Functional lower bounds for arithmetic circuits

and connections to boolean circuit complexity

Michael Forbes
Princeton University

Mrinal Kumar
Rutgers University

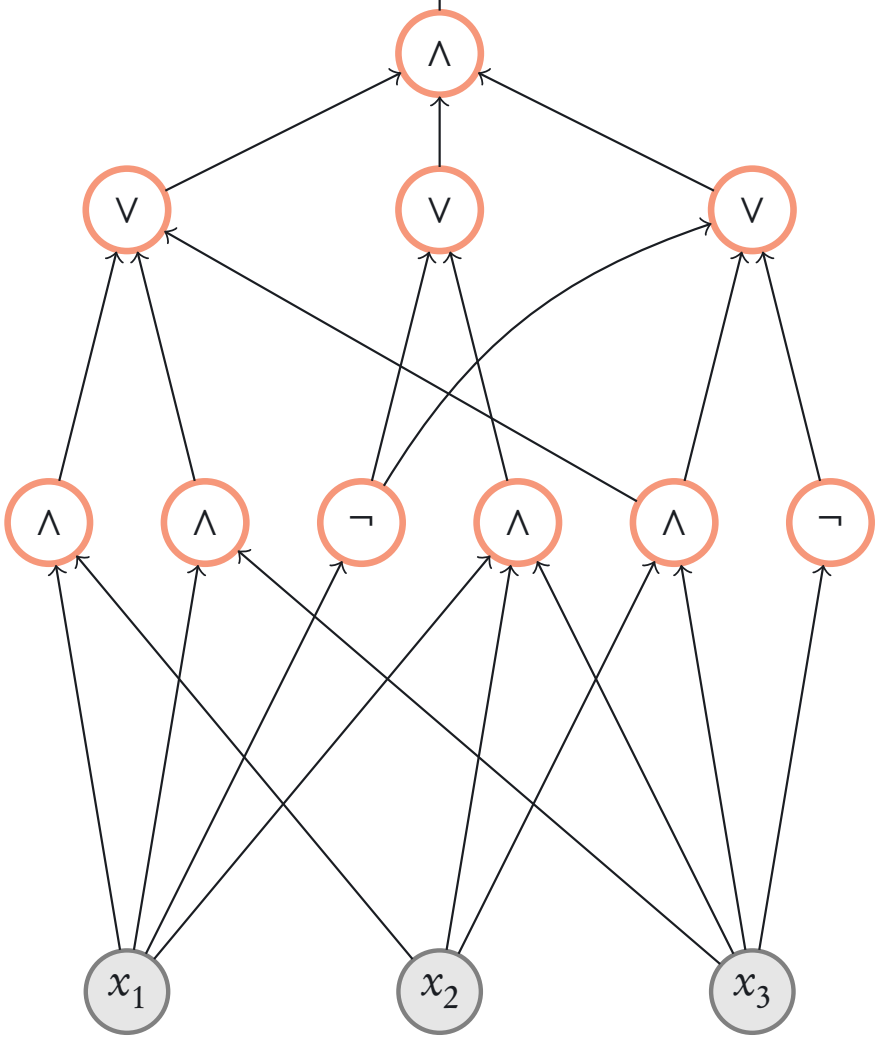
Ramprasad Saptharishi
Tel Aviv University

Computational Complexity Conference (CCC 2016)
Tokyo, Japan

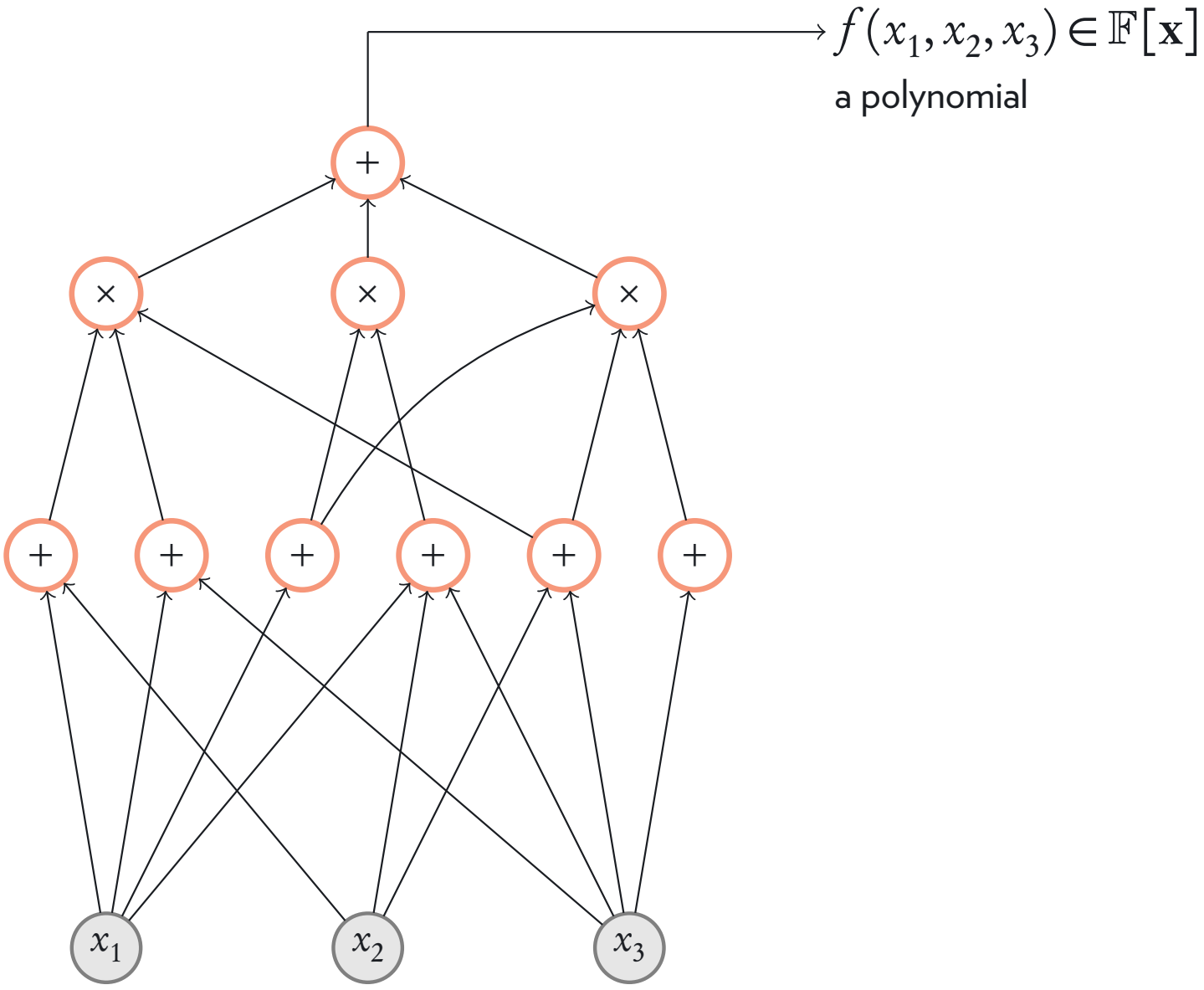
Boolean circuits

$f(x_1, x_2, x_3) : \{0,1\}^n \rightarrow \{0,1\}$

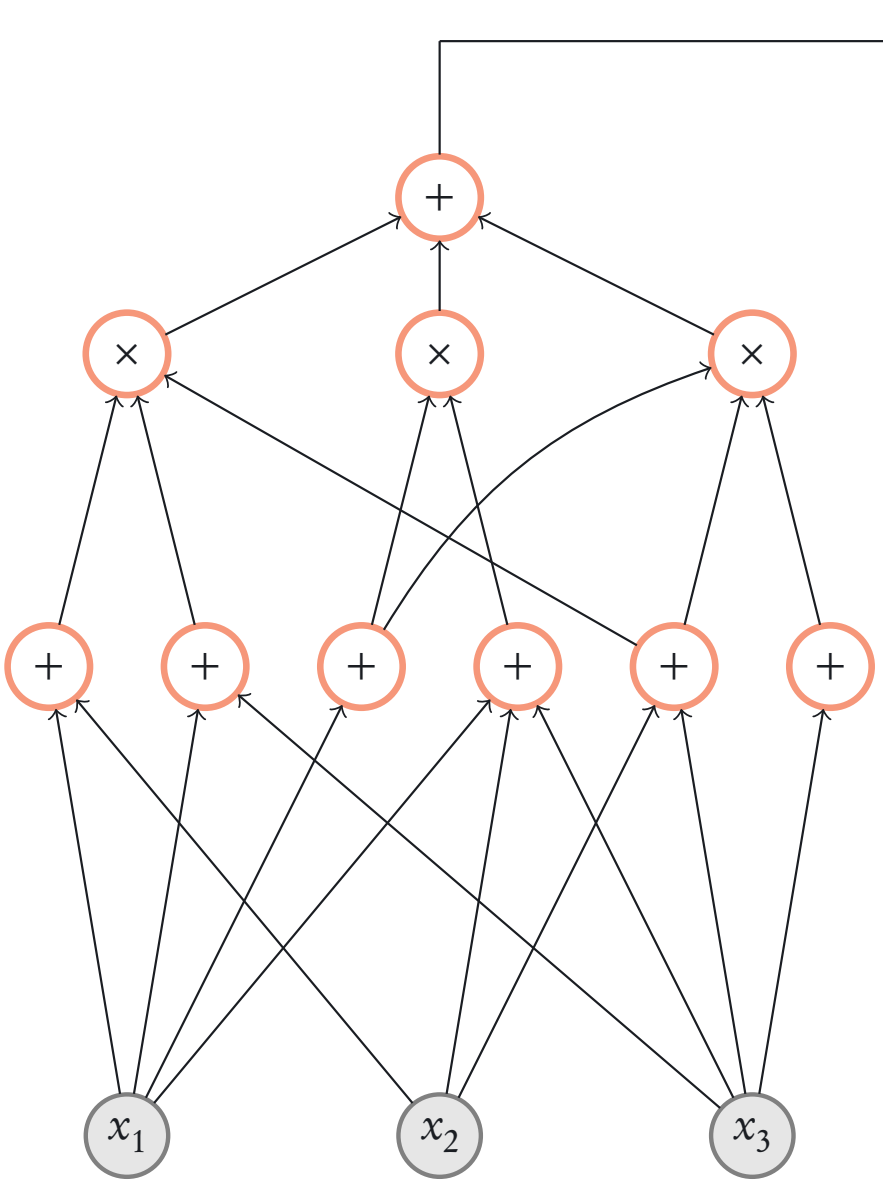
a boolean function



Arithmetic circuits



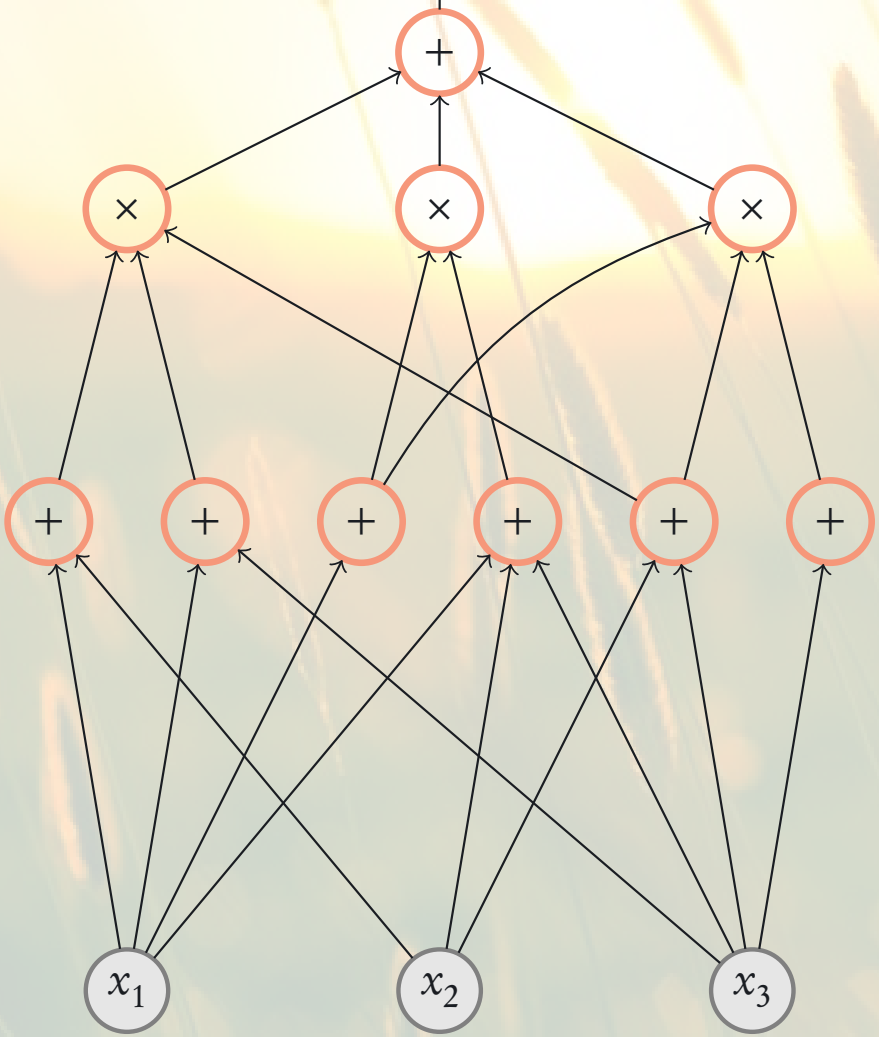
Arithmetic circuits



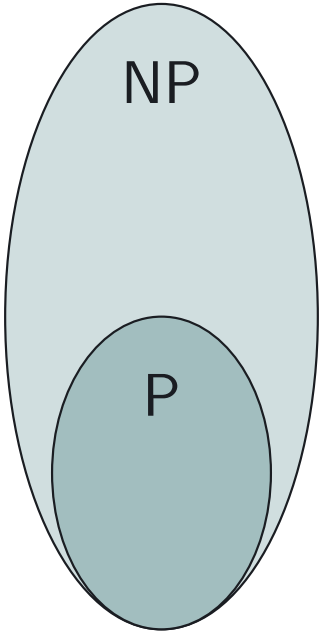
Arithmetic circuits

$f(x_1, x_2, x_3) \in \mathbb{F}[\mathbf{x}]$

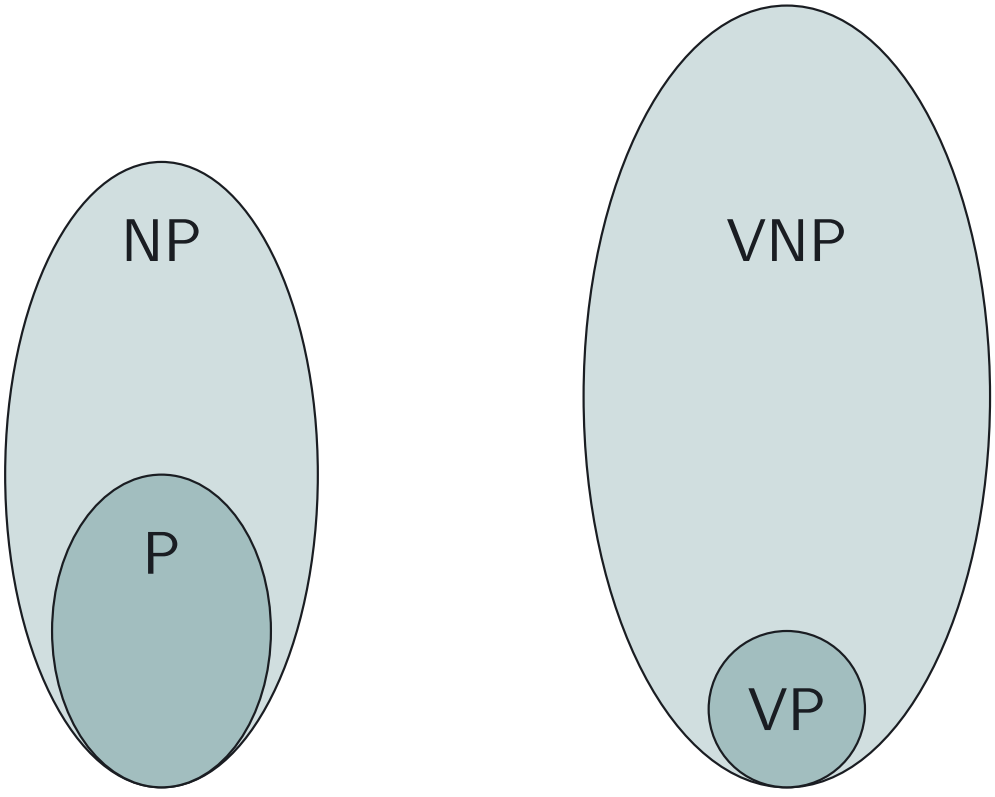
a polynomial of *low* degree



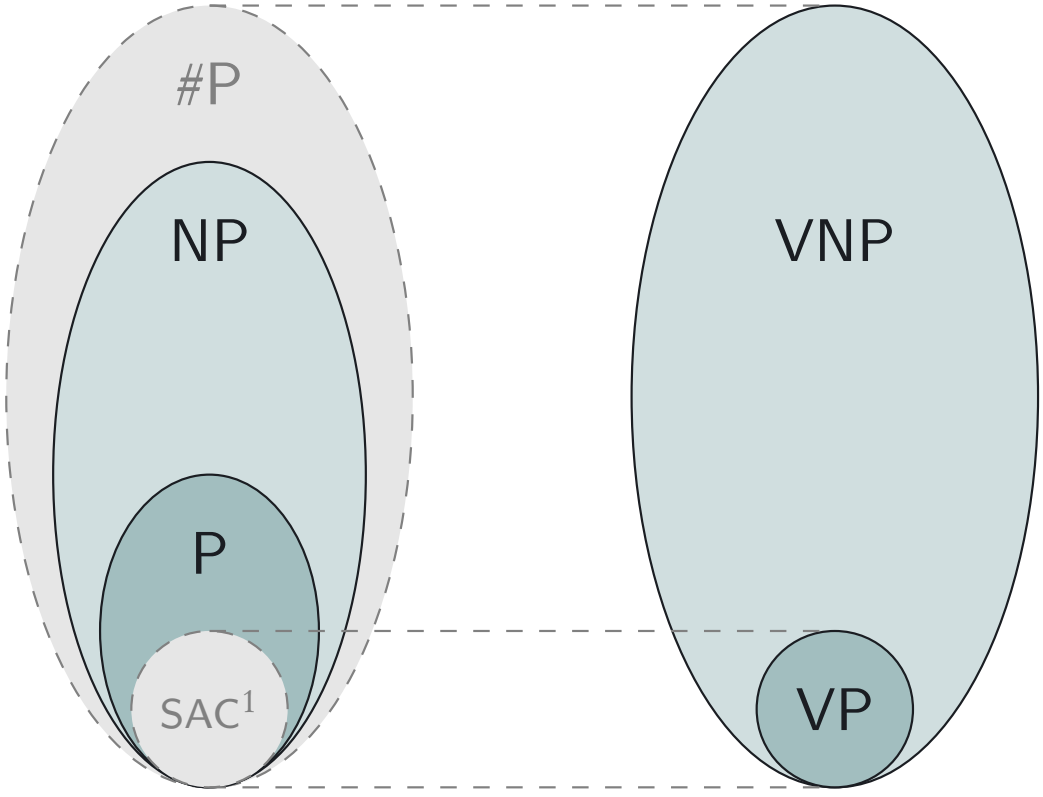
The Open Problem(s)



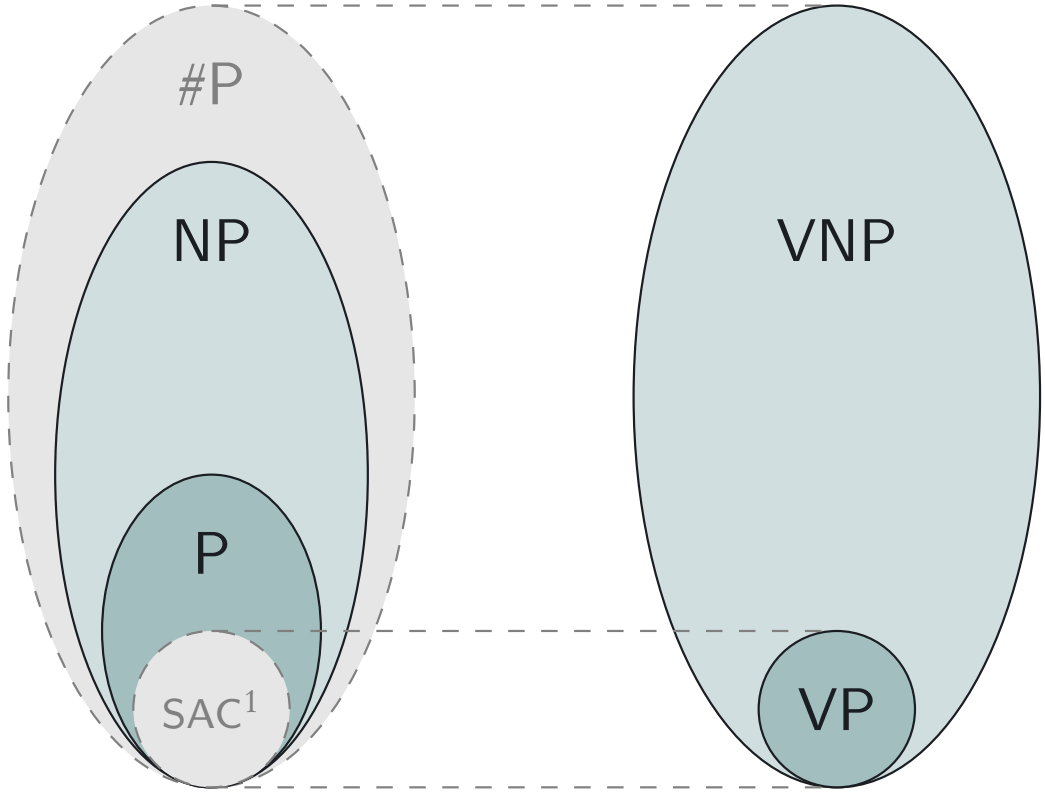
The Open Problem(s)



The Open Problem(s)



The Open Problem(s)



VP ≠ VNP is simpler to prove than P ≠ NP.

The '*Chasm*' at depth four

Theorem ([Agrawal-Vinay, Koiran, Tavenas])

Can be computed by

arithmetic circuits

of "small" size

$\longrightarrow$

Can be computed by

hom. depth-4 circuits

of "not-too-large" size

The '*Chasm*' at depth four

Theorem ([Agrawal-Vinay, Koiran, Tavenas])

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

The '*Chasm*' at depth four

Theorem ([Agrawal-Vinay, Koiran, Tavenas])

Can be computed by | *Can be computed by*

arithmetic circuits ⟶ *hom. depth-4 circuits*

of $\mathrm{poly}(n, d)$ *size* | *of* $n^{O(\sqrt{d})}$ *size*

(Or)

Cannot be computed by | *Cannot be computed by*

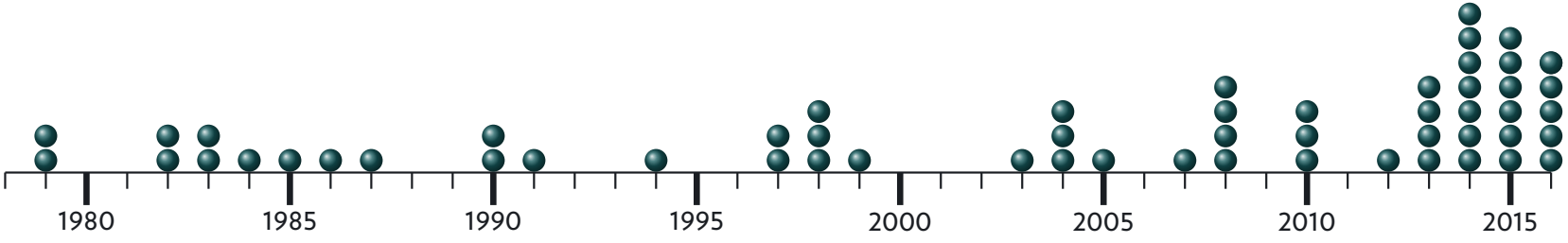
arithmetic circuits ⟵ *hom. depth-4 circuits*

of $\mathrm{poly}(n, d)$ *size* | *of* $n^{O(\sqrt{d})}$ *size*

Recent activity in algebraic complexity

A recent surge in optimism in the field.

Someone even conjectured that VP $\neq$ VNP would be resolved by 2018...

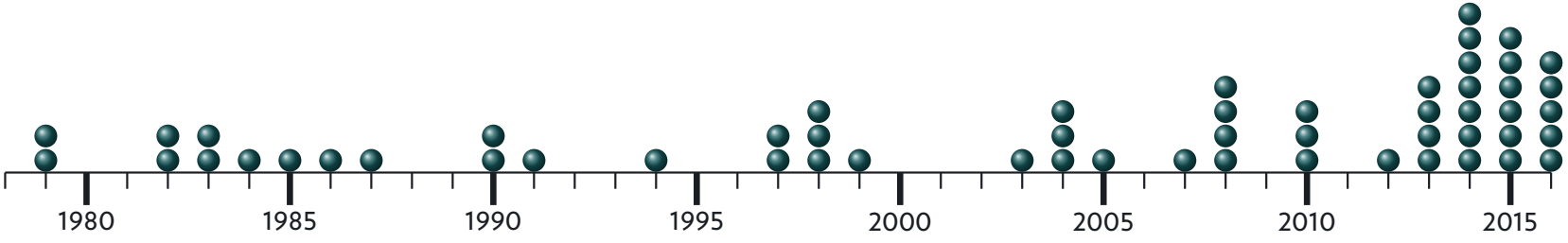


Each ● is one result in algebraic complexity lower bounds.

Recent activity in algebraic complexity

A recent surge in optimism in the field.

Someone even conjectured that VP $\neq$ VNP would be resolved by 2018...



Each ● is one result in algebraic complexity lower bounds.

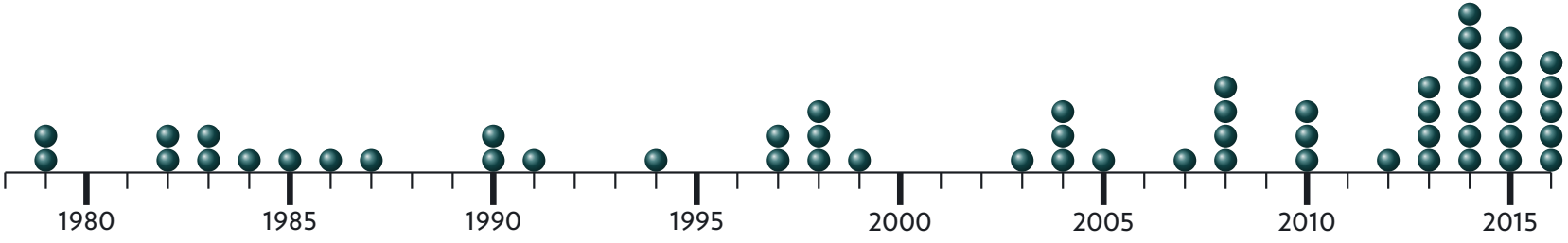
Theorem ([KLSS,KS])

There is an explicit polynomial f with $0/1$ coefficients such that any homogeneous depth-4 arithmetic circuit computing it must have size $n^{\Omega(\sqrt{d})}$.

Recent activity in algebraic complexity

A recent surge in optimism in the field.

Someone even conjectured that VP $\neq$ VNP would be resolved by 2018...



Each ● is one result in algebraic complexity lower bounds.

Theorem ([KLSS,KS])

There is an explicit polynomial f with $0/1$ coefficients such that any homogeneous depth-4 arithmetic circuit computing it must have size $n^{\Omega(\sqrt{d})}$.

Question: Can they be *lifted* to boolean circuits?

A possible application

Theorem ([KLSS,KS])

There is an explicit polynomial f with $0/1$ coefficients such that any homogeneous depth-4 arithmetic circuit computing it must have size $n^{\Omega(\sqrt{d})}$.

A possible application

Theorem ([KLSS,KS])

There is an explicit polynomial f with $0/1$ coefficients such that any homogeneous depth-4 arithmetic circuit computing it must have size $n^{\Omega(\sqrt{d})}$.

One of the key steps in Williams' proof of NEXP $\not\subset$ ACC^0:

Theorem ([Yao, BT, AG])

For any boolean function F computed by an ACC^0 circuit of size s, there is a univariate polynomial $g \in \mathbb{F}[y]$ and a multilinear polynomial $h(\mathbf{x}) = \sum h_\alpha \mathbf{x}^\alpha$ with $2^{\text{poly}\log(s)}$ monomials such that,

$$\forall \mathbf{x} \in \{0,1\}^n \quad , \quad F(\mathbf{x}) \quad = \quad g\left(h(\mathbf{x})\right).$$

A possible application

Theorem ([KLSS,KS])

There is an explicit polynomial f with $0/1$ coefficients such that any homogeneous depth-4 arithmetic circuit computing it must have size $n^{\Omega(\sqrt{d})}$.

One of the key steps in Williams' proof of NEXP $\not\subset$ ACC^0:

Theorem ([Yao, BT, AG])

For any boolean function F computed by an ACC^0 circuit of size s, there is a depth-4 arithmetic circuit C of size $2^{\text{poly}\log(s)}$ such that,

$$\forall \mathbf{x} \in \{0,1\}^n \quad , \quad F(\mathbf{x}) \quad = \quad C(\mathbf{x}).$$

A possible application

Theorem ([KLSS,KS])

There is an explicit polynomial f with $0/1$ coefficients such that any homogeneous depth-4 arithmetic circuit computing it must have size $n^{\Omega(\sqrt{d})}$.

One of the key steps in Williams' proof of NEXP $\not\subset$ ACC^0:

Theorem ([Yao, BT, AG])

For any boolean function F computed by an ACC^0 circuit of size s, there is a depth-4 arithmetic circuit C of size $2^{\text{poly}\log(s)}$ such that,

$$\forall \mathbf{x} \in \{0,1\}^n \quad , \quad F(\mathbf{x}) \quad = \quad C(\mathbf{x}).$$

A possible application

Theorem ([KLSS,KS])

There is an explicit polynomial f with $0/1$ coefficients such that any homogeneous depth-4 arithmetic circuit computing it must have size $n^{\Omega(\sqrt{d})}$.

One of the key steps in Williams' proof of NEXP $\not\subset$ ACC^0:

Theorem ([Yao, BT, AG])

For any boolean function F computed by an ACC^0 circuit of size s, there is a depth-4 arithmetic circuit C of size $2^{\text{poly}\log(s)}$ such that,

$$\forall \mathbf{x} \in \{0,1\}^n \quad , \quad F(\mathbf{x}) \quad = \quad C(\mathbf{x}).$$

Functional Computation

Definition

An arithmetic circuit C is said to *functionally compute* a polynomial F if

$$\forall \mathbf{x} \in \{0,1\}^n \quad , \quad C(\mathbf{x}) \quad = \quad F(\mathbf{x}).$$

Functional Computation

Definition

An arithmetic circuit C is said to *functionally compute* a polynomial F if

$$\forall \mathbf{x} \in \{0,1\}^n \quad , \quad C(\mathbf{x}) \quad = \quad F(\mathbf{x}).$$

- If C computed a multilinear polynomial, then functional computation = syntactic computation.
- But even if C computes a multi-quadratic polynomial, the definition is meaningful.

Functional lower bounds

What we know:

There is an explicit n-variate degree d polynomial F with $0/1$ coefficients such that any homogeneous depth-4 arithmetic circuit computing it must have size $n^{\Omega(\sqrt{d})}$.

Functional lower bounds

What we know:

There is an explicit n-variate degree d polynomial F with $0/1$ coefficients such that any homogeneous depth-4 arithmetic circuit computing it must have size $n^{\Omega(\sqrt{d})}$.

What we'd have liked to prove:

Let C be a homogeneous depth-4 circuit that computes a polynomial P that functionally computes F, i.e.

$$\forall \mathbf{x} \in \{0,1\}^n \quad , \quad P(\mathbf{x}) \quad = \quad F(\mathbf{x}).$$

Then, C must have size $n^{\Omega(\sqrt{d})}$.

Functional lower bounds

What we know:

There is an explicit n-variate degree d polynomial F with $0/1$ coefficients such that any homogeneous depth-4 arithmetic circuit computing it must have size $n^{\Omega(\sqrt{d})}$.

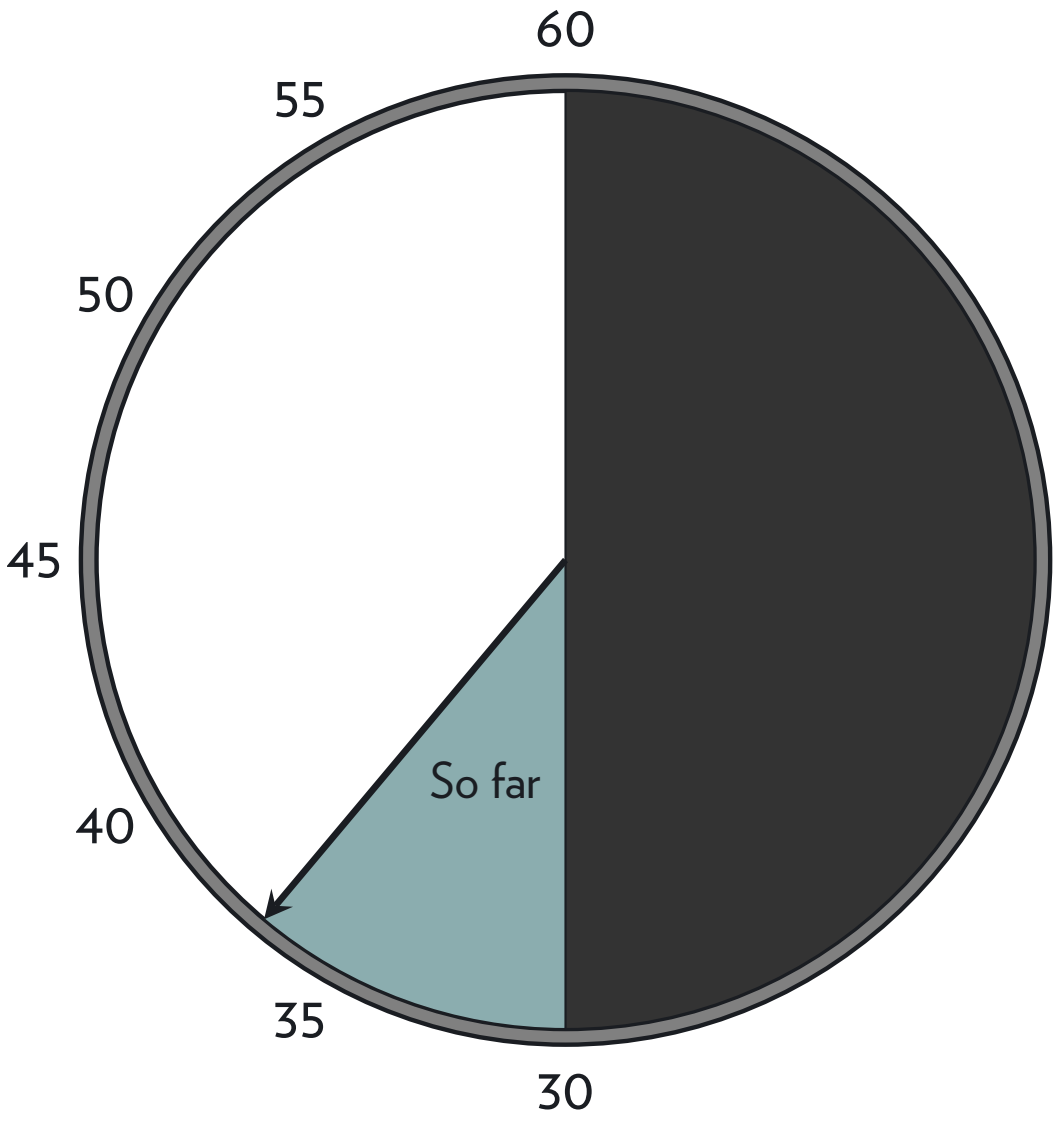
What we prove:

Let C be a homogeneous depth-4 circuit that computes a polynomial P of individual degree at most r that functionally computes F, i.e.

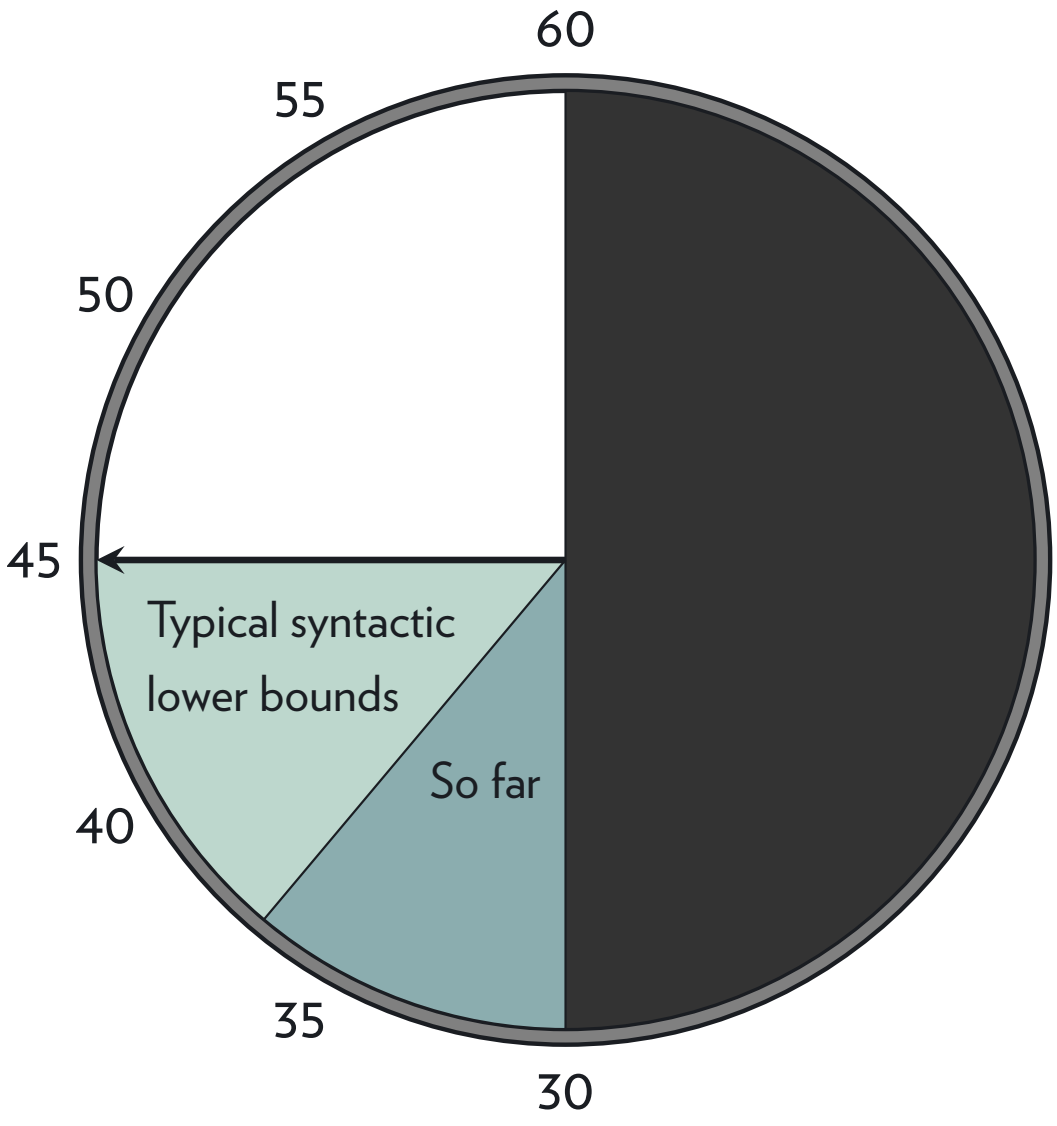
$$\forall \mathbf{x} \in \{0,1\}^n \quad , \quad P(\mathbf{x}) \quad = \quad F(\mathbf{x}).$$

Then, C must have size $n^{\Omega_r(\sqrt{d})}$.

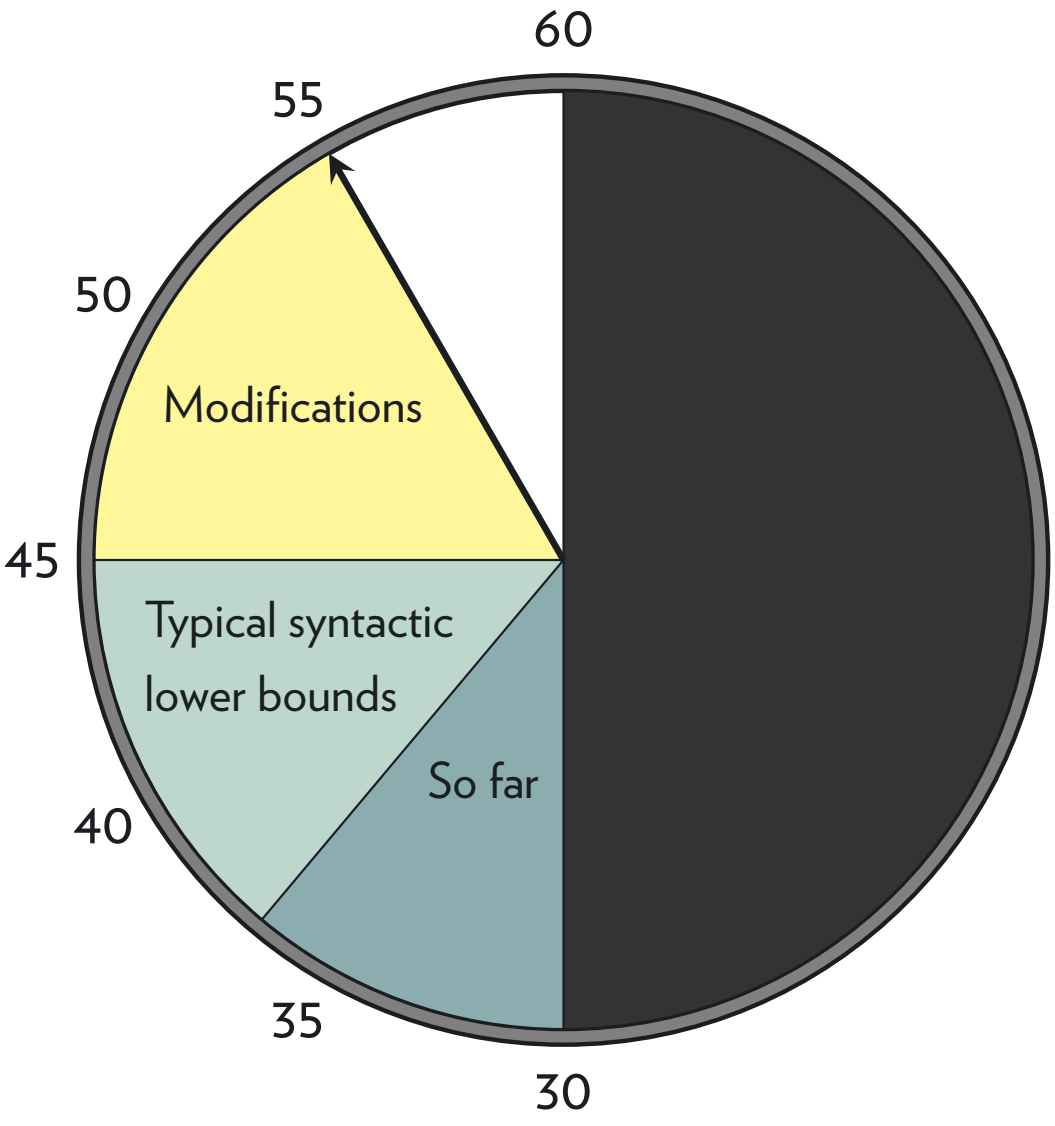
Outline



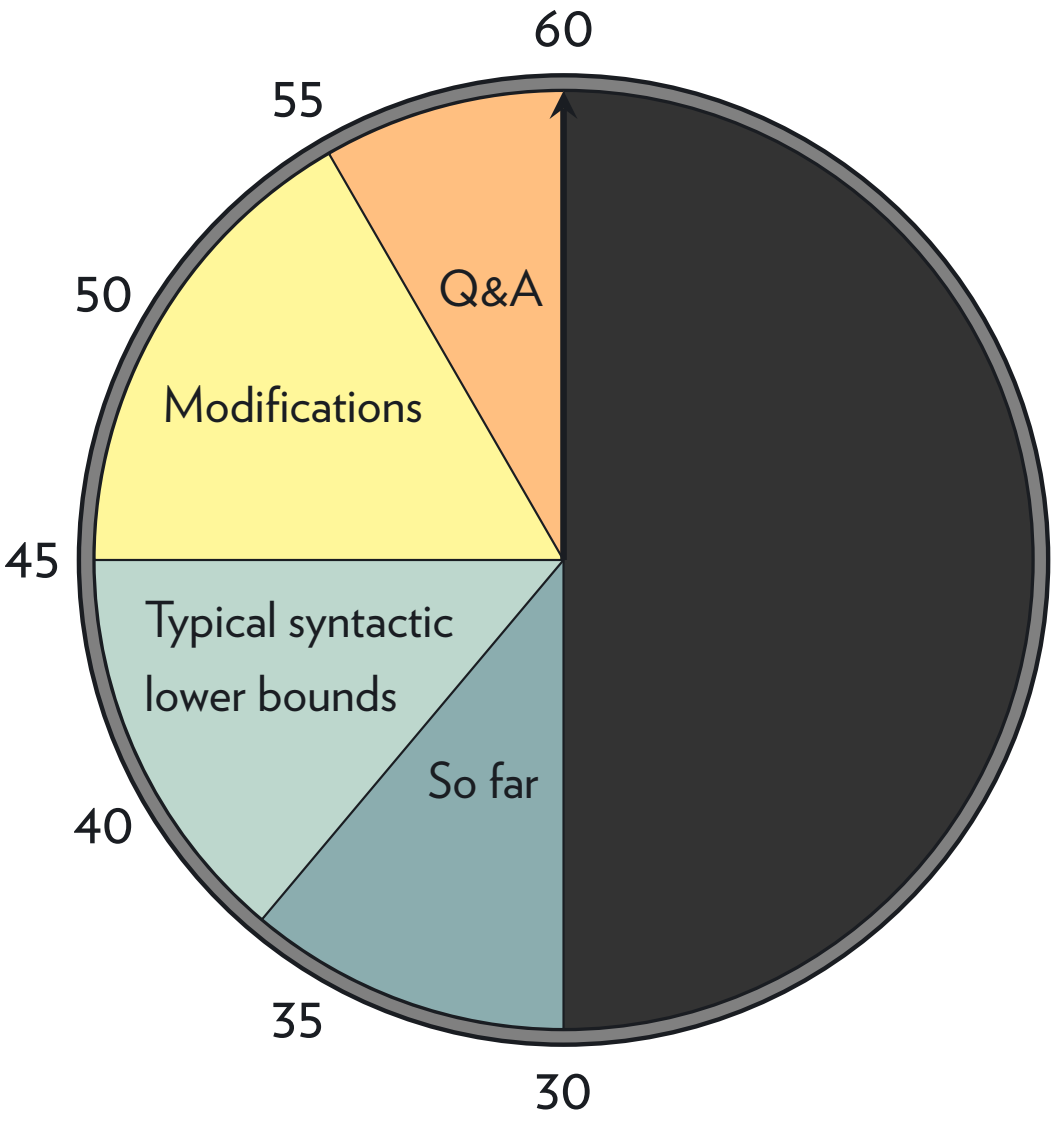
Outline



Outline


60
55
50
45
40
35
30
Modifications
Typical syntactic
lower bounds
So far

Outline


60
55
50
45
40
35
30
Q&A
Modifications
Typical syntactic
lower bounds
So far

Outline

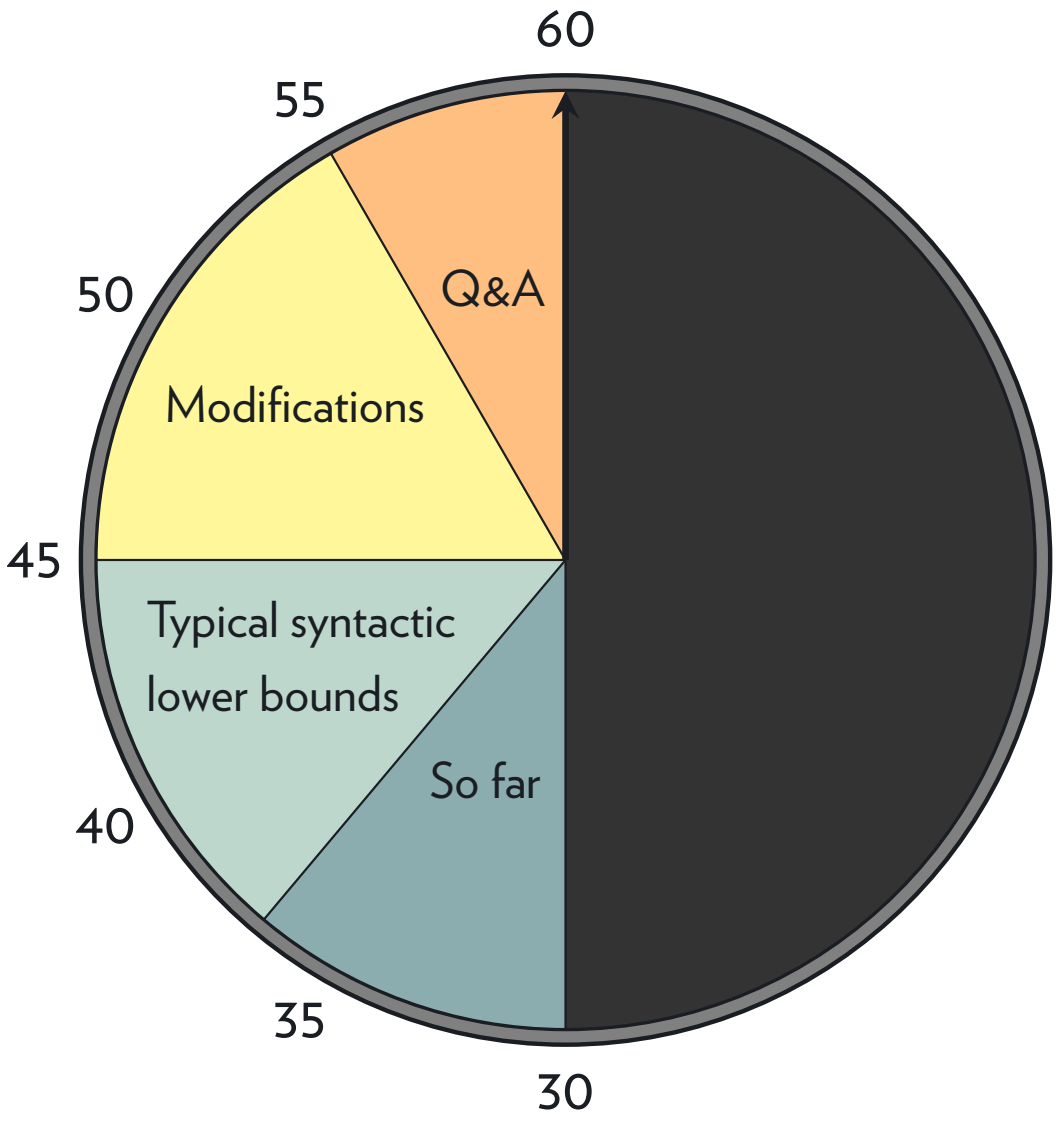


Diagram not to scale

What can functional computation do?

$$\mathrm{Sym}_d(x_1, \ldots, x_n) \quad = \quad \sum_{1 \le i_1 < \cdots < i_d \le n} x_{i_1} \cdots x_{i_d}$$

What can functional computation do?

$$\mathrm{Sym}_d(x_1, \ldots, x_n) \quad = \quad \sum_{1 \le i_1 < \cdots < i_d \le n} x_{i_1} \cdots x_{i_d}$$

If we only care about $\mathbf{x} \in \{0,1\}^n$,

$\ell := \sum x_i$	0	1	2	3	4	5	6	7	8	$\cdots$
Sym_4	0	0	0	0	1	4	15	35	70	$\cdots$

What can functional computation do?

$$\mathrm{Sym}_d(x_1, \ldots, x_n) \quad = \quad \sum_{1 \le i_1 < \cdots < i_d \le n} x_{i_1} \cdots x_{i_d}$$

If we only care about $\mathbf{x} \in \{0,1\}^n$,

$$\mathrm{Sym}_d(\mathbf{x}) = f(\ell)$$

What can functional computation do?

$$\mathrm{Sym}_d(x_1, \ldots, x_n) \quad = \quad \sum_{1 \le i_1 < \cdots < i_d \le n} x_{i_1} \cdots x_{i_d}$$

If we only care about $\mathbf{x} \in \{0,1\}^n$,

$$\begin{aligned} \mathrm{Sym}_d(\mathbf{x}) &= f(\ell) \\ &= a_0 + a_1 \ell + \cdots + a_{n+1} \ell^{n+1} \end{aligned}$$

What can functional computation do?

$$\mathrm{Sym}_d(x_1, \ldots, x_n) = \sum_{1 \le i_1 < \cdots < i_d \le n} x_{i_1} \cdots x_{i_d}$$

If we only care about $\mathbf{x} \in \{0,1\}^n$,

$$\begin{aligned} \mathrm{Sym}_d(\mathbf{x}) &= f(\ell) \\ &= a_0 + a_1 \ell + \cdots + a_{n+1} \ell^{n+1} \\ &\in \text{depth-3 powering circuits} \end{aligned}$$

What can functional computation do?

$$\mathrm{Sym}_d(x_1, \ldots, x_n) \quad = \quad \sum_{1 \le i_1 < \cdots < i_d \le n} x_{i_1} \cdots x_{i_d}$$

If we only care about $\mathbf{x} \in \{0,1\}^n$,

$$\begin{aligned} \mathrm{Sym}_d(\mathbf{x}) &= f(\ell) \\ &= a_0 + a_1 \ell + \cdots + a_{n+1} \ell^{n+1} \\ &\in \text{depth-3 powering circuits} \end{aligned}$$

Syntactic computation of Sym_d by such depth-3 powering circuits require $n^{\Omega(d)}$ size. [Nisan-Wigderson]

Why does the proof break down?

- Lower bounds in alg. complexity use some complexity measure. Associates a number to every polynomial.
- Often is the rank of collection of linear operators.

Why does the proof break down?

- Lower bounds in alg. complexity use some complexity measure. Associates a number to every polynomial.
- Often is the rank of collection of linear operators.
- For depth-3 powering circuits,

$$\Gamma_k(f) \quad = \quad \dim \partial^{=k}(f)$$

Why does the proof break down?

- Lower bounds in alg. complexity use some complexity measure. Associates a number to every polynomial.
- Often is the rank of collection of linear operators.
- For depth-3 powering circuits,

$$\begin{aligned} \Gamma_k(f) &= \dim \partial^{=k}(f) \\ \Gamma_k(\ell^d) &= 1 \\ \Gamma_k(\ell_1^d + \cdots + \ell_s^d) &\leq s \end{aligned}$$

Why does the proof break down?

- Lower bounds in alg. complexity use some complexity measure. Associates a number to every polynomial.
- Often is the rank of collection of linear operators.
- For depth-3 powering circuits,

$$\begin{aligned} \Gamma_k(f) &= \dim \partial^{=k}(f) \\ \Gamma_k(\ell^d) &= 1 \\ \Gamma_k(\ell_1^d + \cdots + \ell_s^d) &\leq s \end{aligned}$$

- Partial derivatives don't behave well with functional computation.

Why does the proof break down?

- Lower bounds in alg. complexity use some complexity measure. Associates a number to every polynomial.
- Often is the rank of collection of linear operators.
- For depth-3 powering circuits,

$$\begin{aligned} \Gamma_k(f) &= \dim \partial^{=k}(f) \\ \Gamma_k(\ell^d) &= 1 \\ \Gamma_k(\ell_1^d + \cdots + \ell_s^d) &\leq s \end{aligned}$$

- Partial derivatives don't behave well with functional computation.

$$(x_1 + \cdots + x_n)^n = x_1 \cdots x_n + \text{(non-multilinear terms)}$$

Why does the proof break down?

- Lower bounds in alg. complexity use some complexity measure. Associates a number to every polynomial.
- Often is the rank of collection of linear operators.
- For depth-3 powering circuits,

$$\begin{aligned} \Gamma_k(f) &= \dim \partial^{=k}(f) \\ \Gamma_k(\ell^d) &= 1 \\ \Gamma_k(\ell_1^d + \cdots + \ell_s^d) &\leq s \end{aligned}$$

- Partial derivatives don't behave well with functional computation.

$$\begin{aligned} (x_1 + \cdots + x_n)^n &= x_1 \cdots x_n + \text{(non-multilinear terms)} \\ &\equiv x_1 \cdots x_n + \text{(lower degree terms)} \end{aligned}$$

Why does the proof break down?

- Lower bounds in alg. complexity use some complexity measure. Associates a number to every polynomial.
- Often is the rank of collection of linear operators.
- For depth-3 powering circuits,

$$\begin{aligned} \Gamma_k(f) &= \dim \partial^{=k}(f) \\ \Gamma_k(\ell^d) &= 1 \\ \Gamma_k(\ell_1^d + \cdots + \ell_s^d) &\leq s \end{aligned}$$

- Partial derivatives don't behave well with functional computation.

$$\begin{aligned} (x_1 + \cdots + x_n)^n &= x_1 \cdots x_n + \text{(non-multilinear terms)} \\ &\equiv x_1 \cdots x_n + \text{(lower degree terms)} \end{aligned}$$

Different partial derivatives have different leading monomials

Measures for various lower bounds

depth-3 powering circuits $\dim \partial^{=k}(f)$

Measures for various lower bounds

depth-3 powering circuits $\dim \partial^{=k}(f)$

hom-$\Sigma\Pi\Sigma$ circuits $\dim \partial^{=k}(f)$

Measures for various lower bounds

depth-3 powering circuits	$\dim \partial^{=k}(f)$
hom-$\Sigma\Pi\Sigma$ circuits	$\dim \partial^{=k}(f)$
hom-$\Sigma\Pi\Sigma\Pi^{[\sqrt{d}]}$ circuits	$\dim \mathbf{x}^{=\ell}\partial^{=k}(f)$

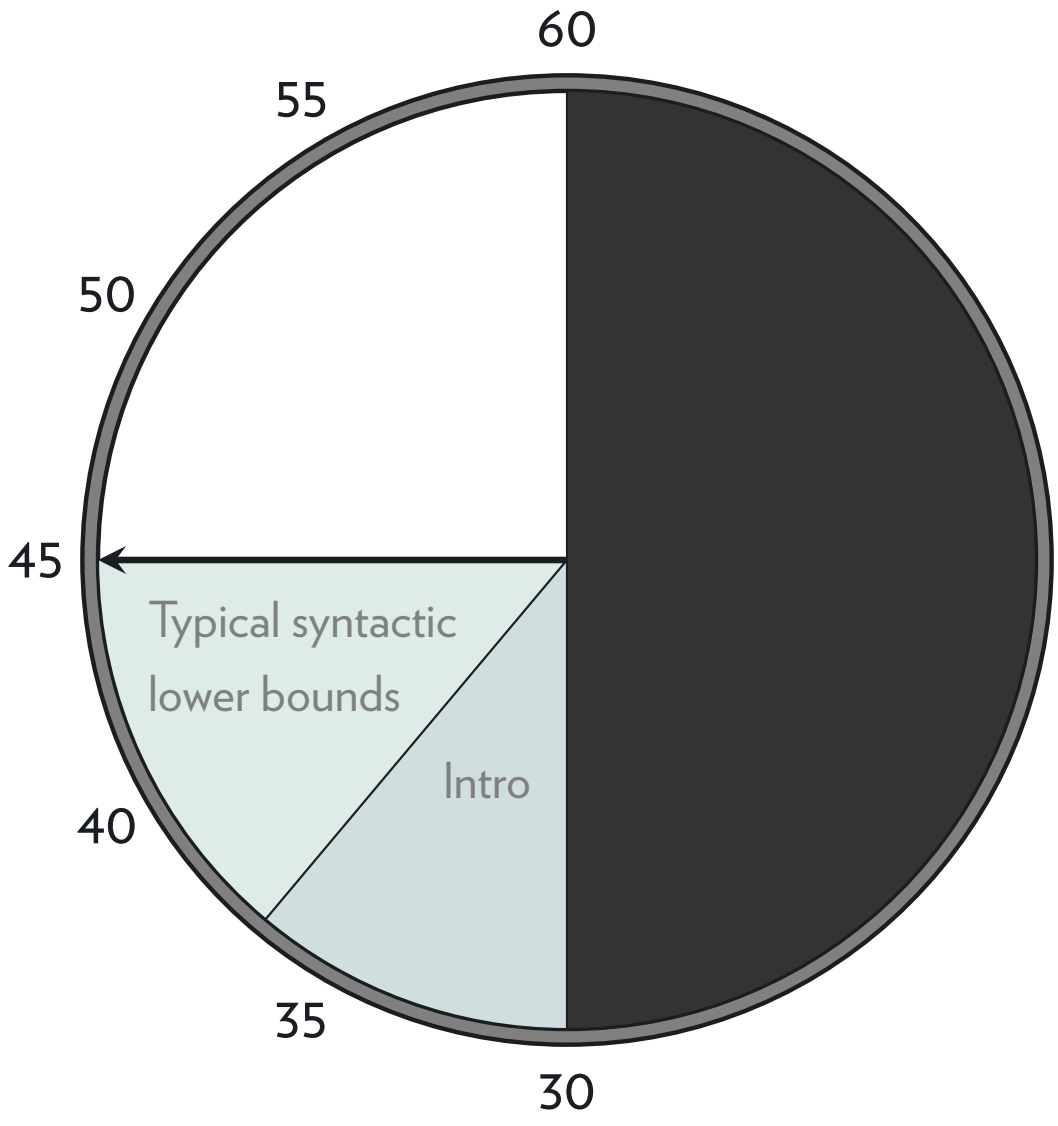
Measures for various lower bounds

depth-3 powering circuits	$\dim \ \partial^{=k}(f)$
hom-$\Sigma\Pi\Sigma$ circuits	$\dim \ \partial^{=k}(f)$
hom-$\Sigma\Pi\Sigma\Pi^{[\sqrt{d}]}$ circuits	$\dim \ \mathbf{x}^{=\ell}\,\partial^{=k}(f)$
hom-$\Sigma\Pi\Sigma\Pi$ circuits	$\dim \ \mathrm{mult}\left(\mathbf{x}^{=\ell}\,\partial^{=k}(f)\right)$

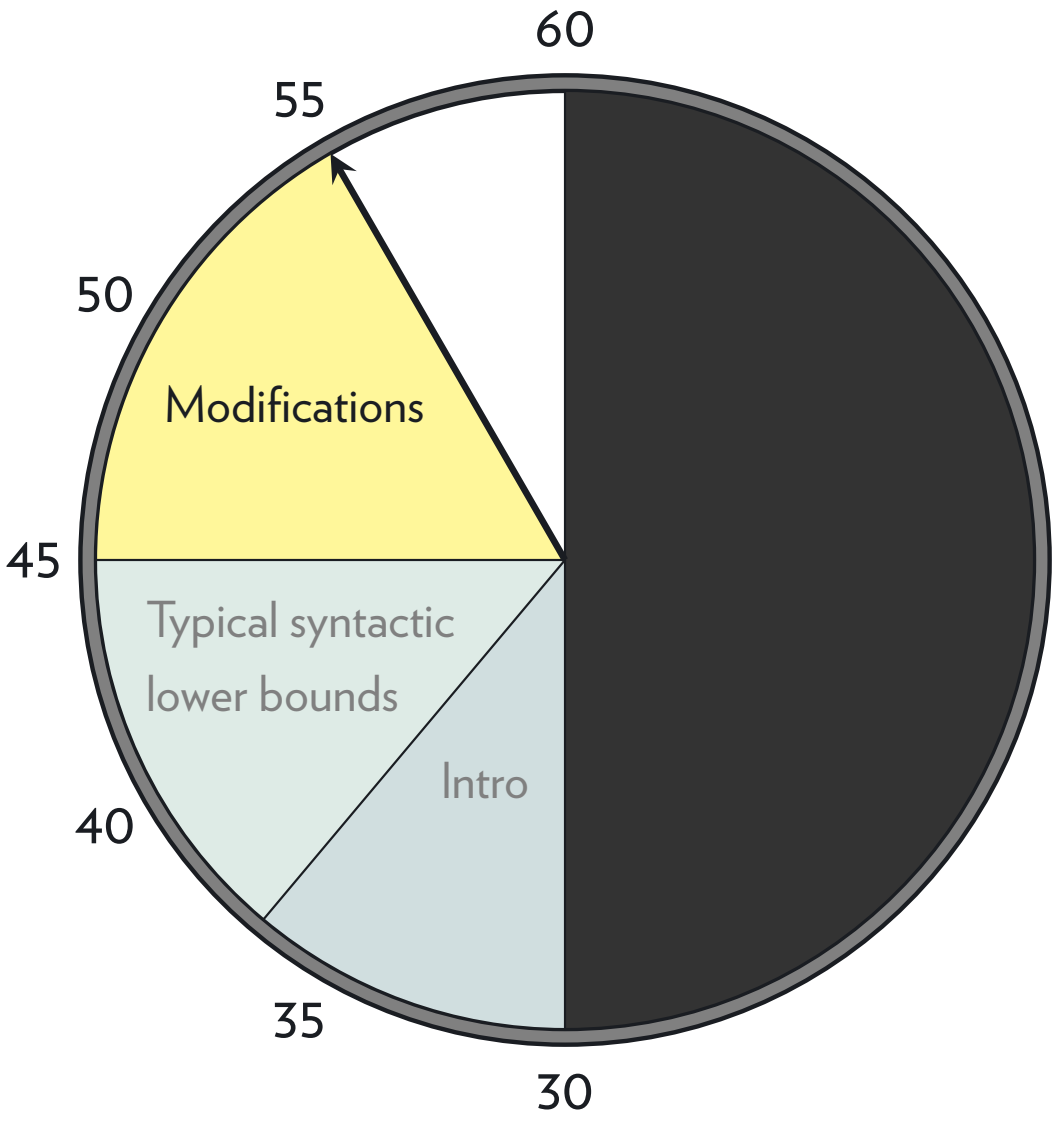
Measures for various lower bounds

depth-3 powering circuits	$\dim \partial^{=k}(f)$
hom-$\Sigma\Pi\Sigma$ circuits	$\dim \partial^{=k}(f)$
hom-$\Sigma\Pi\Sigma\Pi^{[\sqrt{d}]}$ circuits	$\dim \mathbf{x}^{=\ell}\partial^{=k}(f)$
hom-$\Sigma\Pi\Sigma\Pi$ circuits	$\dim \operatorname{mult}\left(\mathbf{x}^{=\ell}\partial^{=k}(f)\right)$
$\vdots$	

Outline



Outline


60
55
50
45
40
35
30
Modifications
Typical syntactic
lower bounds
Intro

A natural attempt

If a circuit $C \in \mathscr{C}$ computes a polynomial P ,
can the *unique multilinear representation* P' be computed efficiently as well?

A natural attempt

If a circuit $C \in \mathscr{C}$ computes a polynomial P ,
can the *unique multilinear representation* P' be computed efficiently as well?

No... (unless VP = VNP)

$$(x_{11}y_1 + \cdots + x_{1n}y_n) \cdots (x_{n1}y_1 + \cdots + x_{nn}y_n)$$

A natural attempt

If a circuit $C \in \mathscr{C}$ computes a polynomial P ,
can the *unique multilinear representation* P' be computed efficiently as well?

No... (unless VP = VNP)

$$(x_{11}y_1 + \cdots + x_{1n}y_n) \cdots (x_{n1}y_1 + \cdots + x_{nn}y_n)$$

$$=$$

$$\text{Perm}(X) \cdot y_1 \cdots y_n \; + \text{ non-multilinear terms}$$

A natural attempt

If a circuit $C \in \mathscr{C}$ computes a polynomial P ,
can the *unique multilinear representation* P' be computed efficiently as well?

No... (unless VP = VNP)

$$(x_{11}y_1 + \cdots + x_{1n}y_n)\cdots(x_{n1}y_1 + \cdots + x_{nn}y_n)$$

$$\equiv$$

$$\mathrm{Perm}(X)\cdot y_1 \cdots y_n \; + \text{ lower degree terms}$$

A natural attempt

If a circuit $C \in \mathscr{C}$ computes a polynomial P ,
can the *unique multilinear representation* P' be computed efficiently as well?

No... (unless VP = VNP)

$$(x_{11}y_1 + \cdots + x_{1n}y_n)\cdots(x_{n1}y_1 + \cdots + x_{nn}y_n)$$

$$\equiv$$

$$\mathrm{Perm}(X)\cdot y_1 \cdots y_n \; + \text{ lower degree terms}$$

...easy to extract homogeneous components.

A natural attempt

If a circuit $C \in \mathscr{C}$ computes a polynomial P ,
can the *unique multilinear representation* P' be computed efficiently as well?

A natural attempt

If a circuit $C \in \mathscr{C}$ computes a polynomial P of low individual degree, can the *unique multilinear representation* P' be computed efficiently as well?

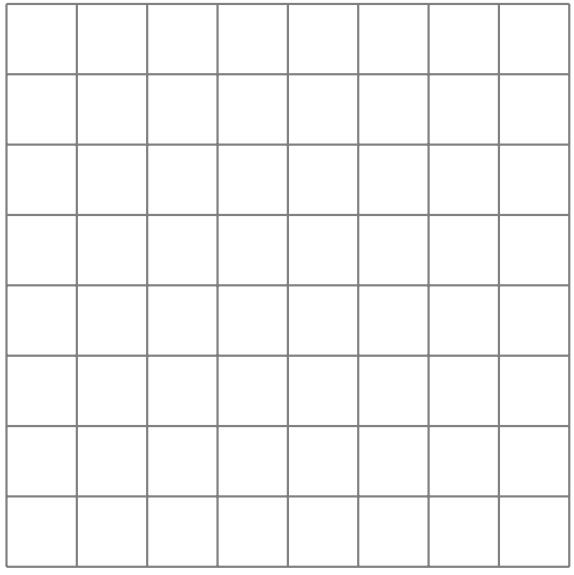
A natural attempt

If a circuit $C \in \mathscr{C}$ computes a polynomial P of low individual degree, can the *unique multilinear representation* P' be computed efficiently as well?

Not clear, even when dealing with multi-quadratics ...

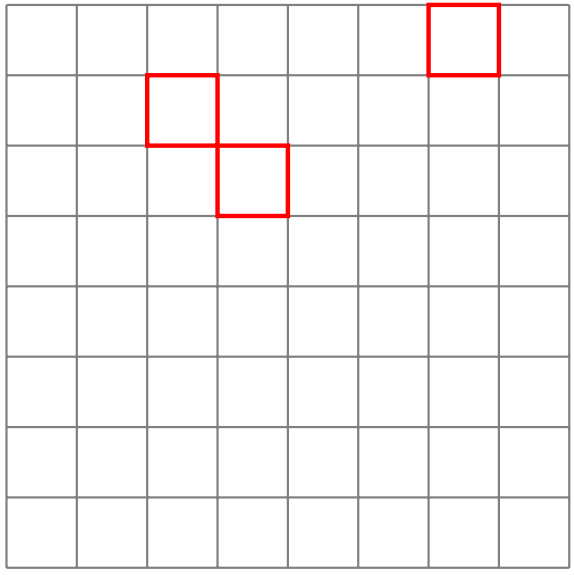
Partial evaluations as proxies

Think of the polynomial Perm...



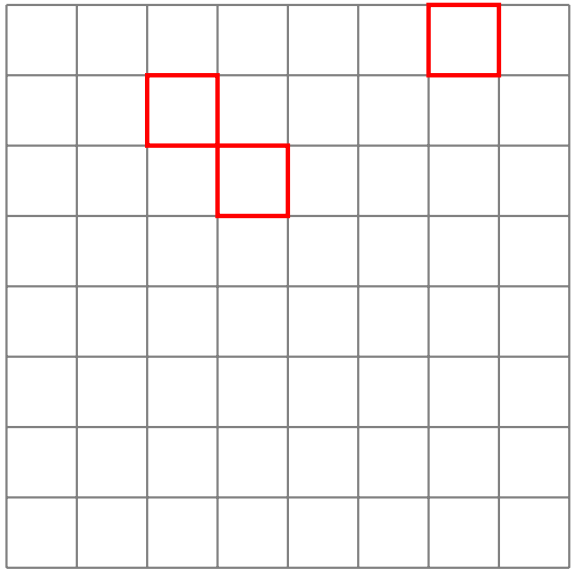
Partial evaluations as proxies

Think of the polynomial Perm...

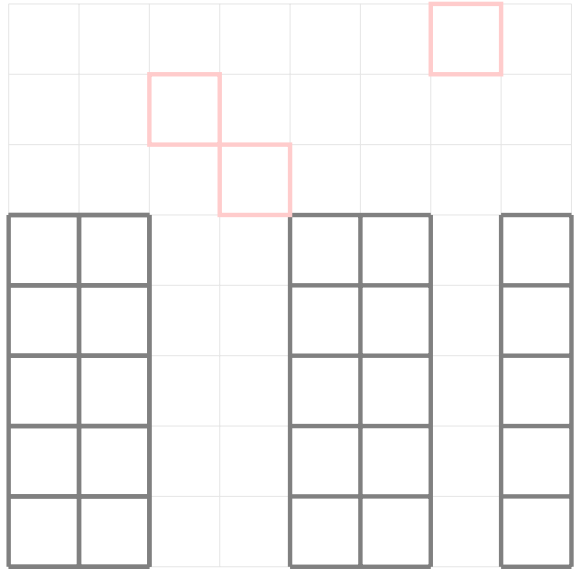


Partial evaluations as proxies

Think of the polynomial Perm...



=

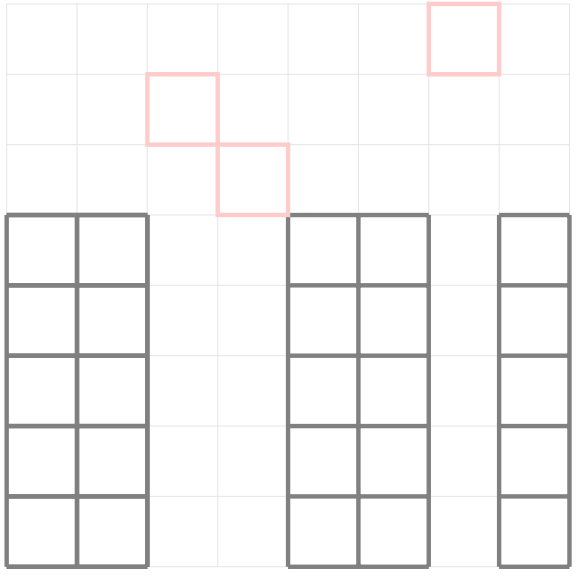


Partial evaluations as proxies

Think of the polynomial Perm...

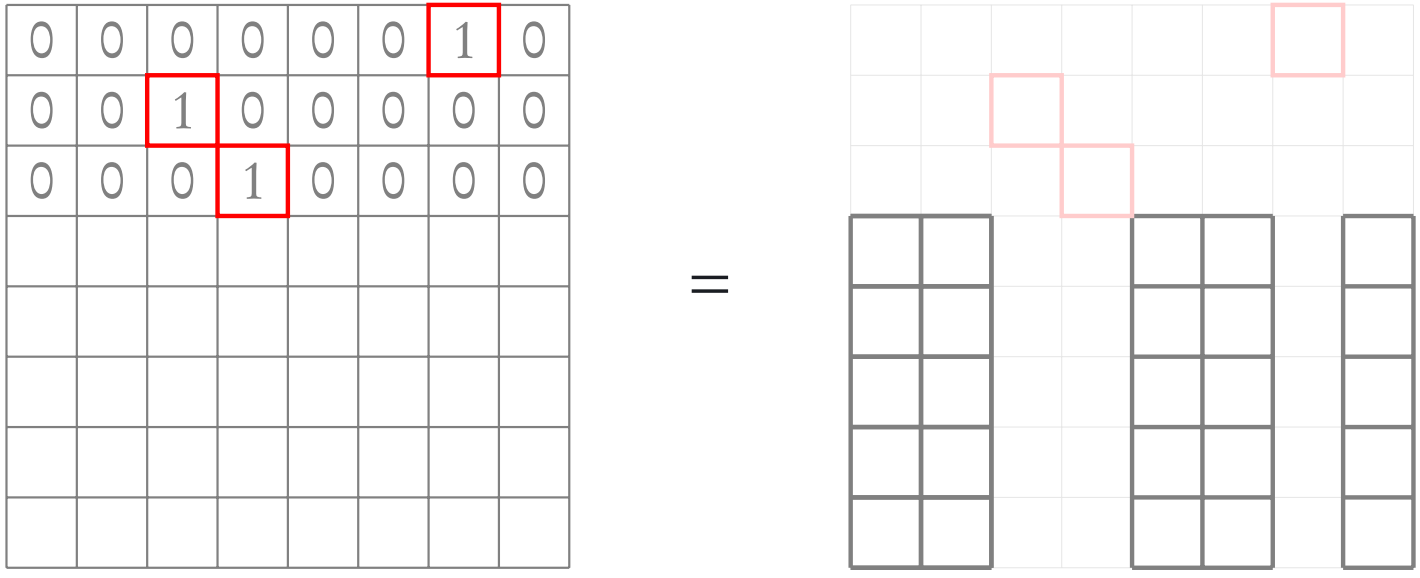
0	0	0	0	0	0	1	0
0	0	1	0	0	0	0	0
0	0	0	1	0	0	0	0

=



Partial evaluations as proxies

Think of the polynomial Perm...



Lemma

For nice polynomials $P(\mathbf{y}, \mathbf{z})$,

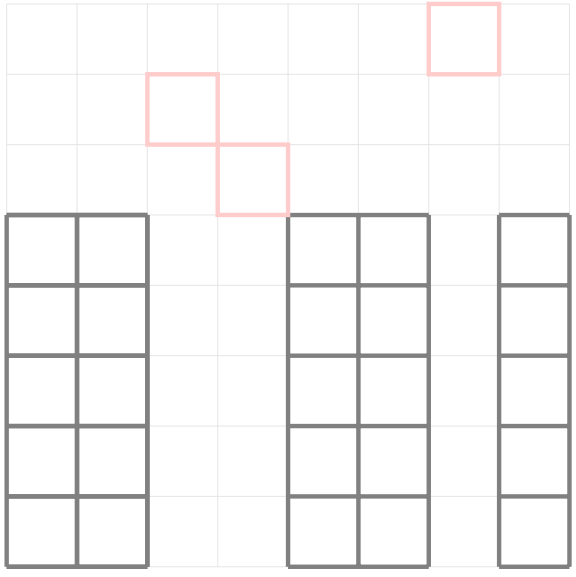
$$\partial_{\mathbf{y}}^{=k}(P) \quad \subseteq \quad \left\{ P(\mathbf{a}, \mathbf{z}) \,:\, \mathbf{a} \in \{0,1\}^{|\mathbf{y}|} \,,\, |\mathbf{a}|_0 = k \right\}$$

Partial evaluations as proxies

Think of the polynomial Perm...

0	0	0	0	0	0	1	0
0	0	1	0	0	0	0	0
0	0	0	1	0	0	0	0

=



Lemma

For set-multilinear polynomials $P(\mathbf{y},\mathbf{z})$,

$$\partial_{\mathbf{y}}^{=k}(P) \quad \subseteq \quad \left\{ P(\mathbf{a},\mathbf{z}) \,:\, \mathbf{a} \in \{0,1\}^{|\mathbf{y}|} \,,\, |\mathbf{a}|_0 = k \right\}$$

Partial evaluations as proxies

Lemma

For set-multilinear polynomials $P(\mathbf{y}, \mathbf{z})$,

$$\partial_{\mathbf{y}}^{=k}(P) \quad \subseteq \quad \left\{ P(\mathbf{a}, \mathbf{z}) \,:\, \mathbf{a} \in \{0,1\}^{|\mathbf{y}|} \,,\, |\mathbf{a}|_0 = k \right\}$$

Partial evaluations as proxies

Lemma

For set-multilinear polynomials $P(\mathbf{y}, \mathbf{z})$,

$$\partial_{\mathbf{y}}^{=k}(P) \subseteq \left\{ P(\mathbf{a}, \mathbf{z}) : \mathbf{a} \in \{0,1\}^{|\mathbf{y}|}, |\mathbf{a}|_0 = k \right\}$$

$$\therefore \quad \dim \partial_{\mathbf{y}}^{=k}(P) \leq \dim \left\{ P(\mathbf{a}, \mathbf{z}) : \mathbf{a} \in \{0,1\}^{|\mathbf{y}|}, |\mathbf{a}|_0 = k \right\}$$

Partial evaluations as proxies ...

For arbitrary polynomials,

If $\dim \partial_{\mathbf{y}}^{=k}(P)$ *is small, does that also imply that* $\dim\{P(\mathbf{a},\mathbf{z})\}$ *also has to be small-ish?*

Partial evaluations as proxies ...

For arbitrary polynomials,

If $\dim \partial_{\mathbf{y}}^{=k}(P)$ *is small, does that also imply that* $\dim\{P(\mathbf{a},\mathbf{z})\}$ *also has to be small-ish?*

Partial evaluations as proxies ...

For arbitrary polynomials,

If $\dim \partial_{\mathbf{y}}^{=k}(P)$ *is small, does that also imply that* $\dim\{P(\mathbf{a},\mathbf{z})\}$ *also has to be small-ish?*

$$P(\mathbf{a}+\mathbf{y},\mathbf{z}) =: P_{\mathbf{z}}(\mathbf{a}+\mathbf{y}) = \sum \left(\partial_{\mathbf{y}^{\mathbf{e}}} P_{\mathbf{z}}\right) \cdot \mathbf{a}^{\mathbf{e}}$$

Partial evaluations as proxies ...

For arbitrary polynomials,

If $\dim \partial_{\mathbf{y}}^{=k}(P)$ *is small, does that also imply that* $\dim\{P(\mathbf{a},\mathbf{z})\}$ *also has to be small-ish?*

$$P(\mathbf{a}+\mathbf{y},\mathbf{z}) =: P_{\mathbf{z}}(\mathbf{a}+\mathbf{y}) = \sum_{|\mathbf{e}|_0 \le k} \left(\partial_{\mathbf{y}^{\mathbf{e}}} P_{\mathbf{z}}\right)\cdot \mathbf{a}^{\mathbf{e}} + \sum_{|\mathbf{e}|_0 > k} \left(\partial_{\mathbf{y}^{\mathbf{e}}} P_{\mathbf{z}}\right)\cdot \mathbf{a}^{\mathbf{e}}$$

Partial evaluations as proxies ...

For arbitrary polynomials,

If $\dim \partial_{\mathbf{y}}^{=k}(P)$ *is small, does that also imply that* $\dim\{P(\mathbf{a},\mathbf{z})\}$ *also has to be small-ish?*

$$P(\mathbf{a}+\mathbf{y},\mathbf{z}) =: P_{\mathbf{z}}(\mathbf{a}+\mathbf{y}) = \sum_{|\mathbf{e}|_0 \le k} \left(\partial_{\mathbf{y}^{\mathbf{e}}} P_{\mathbf{z}}\right) \cdot \mathbf{a}^{\mathbf{e}} + \sum_{|\mathbf{e}|_0 > k} \left(\partial_{\mathbf{y}^{\mathbf{e}}} P_{\mathbf{z}}\right) \cdot \mathbf{a}^{\mathbf{e}}$$

Partial evaluations as proxies ...

For arbitrary polynomials,

If $\dim \partial_{\mathbf{y}}^{=k}(P)$ *is small, does that also imply that* $\dim\{P(\mathbf{a},\mathbf{z})\}$ *also has to be small-ish?*

$$P(\mathbf{a}+\mathbf{y},\mathbf{z}) =: P_{\mathbf{z}}(\mathbf{a}+\mathbf{y}) = \sum_{|\mathbf{e}|_0 \le k} \left(\partial_{\mathbf{y}^{\mathbf{e}}} P_{\mathbf{z}}\right) \cdot \mathbf{a}^{\mathbf{e}}$$

Partial evaluations as proxies ...

For arbitrary polynomials,

If $\dim \partial_{\mathbf{y}}^{=k}(P)$ *is small, does that also imply that* $\dim\{P(\mathbf{a},\mathbf{z})\}$ *also has to be small-ish?*

$$P(\mathbf{a}+\mathbf{y},\mathbf{z}) =: P_{\mathbf{z}}(\mathbf{a}+\mathbf{y}) = \sum_{|\mathbf{e}|_0 \le k} \left(\partial_{\mathbf{y}^{\mathbf{e}}} P_{\mathbf{z}}\right) \cdot \mathbf{a}^{\mathbf{e}}$$

If P has ind. degree r,

$$= \sum_{\substack{|\mathbf{e}|_0 \le k \\ |\mathbf{e}|_1 \le rk}} \left(\partial_{\mathbf{y}^{\mathbf{e}}} P_{\mathbf{z}}\right) \cdot \mathbf{a}^{\mathbf{e}}$$

Partial evaluations as proxies ...

For arbitrary polynomials,

If $\dim \partial_{\mathbf{y}}^{=k}(P)$ *is small, does that also imply that* $\dim\{P(\mathbf{a},\mathbf{z})\}$ *also has to be small-ish?*

$$P(\mathbf{a}+\mathbf{y},\mathbf{z}) =: P_{\mathbf{z}}(\mathbf{a}+\mathbf{y}) = \sum_{|\mathbf{e}|_0 \le k} \left(\partial_{\mathbf{y}^{\mathbf{e}}} P_{\mathbf{z}}\right) \cdot \mathbf{a}^{\mathbf{e}}$$

If P has ind. degree r,

$$= \sum_{\substack{|\mathbf{e}|_0 \le k \\ |\mathbf{e}|_1 \le rk}} \left(\partial_{\mathbf{y}^{\mathbf{e}}} P_{\mathbf{z}}\right) \cdot \mathbf{a}^{\mathbf{e}}$$

$$\therefore P(\mathbf{a},\mathbf{z}) = \sum_{\substack{|\mathbf{e}|_0 \le k \\ |\mathbf{e}|_1 \le rk}} \left(\partial_{\mathbf{y}^{\mathbf{e}}} P_{\mathbf{z}}\right)_{\mathbf{y}=0} \cdot \mathbf{a}^{\mathbf{e}}$$

Partial evaluations as proxies ...

Lemma

For any polynomial P of individual degree at most r, then

$$\left\{P(\mathbf{a},\mathbf{z}) \,:\, \mathbf{a}\in\{0,1\}^{|\mathbf{y}|}\,,\, |\mathbf{a}|_0 = k\right\} \quad \subseteq \quad \operatorname{span}\left\{\left(\partial_{\mathbf{y}}^{=rk}(P)\right)_{\mathbf{y}=0}\right\}$$

Proof.

$$P(\mathbf{a}+\mathbf{y},\mathbf{z}) =: P_{\mathbf{z}}(\mathbf{a}+\mathbf{y}) = \sum_{|\mathbf{e}|_0\le k}\left(\partial_{\mathbf{y}^{\mathbf{e}}}P_{\mathbf{z}}\right)\cdot\mathbf{a}^{\mathbf{e}}$$

If P has ind. degree r, $$= \sum_{\substack{|\mathbf{e}|_0\le k\\ |\mathbf{e}|_1\le rk}}\left(\partial_{\mathbf{y}^{\mathbf{e}}}P_{\mathbf{z}}\right)\cdot\mathbf{a}^{\mathbf{e}}$$

$$\therefore P(\mathbf{a},\mathbf{z}) = \sum_{\substack{|\mathbf{e}|_0\le k\\ |\mathbf{e}|_1\le rk}}\left(\partial_{\mathbf{y}^{\mathbf{e}}}P_{\mathbf{z}}\right)_{\mathbf{y}=0}\cdot\mathbf{a}^{\mathbf{e}} \qquad \square$$

Partial evaluations as proxies ...

Lemma

For any polynomial P of individual degree at most r, then

$$\left\{ P(\mathbf{a},\mathbf{z}) \,:\, \mathbf{a} \in \{0,1\}^{|\mathbf{y}|} \,,\, |\mathbf{a}|_0 = k \right\} \quad \subseteq \quad \operatorname{span}\left\{ \left(\partial_{\mathbf{y}}^{=rk}(P) \right)_{\mathbf{y}=0} \right\}$$

If $\dim \partial^{=rk}(P)$ *is small,*

then $\dim \left\{ P(\mathbf{a},\mathbf{z}) \,:\, \mathbf{a} \in \{0,1\}^{|\mathbf{y}|} \,,\, |\mathbf{a}|_0 = k \right\}$ *is also small.*

Making the measure ‘functional’

$$\Gamma_k^{(1)}(P) := \dim\, \partial_{\mathbf{y}}^{=k} P(\mathbf{y},\mathbf{z}) \qquad \subset \mathbb{F}[\mathbf{y},\mathbf{z}]$$

Making the measure 'functional'

$$\Gamma_k^{(1)}(P) := \dim\ \partial_{\mathbf{y}}^{=k} P(\mathbf{y},\mathbf{z}) \qquad \subset \mathbb{F}[\mathbf{y},\mathbf{z}]$$

$$\Gamma_k^{(2)}(P) := \dim\ \left\{ P(\mathbf{a},\mathbf{z}) \ :\ \mathbf{a} \in \{0,1\}^{|\mathbf{y}|}\ ,\ |\mathbf{a}|_0 \leq k \right\} \qquad \subset \mathbb{F}[\mathbf{z}]$$

Making the measure 'functional'

$$\Gamma_k^{(1)}(P) := \dim\ \partial_{\mathbf{y}}^{=k} P(\mathbf{y},\mathbf{z}) \qquad \subset \mathbb{F}[\mathbf{y},\mathbf{z}]$$

$$\Gamma_k^{(2)}(P) := \dim\ \left\{ P(\mathbf{a},\mathbf{z}) \,:\, \mathbf{a} \in \{0,1\}^{|\mathbf{y}|} \,,\, |\mathbf{a}|_0 \leq k \right\} \qquad \subset \mathbb{F}[\mathbf{z}]$$

$$\Gamma_k^{(3)}(P) := \dim\ \{ P(\mathbf{a},\mathbf{b}) \,:\, \mathbf{a},\mathbf{b} \in \{0,1\}^* \,,\, |\mathbf{a}|_0 \leq k \} \qquad \subset \mathbb{F}^n$$

Making the measure 'functional'

$$\Gamma_k^{(1)}(P) := \dim\ \partial_{\mathbf{y}}^{=k} P(\mathbf{y},\mathbf{z}) \qquad \subset \mathbb{F}[\mathbf{y},\mathbf{z}]$$

$$\Gamma_k^{(2)}(P) := \dim\ \left\{ P(\mathbf{a},\mathbf{z}) \,:\, \mathbf{a} \in \{0,1\}^{|\mathbf{y}|} \,,\, |\mathbf{a}|_0 \leq k \right\} \qquad \subset \mathbb{F}[\mathbf{z}]$$

$$\Gamma_k^{(3)}(P) := \dim\ \{ P(\mathbf{a},\mathbf{b}) \,:\, \mathbf{a},\mathbf{b} \in \{0,1\}^* \,,\, |\mathbf{a}|_0 \leq k \} \qquad \subset \mathbb{F}^n$$

Observation

If $P \equiv F$, then $\Gamma_k^{(3)}(P) = \Gamma_k^{(3)}(F)$.

Making the measure 'functional'

$$\Gamma_k^{(1)}(P) := \dim\ \partial_{\mathbf{y}}^{=k} P(\mathbf{y},\mathbf{z}) \qquad \subset \mathbb{F}[\mathbf{y},\mathbf{z}]$$

$$\Gamma_k^{(2)}(P) := \dim\ \left\{ P(\mathbf{a},\mathbf{z}) \,:\, \mathbf{a} \in \{0,1\}^{|\mathbf{y}|} \,,\, |\mathbf{a}|_0 \leq k \right\} \qquad \subset \mathbb{F}[\mathbf{z}]$$

$$\Gamma_k^{(3)}(P) := \dim\ \{ P(\mathbf{a},\mathbf{b}) \,:\, \mathbf{a},\mathbf{b} \in \{0,1\}^* \,,\, |\mathbf{a}|_0 \leq k \} \qquad \subset \mathbb{F}^n$$

Making the measure 'functional'

$$\Gamma_k^{(1)}(P) := \dim\ \partial_{\mathbf{y}}^{=k} P(\mathbf{y},\mathbf{z}) \qquad \subset \mathbb{F}[\mathbf{y},\mathbf{z}]$$

$$\Gamma_k^{(2)}(P) := \dim\ \left\{ P(\mathbf{a},\mathbf{z}) \,:\, \mathbf{a} \in \{0,1\}^{|\mathbf{y}|} \,,\, |\mathbf{a}|_0 \leq k \right\} \qquad \subset \mathbb{F}[\mathbf{z}]$$

$$\Gamma_k^{(3)}(P) := \dim\ \{ P(\mathbf{a},\mathbf{b}) \,:\, \mathbf{a},\mathbf{b} \in \{0,1\}^* \,,\, |\mathbf{a}|_0 \leq k \} \qquad \subset \mathbb{F}^n$$

Theorem

Let $C \in \mathscr{C}$ be a size s circuit computing a polynomial P of individual degree at most r. If $P \equiv$ Perm, then s must be large.

Making the measure 'functional'

$$\Gamma_k^{(1)}(P) := \dim\ \partial_{\mathbf{y}}^{=k} P(\mathbf{y},\mathbf{z}) \qquad \subset \mathbb{F}[\mathbf{y},\mathbf{z}]$$

$$\Gamma_k^{(2)}(P) := \dim\ \left\{ P(\mathbf{a},\mathbf{z}) \,:\, \mathbf{a} \in \{0,1\}^{|\mathbf{y}|} \,,\, |\mathbf{a}|_0 \leq k \right\} \qquad \subset \mathbb{F}[\mathbf{z}]$$

$$\Gamma_k^{(3)}(P) := \dim\ \{ P(\mathbf{a},\mathbf{b}) \,:\, \mathbf{a},\mathbf{b} \in \{0,1\}^* \,,\, |\mathbf{a}|_0 \leq k \} \qquad \subset \mathbb{F}^n$$

Theorem

Let $C \in \mathscr{C}$ be a size s circuit computing a polynomial P of individual degree at most r. If $P \equiv$ Perm, then s must be large.

Making the measure 'functional'

$$\Gamma_k^{(1)}(P) := \dim \partial_{\mathbf{y}}^{=k} P(\mathbf{y},\mathbf{z}) \qquad \subset \mathbb{F}[\mathbf{y},\mathbf{z}]$$

$$\Gamma_k^{(2)}(P) := \dim \left\{ P(\mathbf{a},\mathbf{z}) : \mathbf{a} \in \{0,1\}^{|\mathbf{y}|}, |\mathbf{a}|_0 \leq k \right\} \qquad \subset \mathbb{F}[\mathbf{z}]$$

$$\Gamma_k^{(3)}(P) := \dim \{ P(\mathbf{a},\mathbf{b}) : \mathbf{a},\mathbf{b} \in \{0,1\}^{*}, |\mathbf{a}|_0 \leq k \} \qquad \subset \mathbb{F}^n$$

Theorem

Let $C \in \mathscr{C}$ be a size s circuit computing a polynomial P of individual degree at most r. If $P \equiv$ Perm, then s must be large.

For the nice polynomial, Perm,

$$\Gamma_k^{(3)}(\text{Perm}) = \Gamma_k^{(2)}(\text{Perm}) = \Gamma_k^{(1)}(\text{Perm})$$

which is huge

Making the measure 'functional'

$$\Gamma_k^{(1)}(P) := \dim \partial_{\mathbf{y}}^{=k} P(\mathbf{y},\mathbf{z}) \qquad \subset \mathbb{F}[\mathbf{y},\mathbf{z}]$$

$$\Gamma_k^{(2)}(P) := \dim \left\{ P(\mathbf{a},\mathbf{z}) : \mathbf{a} \in \{0,1\}^{|\mathbf{y}|}, |\mathbf{a}|_0 \leq k \right\} \qquad \subset \mathbb{F}[\mathbf{z}]$$

$$\Gamma_k^{(3)}(P) := \dim \{ P(\mathbf{a},\mathbf{b}) : \mathbf{a},\mathbf{b} \in \{0,1\}^{*}, |\mathbf{a}|_0 \leq k \} \qquad \subset \mathbb{F}^n$$

Theorem

Let $C \in \mathscr{C}$ be a size s circuit computing a polynomial P of individual degree at most r. If $P \equiv$ Perm, then s must be large.

For the nice polynomial, Perm,

$$\Gamma_k^{(3)}(\text{Perm}) = \Gamma_k^{(2)}(\text{Perm}) = \Gamma_k^{(1)}(\text{Perm})$$

which is huge

For the circuit class,

$$\Gamma_k^{(3)}(P) \leq \Gamma_k^{(2)}(P)$$

Making the measure 'functional'

$$\Gamma_k^{(1)}(P) := \dim \partial_{\mathbf{y}}^{=k} P(\mathbf{y},\mathbf{z}) \qquad \subset \mathbb{F}[\mathbf{y},\mathbf{z}]$$

$$\Gamma_k^{(2)}(P) := \dim \left\{ P(\mathbf{a},\mathbf{z}) : \mathbf{a} \in \{0,1\}^{|\mathbf{y}|}, |\mathbf{a}|_0 \leq k \right\} \qquad \subset \mathbb{F}[\mathbf{z}]$$

$$\Gamma_k^{(3)}(P) := \dim \{ P(\mathbf{a},\mathbf{b}) : \mathbf{a},\mathbf{b} \in \{0,1\}^*, |\mathbf{a}|_0 \leq k \} \qquad \subset \mathbb{F}^n$$

Theorem

Let $C \in \mathscr{C}$ be a size s circuit computing a polynomial P of individual degree at most r. If $P \equiv$ Perm, then s must be large.

For the nice polynomial, Perm,

$$\Gamma_k^{(3)}(\text{Perm}) = \Gamma_k^{(2)}(\text{Perm}) = \Gamma_k^{(1)}(\text{Perm})$$

which is huge

For the circuit class,

$$\Gamma_k^{(3)}(P) \leq \Gamma_k^{(2)}(P) \leq \Gamma_{rk}^{(1)}(P)$$

Making the measure 'functional'

$$\Gamma_k^{(1)}(P) := \dim \partial_{\mathbf{y}}^{=k} P(\mathbf{y},\mathbf{z}) \qquad \subset \mathbb{F}[\mathbf{y},\mathbf{z}]$$

$$\Gamma_k^{(2)}(P) := \dim \left\{ P(\mathbf{a},\mathbf{z}) \,:\, \mathbf{a} \in \{0,1\}^{|\mathbf{y}|} \,,\, |\mathbf{a}|_0 \le k \right\} \qquad \subset \mathbb{F}[\mathbf{z}]$$

$$\Gamma_k^{(3)}(P) := \dim \{ P(\mathbf{a},\mathbf{b}) \,:\, \mathbf{a},\mathbf{b} \in \{0,1\}^* \,,\, |\mathbf{a}|_0 \le k \} \qquad \subset \mathbb{F}^n$$

Theorem

Let $C \in \mathscr{C}$ be a size s circuit computing a polynomial P of individual degree at most r. If $P \equiv$ Perm, then s must be large.

For the nice polynomial, Perm,

$$\begin{aligned} \Gamma_k^{(3)}(\text{Perm}) &= \Gamma_k^{(2)}(\text{Perm}) \\ &= \Gamma_k^{(1)}(\text{Perm}) \end{aligned}$$

which is huge

For the circuit class,

$$\begin{aligned} \Gamma_k^{(3)}(P) &\le \Gamma_k^{(2)}(P) \\ &\le \Gamma_{rk}^{(1)}(P) \end{aligned}$$

which is small

Making the measure 'functional'

$$\Gamma_k^{(1)}(P) := \dim \partial_{\mathbf{y}}^{=k} P(\mathbf{y},\mathbf{z}) \qquad \subset \mathbb{F}[\mathbf{y},\mathbf{z}]$$

$$\Gamma_k^{(2)}(P) := \dim \left\{ P(\mathbf{a},\mathbf{z}) \,:\, \mathbf{a} \in \{0,1\}^{|\mathbf{y}|} \,,\, |\mathbf{a}|_0 \le k \right\} \qquad \subset \mathbb{F}[\mathbf{z}]$$

$$\Gamma_k^{(3)}(P) := \dim \{ P(\mathbf{a},\mathbf{b}) \,:\, \mathbf{a},\mathbf{b} \in \{0,1\}^* \,,\, |\mathbf{a}|_0 \le k \} \qquad \subset \mathbb{F}^n$$

Theorem

Let $C \in \mathscr{C}$ be a size s circuit computing a polynomial P of individual degree at most r. If $P \equiv$ Perm, then s must be large.

For the nice polynomial, Perm,

$$\begin{aligned} \Gamma_k^{(3)}(\text{Perm}) &= \Gamma_k^{(2)}(\text{Perm}) \\ &= \Gamma_k^{(1)}(\text{Perm}) \end{aligned}$$

which is huge

For the circuit class,

$$\begin{aligned} \Gamma_k^{(3)}(P) &\le \Gamma_k^{(2)}(P) \\ &\le \Gamma_{rk}^{(1)}(P) \end{aligned}$$

which is small

unless s is large □

Function versions of common measures

- **Dimension of partial derivatives**

$$\Gamma_k^{(1)}(P) := \dim\ \partial_{\mathbf{y}}^{=k} P(\mathbf{y},\mathbf{z}) \qquad \subset \mathbb{F}[\mathbf{y},\mathbf{z}]$$

$$\Gamma_k^{(2)}(P) := \dim\ \{P(\mathbf{a},\mathbf{b}) \ :\ \mathbf{a},\mathbf{b} \in \{0,1\}^*\ ,\ |\mathbf{a}|_0 \leq k\} \qquad \subset \mathbb{F}^n$$

Function versions of common measures

- **Dimension of partial derivatives**

$$\Gamma_k^{(1)}(P) := \dim \partial_{\mathbf{y}}^{=k} P(\mathbf{y},\mathbf{z}) \qquad \subset \mathbb{F}[\mathbf{y},\mathbf{z}]$$

$$\Gamma_k^{(2)}(P) := \dim \{P(\mathbf{a},\mathbf{b}) : \mathbf{a},\mathbf{b} \in \{0,1\}^*, |\mathbf{a}|_0 \leq k\} \qquad \subset \mathbb{F}^n$$

Useful in the case of depth three powering, and homogeneous depth three circuits.

Function versions of common measures

- **Dimension of partial derivatives**

$$\Gamma_k^{(1)}(P) := \dim\ \partial_{\mathbf{y}}^{=k} P(\mathbf{y},\mathbf{z}) \qquad \subset \mathbb{F}[\mathbf{y},\mathbf{z}]$$

$$\Gamma_k^{(2)}(P) := \dim\ \{P(\mathbf{a},\mathbf{b}) \,:\, \mathbf{a},\mathbf{b} \in \{0,1\}^*\ ,\ |\mathbf{a}|_0 \leq k\} \qquad \subset \mathbb{F}^n$$

Useful in the case of depth three powering, and homogeneous depth three circuits.

- **Dimension of shifted partial derivatives**

$$\Gamma_{k,\ell}^{(1)}(P) := \dim\ (\mathbf{y},\mathbf{z})^{=\ell}\ \partial_{\mathbf{y}}^{=k} P(\mathbf{y},\mathbf{z})$$

Function versions of common measures

- **Dimension of partial derivatives**

$$\Gamma_k^{(1)}(P) := \dim \partial_{\mathbf{y}}^{=k} P(\mathbf{y},\mathbf{z}) \qquad \subset \mathbb{F}[\mathbf{y},\mathbf{z}]$$

$$\Gamma_k^{(2)}(P) := \dim \{P(\mathbf{a},\mathbf{b}) : \mathbf{a},\mathbf{b} \in \{0,1\}^* , |\mathbf{a}|_0 \leq k\} \qquad \subset \mathbb{F}^n$$

Useful in the case of depth three powering, and homogeneous depth three circuits.

- **Dimension of shifted partial derivatives**

$$\Gamma_{k,\ell}^{(1)}(P) := \dim (\mathbf{y},\mathbf{z})^{=\ell} \partial_{\mathbf{y}}^{=k} P(\mathbf{y},\mathbf{z})$$

$$\Gamma_{k,\ell}^{(2)}(P) := \left\{ TT\left(\mathbf{z}^{=\ell} \cdot P(\mathbf{a},\mathbf{z})\right) : \mathbf{a} \in \{0,1\}^{|\mathbf{y}|} , |\mathbf{a}|_0 \leq k \right\}$$

(If you set parameters right)

Function versions of common measures

- **Dimension of partial derivatives**

$$\Gamma_k^{(1)}(P) := \dim\ \partial_{\mathbf{y}}^{=k} P(\mathbf{y},\mathbf{z}) \qquad \subset \mathbb{F}[\mathbf{y},\mathbf{z}]$$

$$\Gamma_k^{(2)}(P) := \dim\ \{P(\mathbf{a},\mathbf{b}) \ :\ \mathbf{a},\mathbf{b} \in \{0,1\}^*\ ,\ |\mathbf{a}|_0 \leq k\} \qquad \subset \mathbb{F}^n$$

Useful in the case of depth three powering, and homogeneous depth three circuits.

- **Dimension of shifted partial derivatives**

$$\Gamma_{k,\ell}^{(1)}(P) := \dim\ (\mathbf{y},\mathbf{z})^{=\ell}\ \partial_{\mathbf{y}}^{=k} P(\mathbf{y},\mathbf{z})$$

$$\Gamma_{k,\ell}^{(2)}(P) := \left\{TT\left(\mathbf{z}^{=\ell} \cdot P(\mathbf{a},\mathbf{z})\right) \ :\ \mathbf{a} \in \{0,1\}^{|\mathbf{y}|}\ ,\ |\mathbf{a}|_0 \leq k\right\}$$

Useful for a natural sub-class of hom. depth four circuits.

The measure for depth four circuits

- Dimension of *projected* shifted partial derivatives

$$\Gamma^{(1)}_{k,\ell}(P(\mathbf{y},\mathbf{z})) \quad := \quad \dim\left\{\mathrm{mult}\left(\mathbf{x}^{=\ell}\cdot\partial^{=k}_{\mathbf{y}}(P)\right)\right\}$$

The measure for depth four circuits

- **Dimension of *projected* shifted partial derivatives**

$$\begin{aligned}\Gamma^{(1)}_{k,\ell}(P(\mathbf{y},\mathbf{z})) &:= \dim\left\{\mathrm{mult}\left(\mathbf{x}^{=\ell}\cdot\partial^{=k}_{\mathbf{y}}(P)\right)\right\}\\ &= \dim\left\{\left(\mathbf{x}^{=\ell}\cdot\partial^{=k}_{\mathbf{y}}(P)\right) \bmod \langle x_i^2 = 0\rangle\right\}\end{aligned}$$

The measure for depth four circuits

- **Dimension of *projected* shifted partial derivatives**

$$\begin{aligned}\Gamma^{(1)}_{k,\ell}(P(\mathbf{y},\mathbf{z})) &:= \dim\left\{\mathrm{mult}\left(\mathbf{x}^{=\ell}\cdot\partial^{=k}_{\mathbf{y}}(P)\right)\right\}\\ &= \dim\left\{\left(\mathbf{x}^{=\ell}\cdot\partial^{=k}_{\mathbf{y}}(P)\right) \bmod \langle x_i^2 = 0\rangle\right\}\end{aligned}$$

Messes up evaluations

The measure for depth four circuits

- Dimension of *projected* shifted partial derivatives

$$\Gamma^{(1)}_{k,\ell}(P(\mathbf{y},\mathbf{z})) := \dim\left\{\mathrm{mult}\left(\mathbf{x}^{=\ell}\cdot\partial^{=k}_{\mathbf{y}}(P)\right)\right\}$$
$$= \dim\left\{\left(\mathbf{x}^{=\ell}\cdot\partial^{=k}_{\mathbf{y}}(P)\right) \bmod \langle x_i^2 = 0\rangle\right\}$$

$$\Gamma^{(2)}_{k,\ell}(P(\mathbf{y},\mathbf{z})) := \dim\left\{\left(\mathbf{x}^{=\ell}\cdot\partial^{=k}_{\mathbf{y}}(P)\right) \bmod \langle x_i^2 = x_i\rangle\right\}$$

The measure for depth four circuits

- Dimension of *projected* shifted partial derivatives

$$\Gamma^{(1)}_{k,\ell}(P(\mathbf{y},\mathbf{z})) := \dim\left\{\mathrm{mult}\left(\mathbf{x}^{=\ell}\cdot\partial^{=k}_{\mathbf{y}}(P)\right)\right\}$$
$$= \dim\left\{\left(\mathbf{x}^{=\ell}\cdot\partial^{=k}_{\mathbf{y}}(P)\right) \bmod \left\langle x_i^2 = 0\right\rangle\right\}$$

$$\Gamma^{(2)}_{k,\ell}(P(\mathbf{y},\mathbf{z})) := \dim\left\{\left(\mathbf{x}^{=\ell}\cdot\partial^{=k}_{\mathbf{y}}(P)\right) \bmod \left\langle x_i^2 = x_i\right\rangle\right\}$$

$$\Gamma^{(3)}_{k,\ell}(P(\mathbf{y},\mathbf{z})) := \dim\left\{\left(\mathbf{z}^{=\ell}\cdot P(\mathbf{a},\mathbf{z})\right) : \mathbf{a}\in\{0,1\}^{|\mathbf{y}|}, |\mathbf{a}|_0 \le k\right\}$$

The measure for depth four circuits

- **Dimension of *projected* shifted partial derivatives**

$$\Gamma^{(1)}_{k,\ell}(P(\mathbf{y},\mathbf{z})) := \dim\left\{\mathrm{mult}\left(\mathbf{x}^{=\ell}\cdot\partial^{=k}_{\mathbf{y}}(P)\right)\right\}$$
$$= \dim\left\{\left(\mathbf{x}^{=\ell}\cdot\partial^{=k}_{\mathbf{y}}(P)\right) \bmod \langle x_i^2 = 0\rangle\right\}$$

$$\Gamma^{(2)}_{k,\ell}(P(\mathbf{y},\mathbf{z})) := \dim\left\{\left(\mathbf{x}^{=\ell}\cdot\partial^{=k}_{\mathbf{y}}(P)\right) \bmod \langle x_i^2 = x_i\rangle\right\}$$

$$\Gamma^{(3)}_{k,\ell}(P(\mathbf{y},\mathbf{z})) := \dim\left\{\left(\mathbf{z}^{=\ell}\cdot P(\mathbf{a},\mathbf{z})\right) : \mathbf{a}\in\{0,1\}^{|\mathbf{y}|}, |\mathbf{a}|_0 \le k\right\}$$

$$\Gamma^{(4)}_{k,\ell}(P(\mathbf{y},\mathbf{z})) := \dim\left\{TT\left(\mathbf{z}^{=\ell}\cdot P(\mathbf{a},\mathbf{z})\right) : \mathbf{a}\in\{0,1\}^{|\mathbf{y}|}, |\mathbf{a}|_0 \le k\right\}$$

The measure for depth four circuits

- **Dimension of *projected* shifted partial derivatives**

$$\Gamma^{(1)}_{k,\ell}(P(\mathbf{y},\mathbf{z})) := \dim\left\{\mathrm{mult}\left(\mathbf{x}^{=\ell}\cdot\partial^{=k}_{\mathbf{y}}(P)\right)\right\} = \dim\left\{\left(\mathbf{x}^{=\ell}\cdot\partial^{=k}_{\mathbf{y}}(P)\right) \bmod \left\langle x_i^2 = 0\right\rangle\right\}$$

$$\Gamma^{(2)}_{k,\ell}(P(\mathbf{y},\mathbf{z})) := \dim\left\{\left(\mathbf{x}^{=\ell}\cdot\partial^{=k}_{\mathbf{y}}(P)\right) \bmod \left\langle x_i^2 = x_i\right\rangle\right\}$$

$$\Gamma^{(3)}_{k,\ell}(P(\mathbf{y},\mathbf{z})) := \dim\left\{\left(\mathbf{z}^{=\ell}\cdot P(\mathbf{a},\mathbf{z})\right) \,:\, \mathbf{a}\in\{0,1\}^{|\mathbf{y}|}\,,\, |\mathbf{a}|_0 \le k\right\}$$

$$\Gamma^{(4)}_{k,\ell}(P(\mathbf{y},\mathbf{z})) := \dim\left\{TT\left(\mathbf{z}^{=\ell}\cdot P(\mathbf{a},\mathbf{z})\right) \,:\, \mathbf{a}\in\{0,1\}^{|\mathbf{y}|}\,,\, |\mathbf{a}|_0 \le k\right\}$$

Finally, left to check that

$$\Gamma^{(4)}_{k,\ell}(\text{circuit class}) \le \Gamma^{(1)}_{rk,\ell}(\text{circuit class}) \ll \Gamma^{(4)}_{k,\ell}(\text{hard polynomial})$$

The measure for depth four circuits

- **Dimension of *projected* shifted partial derivatives**

$$\Gamma^{(1)}_{k,\ell}(P(\mathbf{y},\mathbf{z})) := \dim\left\{\mathrm{mult}\left(\mathbf{x}^{=\ell}\cdot\partial^{=k}_{\mathbf{y}}(P)\right)\right\} = \dim\left\{\left(\mathbf{x}^{=\ell}\cdot\partial^{=k}_{\mathbf{y}}(P)\right) \bmod \left\langle x_i^2 = 0\right\rangle\right\}$$

$$\Gamma^{(2)}_{k,\ell}(P(\mathbf{y},\mathbf{z})) := \dim\left\{\left(\mathbf{x}^{=\ell}\cdot\partial^{=k}_{\mathbf{y}}(P)\right) \bmod \left\langle x_i^2 = x_i\right\rangle\right\}$$

$$\Gamma^{(3)}_{k,\ell}(P(\mathbf{y},\mathbf{z})) := \dim\left\{\left(\mathbf{z}^{=\ell}\cdot P(\mathbf{a},\mathbf{z})\right) : \mathbf{a}\in\{0,1\}^{|\mathbf{y}|}, |\mathbf{a}|_0 \le k\right\}$$

$$\Gamma^{(4)}_{k,\ell}(P(\mathbf{y},\mathbf{z})) := \dim\left\{TT\left(\mathbf{z}^{=\ell}\cdot P(\mathbf{a},\mathbf{z})\right) : \mathbf{a}\in\{0,1\}^{|\mathbf{y}|}, |\mathbf{a}|_0 \le k\right\}$$

Finally, left to check that

$$\Gamma^{(4)}_{k,\ell}(\text{circuit class}) \le \Gamma^{(1)}_{rk,\ell}(\text{circuit class}) \ll \Gamma^{(4)}_{k,\ell}(\text{hard polynomial})$$ □

Closing remarks

- Always worth asking if syntactic lower bounds also extend to the functional lower bounds. Might have connections to boolean complexity and proof complexity.
- Possible to use proxies like additive derivatives ($f(\mathbf{x}+\mathbf{a})-f(\mathbf{x})$), partial evaluations, or Taylor expansion tricks etc. to lift known examples.

Closing remarks

- Always worth asking if syntactic lower bounds also extend to the functional lower bounds. Might have connections to boolean complexity and proof complexity.
- Possible to use proxies like additive derivatives $(f(\mathbf{x}+\mathbf{a})-f(\mathbf{x}))$, partial evaluations, or Taylor expansion tricks etc. to lift known examples.
- The individual degree restriction is annoying...

Closing remarks

- Always worth asking if syntactic lower bounds also extend to the functional lower bounds. Might have connections to boolean complexity and proof complexity.
- Possible to use proxies like additive derivatives ($f(\mathbf{x}+\mathbf{a})-f(\mathbf{x})$), partial evaluations, or Taylor expansion tricks etc. to lift known examples.
- The individual degree restriction is annoying...

- **Question:** Can we remove the ind. degree restriction and prove functional lower bounds for *sums of powers of quadratics*?

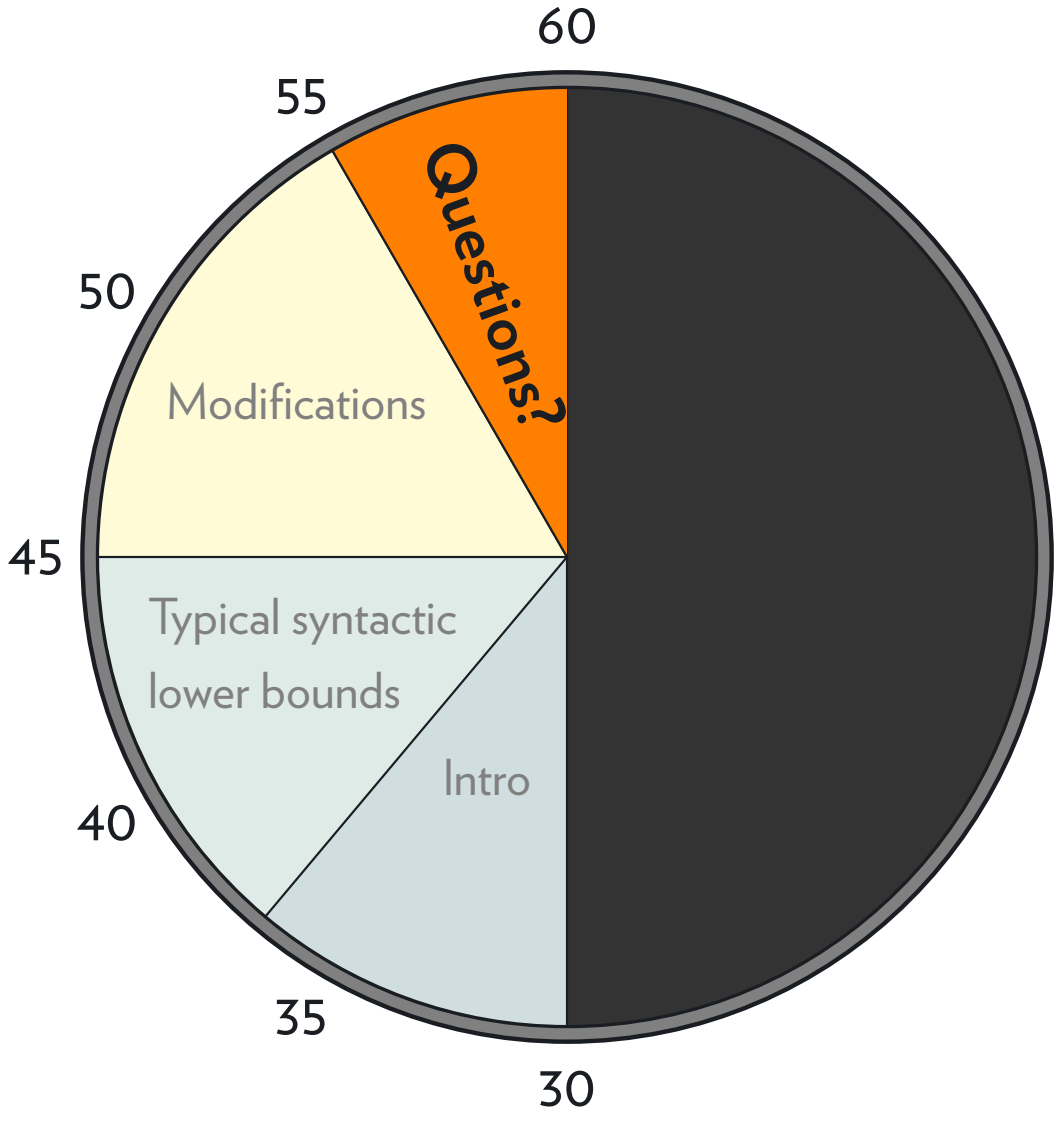
Closing remarks

- Always worth asking if syntactic lower bounds also extend to the functional lower bounds. Might have connections to boolean complexity and proof complexity.
- Possible to use proxies like additive derivatives $(f(\mathbf{x}+\mathbf{a})-f(\mathbf{x}))$, partial evaluations, or Taylor expansion tricks etc. to lift known examples.
- The individual degree restriction is annoying...

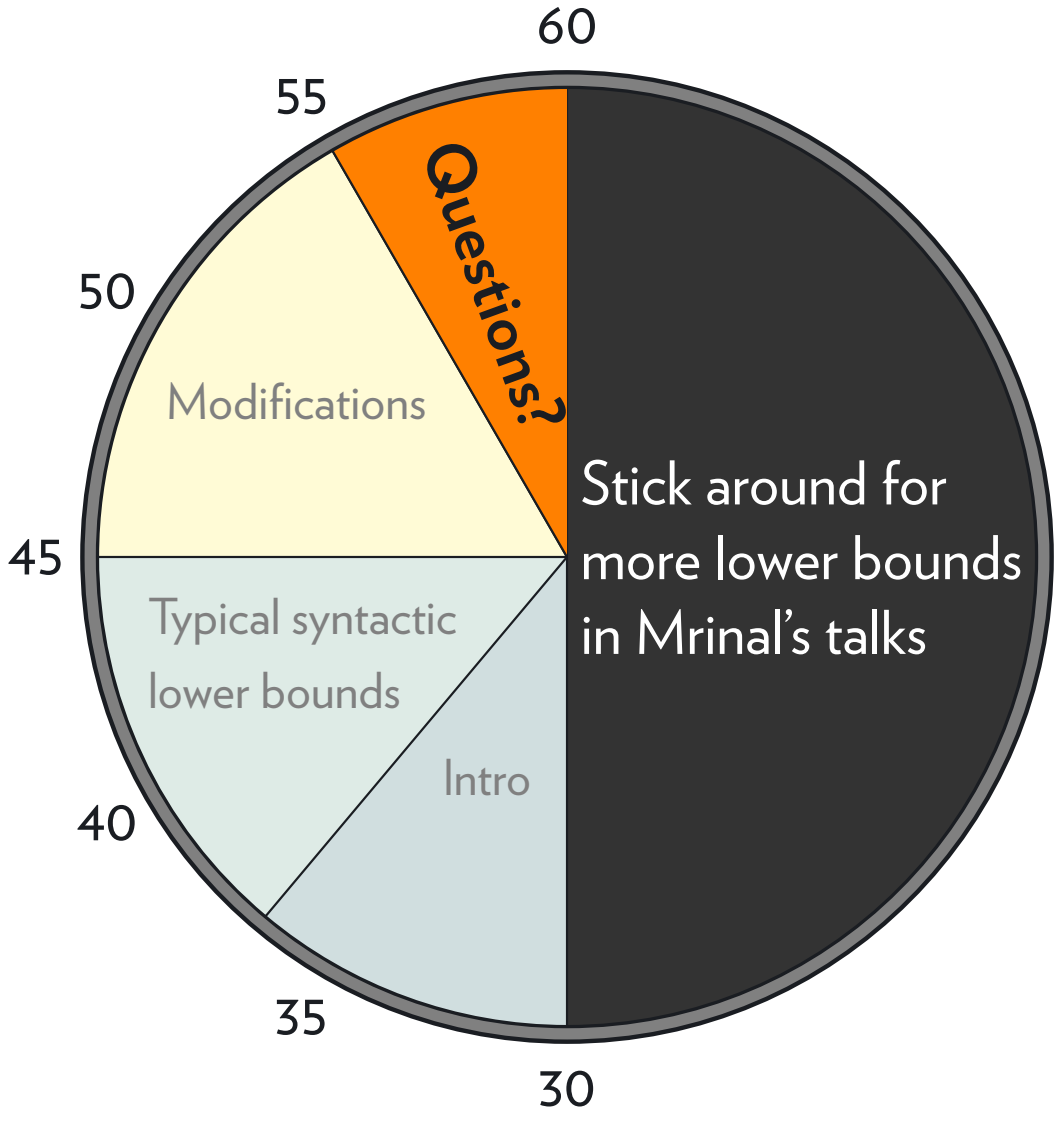
- **Question:** Can we remove the ind. degree restriction and prove functional lower bounds for *sums of powers of quadratics*?

- **Question:** What about approximate functional computation, i.e. agreement on *most* points on $\{0,1\}^n$?

Thank you


60
55
50
45
40
35
30
Questions?
Modifications
Typical syntactic
lower bounds
Intro

Thank you


60
55
50
45
40
35
30
Questions?
Modifications
Typical syntactic lower bounds
Intro
Stick around for more lower bounds in Mrinal's talks