\Sigma\Pi$ circuits: terms like $Q_1 \cdots Q_b$ with total degree d.

  - Idea 1 - Random restrictions: Randomly set a small number of variables to zero
  - Idea 2 - Multilinear projection: Discard all non-multilinear monomials

$$\Gamma(f) \quad = \quad \dim(\mathbf{x}^{=\ell} \partial^{=k}(f))$$

Dimension of shifted partials of f.

Examples...

- [Kayal-Limaye-Saha-Srinivasan-13], [Kumar-Saraf-13]:
  hom. $\Sigma\Pi\Sigma\Pi$ circuits: terms like $Q_1 \cdots Q_b$ with total degree d.
  - IDEA 1 - RANDOM RESTRICTIONS: Randomly set a small number of variables to zero
  - IDEA 2 - MULTILINEAR PROJECTION: Discard all non-multilinear monomials

$$\Gamma(f) \quad = \quad \dim(\mathbf{x}^{=\ell}\partial^{=k}(\rho(f)))$$

Dimension of shifted partials of a random restriction of f.

Examples...

- [Kayal-Limaye-Saha-Srinivasan-13], [Kumar-Saraf-13]:
  hom. $\Sigma\Pi\Sigma\Pi$ circuits: terms like $Q_1 \cdots Q_b$ with total degree d.
  - IDEA 1 - RANDOM RESTRICTIONS: Randomly set a small number of variables to zero
  - IDEA 2 - MULTILINEAR PROJECTION: Discard all non-multilinear monomials

$$\Gamma(f) \quad = \quad \dim(\mathrm{mult} \circ \mathbf{x}^{=\ell} \partial^{=k}(\rho(f)))$$

Dimension of projected shifted partials of a random restriction of f.

Examples...

- [Kayal-Limaye-Saha-Srinivasan-13], [Kumar-Saraf-13]:
  hom. $\Sigma\Pi\Sigma\Pi$ circuits: terms like $Q_1 \cdots Q_b$ with total degree d.

$$\Gamma(f) \quad = \quad \dim(\mathrm{mult} \circ \mathbf{x}^{=\ell} \partial^{=k}(\rho(f)))$$

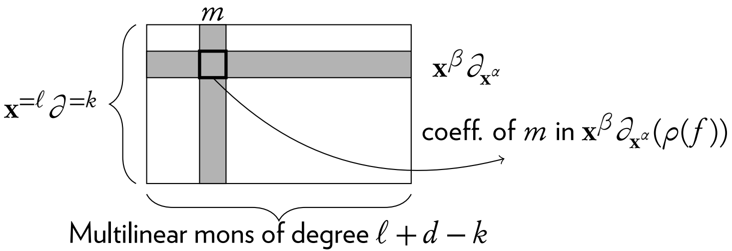
Dimension of projected shifted partials of a random restriction of f.

Examples...

- [Kayal-Limaye-Saha-Srinivasan-13], [Kumar-Saraf-13]:
  hom. $\Sigma\Pi\Sigma\Pi$ circuits: terms like $Q_1 \cdots Q_b$ with total degree d.

$$\Gamma(f) \quad = \quad \dim(\text{mult} \circ \mathbf{x}^{=\ell} \partial^{=k}(\rho(f)))$$

Dimension of projected shifted partials of a random restriction of f.



Moving to depth five

$$\Sigma\Pi\Sigma\Pi\Sigma$$

Sums of products of depth-3 circuits

$\Sigma\Pi\Sigma\Pi\Sigma$

Sums of products of depth-3 circuits

- Projected shifted partials heavily rely on *monomials* and *sparsity*.

$\Sigma\Pi\Sigma\Pi\Sigma$

Sums of products of depth-3 circuits

- Projected shifted partials heavily rely on *monomials* and *sparsity*.
- Even a single term $(x_1 + \cdots + x_n)^d$ can mess up sparsity.

$$\Sigma\Pi\Sigma\Pi\Sigma$$

Sums of products of depth-3 circuits

- Projected shifted partials heavily rely on *monomials* and *sparsity*.
- Even a single term $(x_1 + \cdots + x_n)^d$ can mess up sparsity.
  If bottom sparsity controlled, similar technique works.

$$\Sigma\Pi\Sigma\Pi\Sigma^{n^{0.5-\epsilon}}$$

Sums of products of depth-3 circuits

- Projected shifted partials heavily rely on *monomials* and *sparsity*.
- Even a single term $(x_1 + \cdots + x_n)^d$ can mess up sparsity.
  If bottom sparsity controlled, similar technique works.
  [Bera-Chakrabarti-15]

Moving to depth five

$$\Sigma\Pi\Sigma\Pi\Sigma^{n^{1-\epsilon}}$$

Sums of products of depth-3 circuits

- Projected shifted partials heavily rely on *monomials* and *sparsity*.
- Even a single term $(x_1 + \cdots + x_n)^d$ can mess up sparsity.
  If bottom sparsity controlled, similar technique works.
  [Bera-Chakrabarti-15], [Kayal-Saha-15]

$\Sigma\Pi\Sigma\Pi\Sigma$

Sums of products of depth-3 circuits

- Projected shifted partials heavily rely on *monomials* and *sparsity*.
- Even a single term $(x_1 + \cdots + x_n)^d$ can mess up sparsity.
  If bottom sparsity controlled, similar technique works.

$\Sigma\Pi\Sigma\Pi\Sigma$

Sums of products of depth-3 circuits

- Projected shifted partials heavily rely on *monomials* and *sparsity*.
- Even a single term $(x_1 + \cdots + x_n)^d$ can mess up sparsity.
  If bottom sparsity controlled, similar technique works.
- What is the right analogue of 'support' here?

$$\Sigma\Pi\Sigma\Pi\Sigma$$

Sums of products of depth-3 circuits

- Projected shifted partials heavily rely on *monomials* and *sparsity*.
- Even a single term $(x_1 + \cdots + x_n)^d$ can mess up sparsity.
  If bottom sparsity controlled, similar technique works.
- What is the right analogue of 'support' here?
- **Answer:** The rank.

Types of products of linear polynomials:

Low degree products.	High degree products.

Types of products of linear polynomials:

Low degree products.	High degree products.
✓ [GKKS-12]	

Types of products of linear polynomials:

Low degree products.	High degree, large rank products.	High degree, small rank products.
✓ [GKKS-12]	Eg. $\ell_1 \cdots \ell_d$	Eg. $\ell_1^{d/2} \ell_2^{d/2}$

Types of products of linear polynomials:

Low degree products.	High degree, large rank products.	High degree, small rank products.
✓ [GKKS-12]	Eg. $\ell_1 \cdots \ell_d$	Eg. $\ell_1^{d/2} \ell_2^{d/2}$

- **IDEA 1 - MULTILINEARIZATION:**
  Looking at only evaluations on $\{0,1\}^n$.

Types of products of linear polynomials:

Low degree products.	High degree, large rank products.	High degree, small rank products.
√ [GKKS-12]	Eg. $\ell_1 \cdots \ell_d$	Eg. $\ell_1^{d/2} \ell_2^{d/2}$

- **IDEA 1 - MULTILINEARIZATION:**
  Looking at only evaluations on $\{0,1\}^n$. Low rank $\implies$ low degree as $x_i^2 = x_i$ on $\{0,1\}^n$.

Types of products of linear polynomials:

Low degree products.	High degree, large rank products.	High degree, small rank products.
✓ [GKKS-12]	Eg. $\ell_1 \cdots \ell_d$	Eg. $\ell_1^{d/2} \ell_2^{d/2}$ ✓

- **Idea 1 - Multilinearization:**
  Looking at only evaluations on $\{0,1\}^n$. Low rank $\implies$ low degree as $x_i^2 = x_i$ on $\{0,1\}^n$.

Types of products of linear polynomials:

Low degree products.	High degree, large rank products.	High degree, small rank products.
✓ [GKKS-12]	Eg. $\ell_1 \cdots \ell_d$	Eg. $\ell_1^{d/2} \ell_2^{d/2}$ ✓

- **IDEA 1 - MULTILINEARIZATION:**
  Looking at only evaluations on $\{0,1\}^n$. Low rank $\implies$ low degree as $x_i^2 = x_i$ on $\{0,1\}^n$. (Multilinear projection is $x_i^2 = 0$.)

Types of products of linear polynomials:

Low degree products.	High degree, large rank products.	High degree, small rank products.
✓ [GKKS-12]	Eg. $\ell_1 \cdots \ell_d$	Eg. $\ell_1^{d/2} \ell_2^{d/2}$ ✓

- **IDEA 1 - MULTILINEARIZATION:** Looking at only evaluations on $\{0,1\}^n$. Low rank $\implies$ low degree as $x_i^2 = x_i$ on $\{0,1\}^n$. (Multilinear projection is $x_i^2 = 0$.)
- **IDEA 2 - HIGH-RANK EVALUATIONS OVER $\mathbb{F}_q$:** Over a small field, large rank terms almost always evaluate to zero.

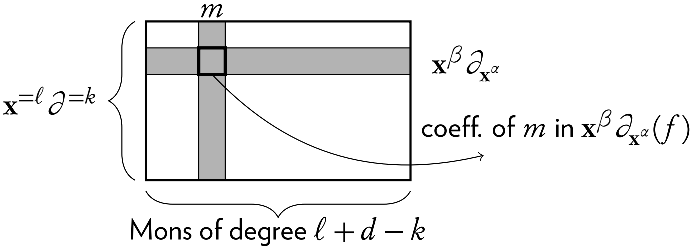
Types of products of linear polynomials:

Low degree products.	High degree, large rank products.	High degree, small rank products.
✓ [GKKS-12]	Eg. $\ell_1 \cdots \ell_d$	Eg. $\ell_1^{d/2} \ell_2^{d/2}$ ✓

- **IDEA 1 - MULTILINEARIZATION:** Looking at only evaluations on $\{0,1\}^n$. Low rank $\implies$ low degree as $x_i^2 = x_i$ on $\{0,1\}^n$. (Multilinear projection is $x_i^2 = 0$.)
- **IDEA 2 - HIGH-RANK EVALUATIONS OVER $\mathbb{F}_q$:** Over a small field, large rank terms almost always evaluate to zero.

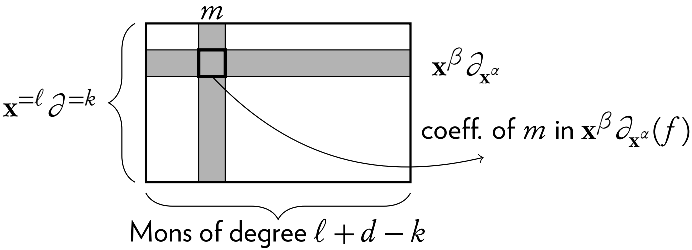
Switching to the evaluation perspective

What has been studied so far:

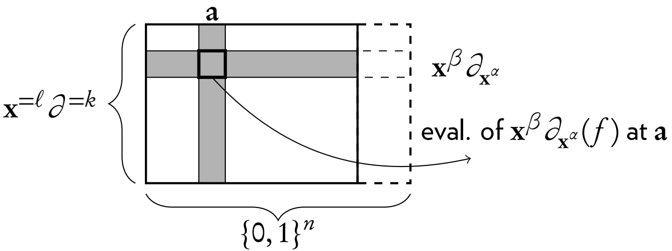


Switching to the evaluation perspective

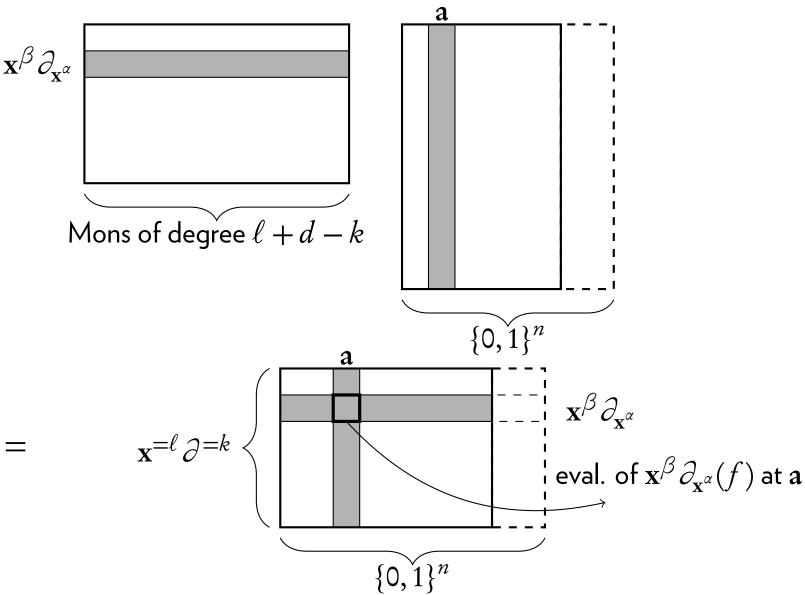
What has been studied so far:



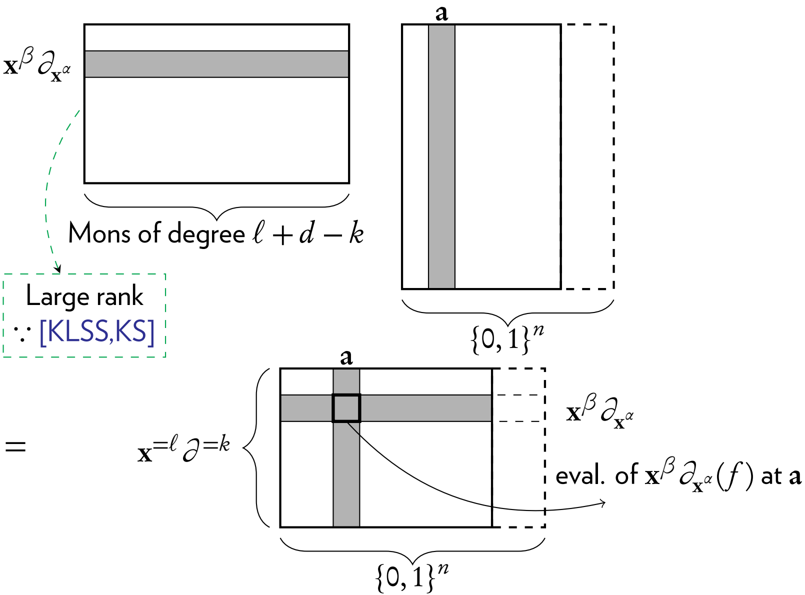
What we need now:



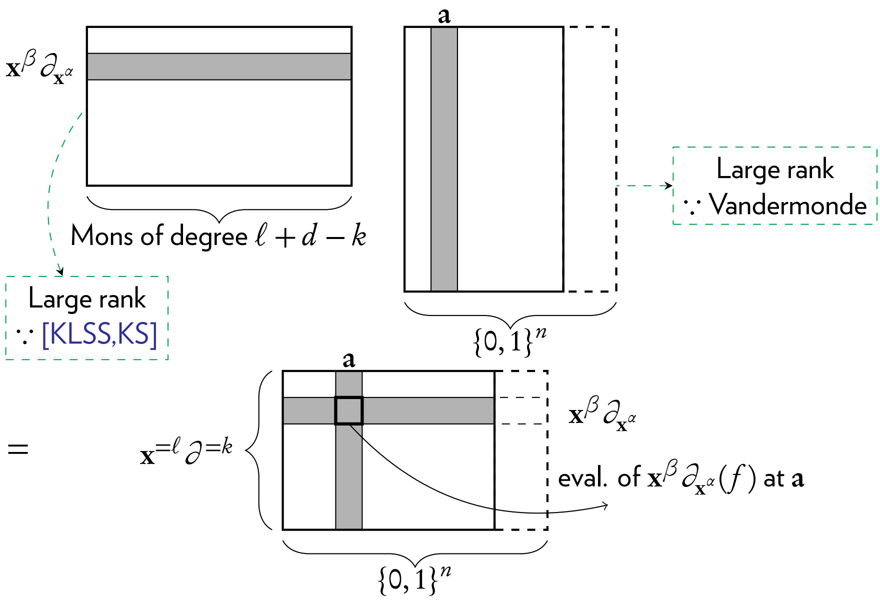
Switching to the evaluation perspective



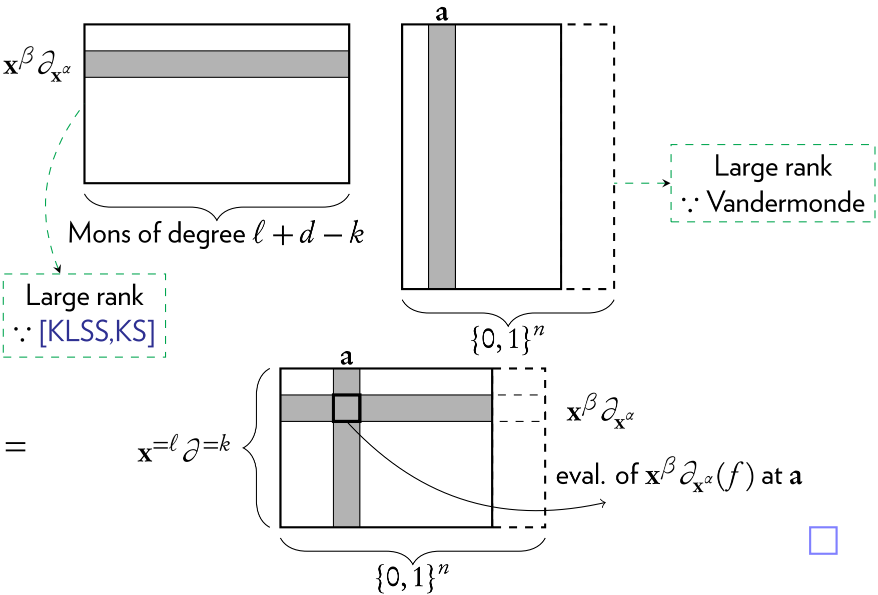
Switching to the evaluation perspective



Switching to the evaluation perspective



Switching to the evaluation perspective



A lower bound

Theorem ([Kumar-Saptharishi-15])

There is a polynomial $f \in$ VNP such that, for every finite field $\mathbb{F}_q$, any hom. $\Sigma\Pi\Sigma\Pi\Sigma$ circuit computing f over $\mathbb{F}_q$ must have size $\exp(\Omega_q(\sqrt{d}))$.

A lower bound

Theorem ([Kumar-Saptharishi-15])

There is a polynomial $f \in VNP$ such that, for every finite field $\mathbb{F}_q$, any hom. $\Sigma\Pi\Sigma\Pi\Sigma$ circuit computing f over $\mathbb{F}_q$ must have size $\exp(\Omega_q(\sqrt{d}))$.

Remarks:

- The dual evaluation perspective was also adopted in [Grigoriev-Karpinski-98] for $\Sigma\Pi\Sigma$ circuits over finite fields.

A lower bound

Theorem ([Kumar-Saptharishi-15])

There is a polynomial $f \in VNP$ such that, for every finite field $\mathbb{F}_q$, any hom. $\Sigma\Pi\Sigma\Pi\Sigma$ circuit computing f over $\mathbb{F}_q$ must have size $\exp(\Omega_q(\sqrt{d}))$.

REMARKS:

- The dual evaluation perspective was also adopted in [Grigoriev-Karpinski-98] for $\Sigma\Pi\Sigma$ circuits over finite fields.
- The proof ought to work for VP also but we don't have a tight enough analysis (yet).

A lower bound

Theorem ([Kumar-Saptharishi-15])

There is a polynomial $f \in VNP$ such that, for every finite field $\mathbb{F}_q$, any hom. $\Sigma\Pi\Sigma\Pi\Sigma$ circuit computing f over $\mathbb{F}_q$ must have size $\exp(\Omega_q(\sqrt{d}))$.

REMARKS:

- The dual evaluation perspective was also adopted in [Grigoriev-Karpinski-98] for $\Sigma\Pi\Sigma$ circuits over finite fields.
- The proof ought to work for VP also but we don't have a tight enough analysis (yet).
- Shows why the [Kayal-Limaye-Saha-Srinivasan-14, Kumar-Saraf-14] technique couldn't separate depth five from depth four.

A lower bound

Theorem ([Kumar-Saptharishi-15])

There is a polynomial $f \in VNP$ such that, for every finite field $\mathbb{F}_q$, any hom. $\Sigma\Pi\Sigma\Pi\Sigma$ circuit computing f over $\mathbb{F}_q$ must have size $\exp(\Omega_q(\sqrt{d}))$.

Remarks:

- The dual evaluation perspective was also adopted in [Grigoriev-Karpinski-98] for $\Sigma\Pi\Sigma$ circuits over finite fields.
- The proof ought to work for VP also but we don't have a tight enough analysis (yet).
- Shows why the [Kayal-Limaye-Saha-Srinivasan-14, Kumar-Saraf-14] technique couldn't separate depth five from depth four.
- Other fields?

Summary

"I lost you a while back... what do I need to remember?"

- Two possible ways to prove VP $\neq$ VNP:

  Prove an $n^{\omega(\sqrt{d})}$ lower bound for $\Sigma\Pi\Sigma^{\sqrt{d}}$ circuits over $\mathbb{Q}$.

  Prove an $n^{\omega(\sqrt{d})}$ lower bound for $\Sigma\Pi^{\sqrt{d}}\Sigma\Pi^{\sqrt{d}}$ circuits.

Summary

"I lost you a while back... what do I need to remember?"

- Two possible ways to prove VP $\neq$ VNP:

  Prove an $n^{\omega(\sqrt{d})}$ lower bound for $\Sigma\Pi\Sigma^{\sqrt{d}}$ circuits over $\mathbb{Q}$.

  Prove an $n^{\omega(\sqrt{d})}$ lower bound for $\Sigma\Pi^{\sqrt{d}}\Sigma\Pi^{\sqrt{d}}$ circuits.

- We already have $n^{\Omega(\sqrt{d})}$ lower bounds in both cases, in fact for slightly more general classes!

Summary

"I lost you a while back... what do I need to remember?"

- Two possible ways to prove VP $\neq$ VNP:

  Prove an $n^{\omega(\sqrt{d})}$ lower bound for $\Sigma\Pi\Sigma^{\sqrt{d}}$ circuits over $\mathbb{Q}$.

  Prove an $n^{\omega(\sqrt{d})}$ lower bound for $\Sigma\Pi^{\sqrt{d}}\Sigma\Pi^{\sqrt{d}}$ circuits.

- We already have $n^{\Omega(\sqrt{d})}$ lower bounds in both cases, in fact for slightly more general classes!

- Some stuff happened with depth five circuits over small fields.

Summary

"I lost you a while back... what do I need to remember?"

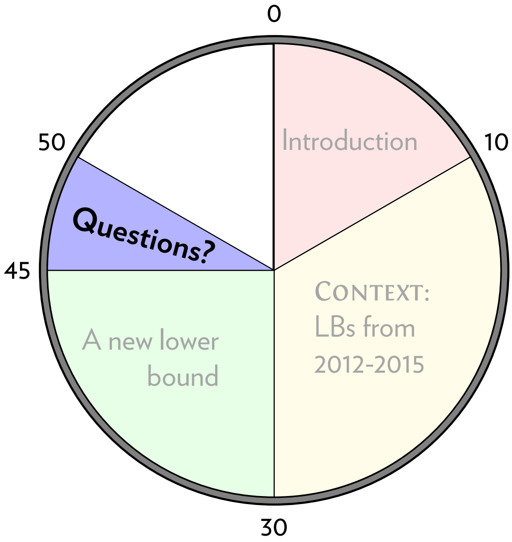
- Two possible ways to prove VP $\neq$ VNP:

  Prove an $n^{\omega(\sqrt{d})}$ lower bound for $\Sigma\Pi\Sigma^{\sqrt{d}}$ circuits over $\mathbb{Q}$.

  Prove an $n^{\omega(\sqrt{d})}$ lower bound for $\Sigma\Pi^{\sqrt{d}}\Sigma\Pi^{\sqrt{d}}$ circuits.

- We already have $n^{\Omega(\sqrt{d})}$ lower bounds in both cases, in fact for slightly more general classes!
- Some stuff happened with depth five circuits over small fields.
- You should be super-excited by all this!

Thank you


0
10
30
45
50
Introduction
CONTEXT:
LBs from
2012-2015
A new lower
bound
Questions?