On TC^0 Lower Bounds for the Permanent

Jeff Kinne

Indiana State University, USA

COCOON, August 22, 2012

Note: slides online at kinnejeff.com

Main Result, Definitions and Context

Theorem (Main Result)

Theorem (Main Result)

Lower bound for Perm *on threshold circuits with depth* d*, advice* a*, size* s*, s.t.*

- $d = O(1)$, $a = \text{poly-log}(n)$, s s.t. $s^{(O(1))}(n) < 2^n$
- $d = o(\log\log n)$, $a = \text{poly-log}(n)$, $s = n^{O(1)}$
- $d = O(1)$, $a = n^{o(1)}$, $s = n^{O(1)}$

Theorem (Main Result)

Lower bound for Perm *on threshold circuits with depth* d, *advice* a, *size* s, *s.t.*

- $d = O(1)$, $a = \text{poly-log}(n)$, s s.t. $s^{(O(1))}(n) < 2^n$
- $d = o(\log \log n)$, $a = \text{poly-log}(n)$, $s = n^{O(1)}$
- $d = O(1)$, $a = n^{o(1)}$, $s = n^{O(1)}$

Theorem (Main Result)

Lower bound for Perm *on threshold circuits with depth* d, *advice* a, *size* s, *s.t.*

- $d = O(1)$, $a = \text{poly-log}(n)$, s s.t. $s^{(O(1))}(n) < 2^n$
- $d = o(\log\log n)$, $a = \text{poly-log}(n)$, $s = n^{O(1)}$
- $d = O(1)$, $a = n^{o(1)}$, $s = n^{O(1)}$

Basic info: Complexity Zoo

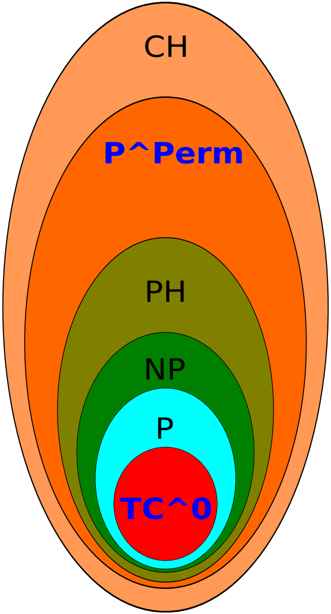
Theorem (Main Result)

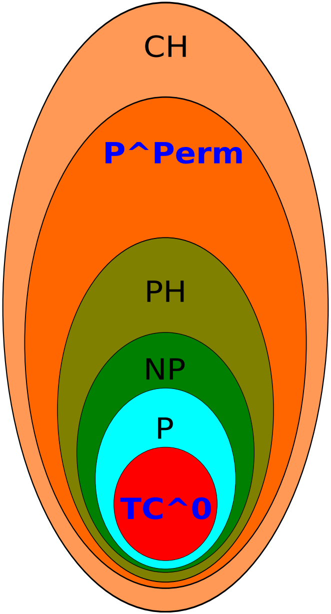
Lower bound for Perm *on threshold circuits with depth* d, *advice* a, *size* s, *s.t.*

- $d = O(1)$, $a = \text{poly-log}(n)$, s s.t. $s^{(O(1))}(n) < 2^n$
- $d = o(\log \log n)$, $a = \text{poly-log}(n)$, $s = n^{O(1)}$
- $d = O(1)$, $a = n^{o(1)}$, $s = n^{O(1)}$

Basic info: Complexity Zoo

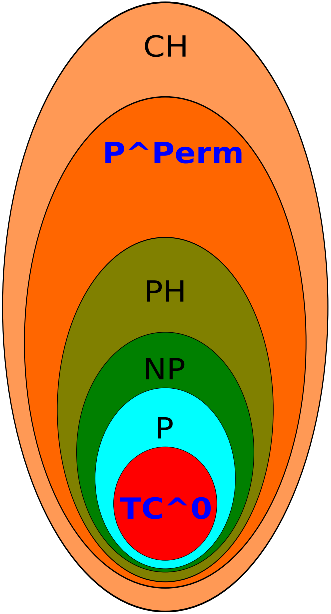
Main result also discovered by [CK12]


CH
P^Perm
PH
NP
P
TC^0



Permanent

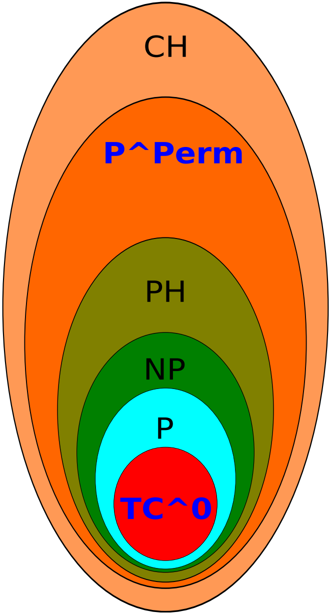
- Determinant without minus signs
- #P, PP, VNP-complete



Permanent

- Determinant without minus signs
- #P, PP, VNP-complete

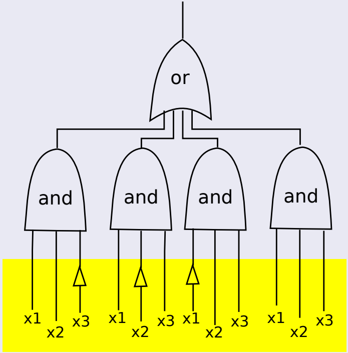
TC^0- Threshold Circuits

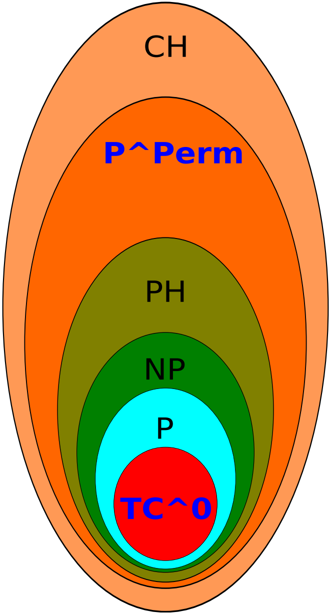


Permanent

- Determinant without minus signs
- #P, PP, VNP-complete

TC^0- Threshold Circuits

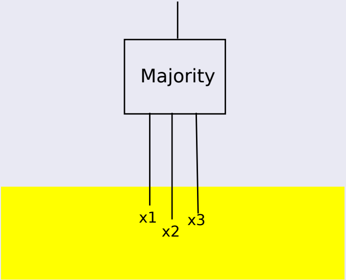


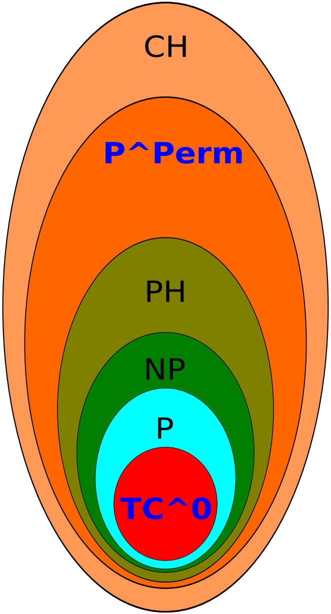


Permanent

- Determinant without minus signs
- #P, PP, VNP-complete

TC^0- Threshold Circuits

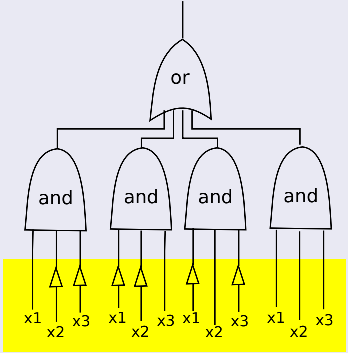


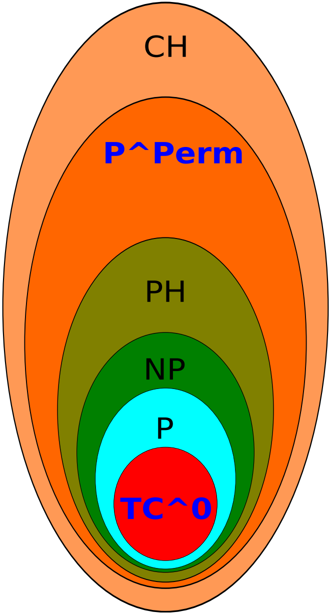


Permanent

- Determinant without minus signs
- #P, PP, VNP-complete

TC^0- Threshold Circuits

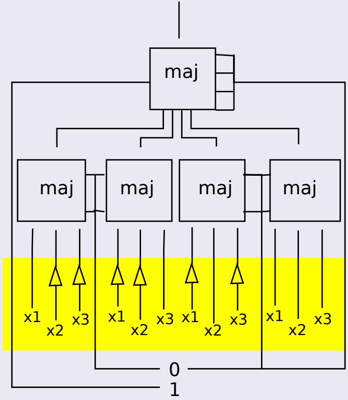


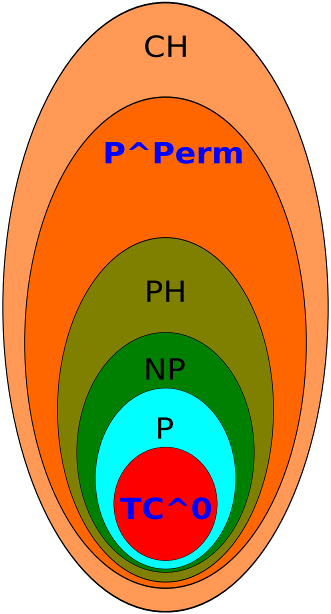


Permanent

- Determinant without minus signs
- #P, PP, VNP-complete

TC^0- Threshold Circuits



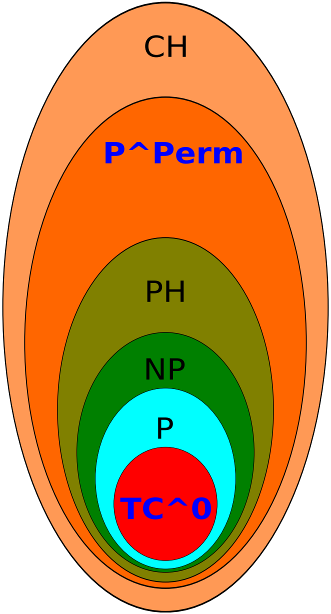


Permanent

- Determinant without minus signs
- #P, PP, VNP-complete

TC^0- Threshold Circuits

- constant depth, $\approx$ const parallel time

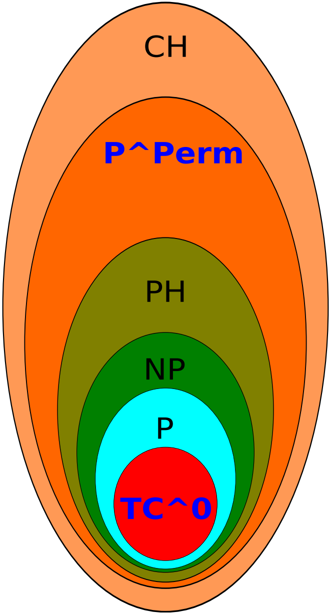


Permanent

- Determinant without minus signs
- #P, PP, VNP-complete

TC^0- Threshold Circuits

- constant depth, $\approx$ const parallel time
- integer arithmetic: $+$ - * /



Permanent

- Determinant without minus signs
- #P, PP, VNP-complete

TC^0- Threshold Circuits

- constant depth, $\approx$ const parallel time
- integer arithmetic: $+$ - * /
- PRGs, crypto? [NRR02]

TC^0 Lower Bounds

TC^0 Lower Bounds

- DTIME(super-poly) $\neq \mathrm{TC}^0$ (time hierarchy)

TC^0 Lower Bounds

- DTIME(super-poly) $\neq \mathrm{TC}^0$ (time hierarchy)
- SPACE(super-log) $\neq \mathrm{TC}^0$ (space hierarchy)

TC^0 Lower Bounds

- DTIME(super-poly) $\neq \mathrm{TC}^0$ (time hierarchy)
- SPACE(super-log) $\neq \mathrm{TC}^0$ (space hierarchy)

Threshold Circuit Lower Bounds

TC^0 Lower Bounds

- DTIME(super-poly) $\neq \mathrm{TC}^0$ (time hierarchy)
- SPACE(super-log) $\neq \mathrm{TC}^0$ (space hierarchy)

Threshold Circuit Lower Bounds

- $\mathrm{Perm} \not\subseteq$ TC size s, $s^{(O(1))} < 2^n$ [All99]

TC^0 Lower Bounds

- DTIME(super-poly) $\neq \mathrm{TC}^0$ (time hierarchy)
- SPACE(super-log) $\neq \mathrm{TC}^0$ (space hierarchy)

Threshold Circuit Lower Bounds

- $\mathrm{Perm} \not\subseteq$ TC size s, $s^{(O(1))} < 2^n$ [All99]
- $\mathrm{Perm} \not\subseteq$ TC depth $o(\log \log n)$, poly size [KP09]

TC^0 Lower Bounds

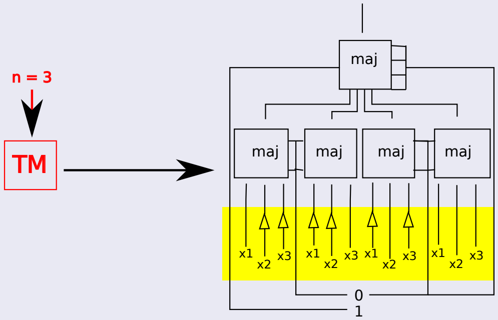
- DTIME(super-poly) $\neq \mathrm{TC}^0$ (time hierarchy)
- SPACE(super-log) $\neq \mathrm{TC}^0$ (space hierarchy)

Threshold Circuit Lower Bounds

- $\mathrm{Perm} \not\subseteq$ TC size s, $s^{(O(1))} < 2^n$ [All99]
- $\mathrm{Perm} \not\subseteq$ TC depth $o(\log\log n)$, poly size [KP09]
- $\mathrm{Perm} \not\subseteq$ arithmetic circuits with $n^{o(1)}$ advice [JS12]

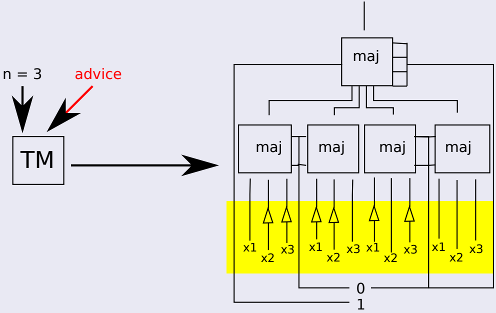
Uniform TC^0

Uniform TC^0

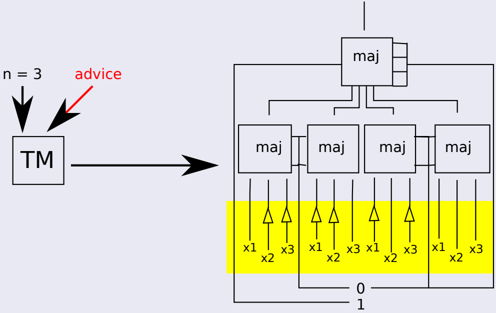


Non-uniform TC^0

Non-uniform TC^0

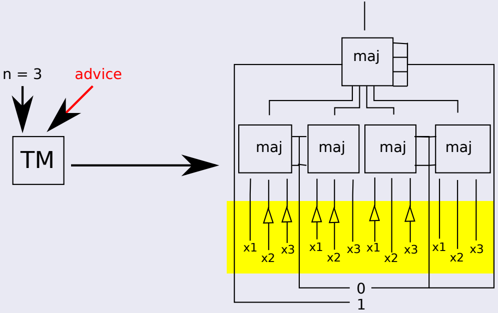


Non-uniform TC^0



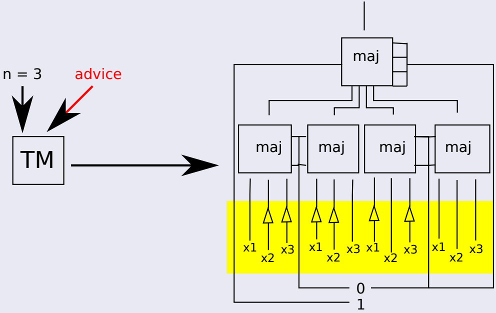
- Uniform: $|advice| = 0$

Non-uniform TC^0



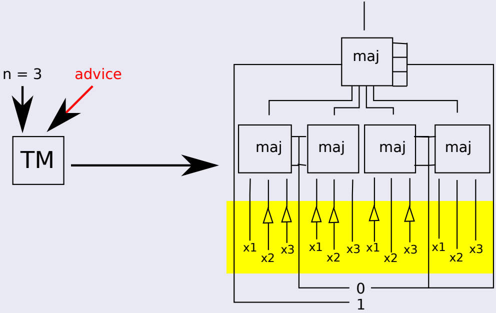
- Uniform: $|advice| = 0$
- Fully non-uniform: $|advice| \approx$ circuit size

Non-uniform TC^0



- Uniform: $|advice| = 0$
- Fully non-uniform: $|advice| \approx$ circuit size
- Slightly non-uniform: $|advice| << $ circuit size

Non-uniform TC^0



- Uniform: $|advice| = 0$
- Fully non-uniform: $|advice| \approx$ circuit size
- Slightly non-uniform: $|advice| << $ circuit size

Why Non-uniform Lower Bounds?

Why Non-uniform Lower Bounds?

- Search for mathematical truth...

Why Non-uniform Lower Bounds?

- Search for mathematical truth...
- Crytpo adversary

Why Non-uniform Lower Bounds?

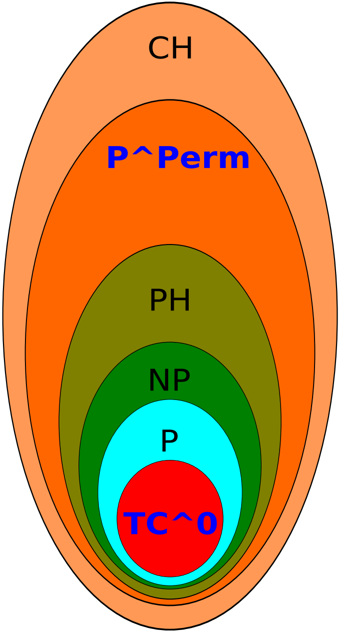
- Search for mathematical truth...
- Crytpo adversary
- Connections to derandomization

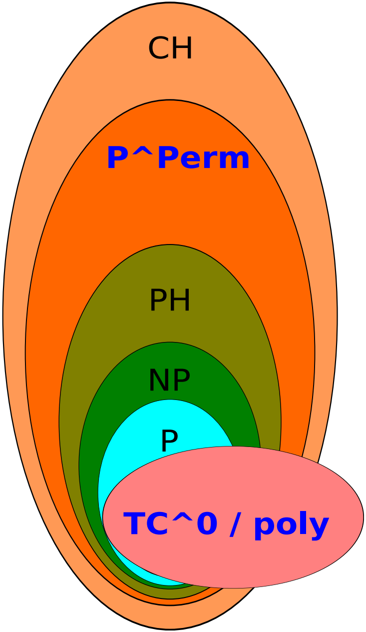
Why Non-uniform Lower Bounds?

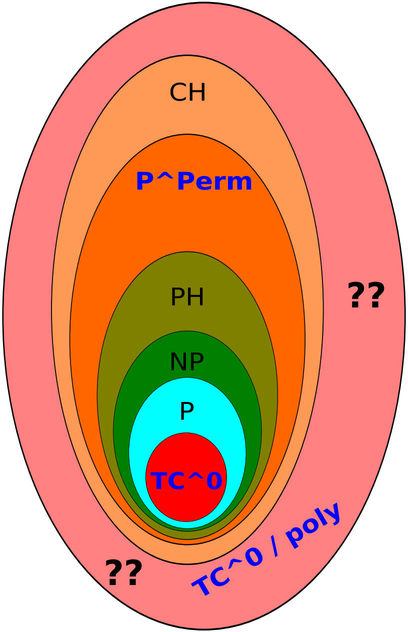
- Search for mathematical truth...
- Crytpo adversary
- Connections to derandomization
  $E \not\subseteq SIZE(2^{\epsilon n}) \Rightarrow BPP{=}P$ [IW97]

Why Non-uniform Lower Bounds?

- Search for mathematical truth...
- Crytpo adversary
- Connections to derandomization
  $E \not\subseteq \text{SIZE}(2^{\epsilon n}) \Rightarrow \text{BPP}=\text{P}$ [IW97]
  derandomization $\Rightarrow$ non-uniform lower bounds [KI04, AM11]


CH
P^Perm
PH
NP
P
TC^0


CH
P^Perm
PH
NP
P
TC^0 / poly


CH
P^Perm
PH
NP
P
TC^0
??
??
TC^0 / poly

Theorem (Main Result)

Theorem (Main Result)

Lower bound for Perm *on threshold circuits with depth* d, *advice* a, *size* s *s.t.*

- $d = O(1)$, $a = \text{poly-log}(n)$, s *s.t.* $s^{(O(1))}(n) < 2^n$
- $d = o(\log \log n)$, $a = \text{poly-log}(n)$, $s = n^{O(1)}$
- $d = O(1)$, $a = n^{o(1)}$, $s = n^{O(1)}$

Theorem (Main Result)

Lower bound for Perm *on threshold circuits with depth* d, *advice* a, *size* s *s.t.*

- $d = O(1)$, $a = \text{poly-log}(n)$, s s.t. $s^{(O(1))}(n) < 2^n$ $\approx\Rightarrow$ [All99]
- $d = o(\log\log n)$, $a = \text{poly-log}(n)$, $s = n^{O(1)}$
- $d = O(1)$, $a = n^{o(1)}$, $s = n^{O(1)}$

Theorem (Main Result)

Lower bound for Perm *on threshold circuits with depth* d*, advice* a*, size* s *s.t.*

- $d = O(1)$, $a = \text{poly-log}(n)$, s *s.t.* $s^{(O(1))}(n) < 2^n$ $\approx\Rightarrow$ *[All99]*
- $d = o(\log\log n)$, $a = \text{poly-log}(n)$, $s = n^{O(1)}$ $\Rightarrow$ *[KP09]*
- $d = O(1)$, $a = n^{o(1)}$, $s = n^{O(1)}$

Theorem (Main Result)

Lower bound for Perm *on threshold circuits with depth* d*, advice* a*, size* s *s.t.*

- $d = O(1)$, $a = \text{poly-log}(n)$, s s.t. $s^{(O(1))}(n) < 2^n$ $\approx\Rightarrow$ *[All99]*
- $d = o(\log\log n)$, $a = \text{poly-log}(n)$, $s = n^{O(1)}$ $\Rightarrow$ *[KP09]*
- $d = O(1)$, $a = n^{o(1)}$, $s = n^{O(1)}$ $\Rightarrow$ *[JS12]*

Theorem (Main Result)

Lower bound for Perm *on threshold circuits with depth* d*, advice* a*, size* s *s.t.*

- $d = O(1)$, $a = \text{poly-log}(n)$, s s.t. $s^{(O(1))}(n) < 2^n$ $\approx\Rightarrow$ *[All99]*
- $d = o(\log \log n)$, $a = \text{poly-log}(n)$, $s = n^{O(1)}$ $\Rightarrow$ *[KP09]*
- $d = O(1)$, $a = n^{o(1)}$, $s = n^{O(1)}$ $\Rightarrow$ *[JS12]*
- **Tradeoff between** d**,** a**,** s

Theorem (Main Result)

Lower bound for Perm *on threshold circuits with depth* d*, advice* a*, size* s *s.t.*

- $d = O(1)$, $a = \text{poly-log}(n)$, s s.t. $s^{(O(1))}(n) < 2^n$ $\approx\Rightarrow$ *[All99]*
- $d = o(\log\log n)$, $a = \text{poly-log}(n)$, $s = n^{O(1)}$ $\Rightarrow$ *[KP09]*
- $d = O(1)$, $a = n^{o(1)}$, $s = n^{O(1)}$ $\Rightarrow$ *[JS12]*
- **Tradeoff between** d**,** a**,** s

Compare to Known Results, Conjectures

Theorem (Main Result)

Lower bound for Perm *on threshold circuits with depth d, advice a, size s s.t.*

- $d = O(1)$, $a = \text{poly-log}(n)$, s s.t. $s^{(O(1))}(n) < 2^n$ $\approx\Rightarrow$ [All99]
- $d = o(\log\log n)$, $a = \text{poly-log}(n)$, $s = n^{O(1)}$ $\Rightarrow$ [KP09]
- $d = O(1)$, $a = n^{o(1)}$, $s = n^{O(1)}$ $\Rightarrow$ [JS12]
- **Tradeoff between** d**,** a**,** s

Compare to Known Results, Conjectures

- Ryser's formula for Perm: $O(n \cdot 2^n)$ time

Theorem (Main Result)

Lower bound for Perm *on threshold circuits with depth* d*, advice* a*, size* s *s.t.*

- $d = O(1)$, $a = \text{poly-log}(n)$, s s.t. $s^{(O(1))}(n) < 2^n$ $\approx\Rightarrow$ *[All99]*
- $d = o(\log\log n)$, $a = \text{poly-log}(n)$, $s = n^{O(1)}$ $\Rightarrow$ *[KP09]*
- $d = O(1)$, $a = n^{o(1)}$, $s = n^{O(1)}$ $\Rightarrow$ *[JS12]*
- **Tradeoff between** d**,** a**,** s

Compare to Known Results, Conjectures

- Ryser's formula for Perm: $O(n \cdot 2^n)$ time
- Parity $\not\subseteq$ non-uniform AC^0 size $2^{n^{o(1)}}$ [Hås87]

Theorem (Main Result)

Lower bound for Perm *on threshold circuits with depth* d*, advice* a*, size* s *s.t.*

- $d = O(1)$, $a = \text{poly-log}(n)$, s s.t. $s^{(O(1))}(n) < 2^n$ $\approx\Rightarrow$ *[All99]*
- $d = o(\log \log n)$, $a = \text{poly-log}(n)$, $s = n^{O(1)}$ $\Rightarrow$ *[KP09]*
- $d = O(1)$, $a = n^{o(1)}$, $s = n^{O(1)}$ $\Rightarrow$ *[JS12]*
- **Tradeoff between** d, a, s

Compare to Known Results, Conjectures

- Ryser's formula for Perm: $O(n \cdot 2^n)$ time
- Parity $\not\subseteq$ non-uniform AC^0 size $2^{n^{o(1)}}$ [Hås87]
- NEXP $\not\subseteq$ non-uniform ACC^0 poly size [Wil11]

Theorem (Main Result)

Lower bound for Perm *on threshold circuits with depth* d*, advice* a*, size* s *s.t.*

- $d = O(1)$, $a = \text{poly-log}(n)$, s s.t. $s^{(O(1))}(n) < 2^n$ $\approx\Rightarrow$ *[All99]*
- $d = o(\log\log n)$, $a = \text{poly-log}(n)$, $s = n^{O(1)}$ $\Rightarrow$ *[KP09]*
- $d = O(1)$, $a = n^{o(1)}$, $s = n^{O(1)}$ $\Rightarrow$ *[JS12]*
- **Tradeoff between** d, a, s

Compare to Known Results, Conjectures

- Ryser's formula for Perm: $O(n \cdot 2^n)$ time
- Parity $\not\subseteq$ non-uniform AC^0 size $2^{n^{o(1)}}$ [Hås87]
- NEXP $\not\subseteq$ non-uniform ACC^0 poly size [Wil11]
- Conjecture: NP, Perm $\not\subseteq$ SIZE$(2^{n^{o(1)}})$

Proofs

Theorem (Main Result)

Lower bound for Perm *on threshold circuits with depth* d, *advice* a, *size* s *s.t.*

- $d = O(1)$, $a = \text{poly-log}(n)$, s *s.t.* $s^{(O(1))}(n) < 2^n$
- $d = o(\log \log n)$, $a = \text{poly-log}(n)$, $s = n^{O(1)}$
- $d = O(1)$, $a = n^{o(1)}$, $s = n^{O(1)}$
- *Tradeoff between* d, a, s

Theorem (Main Result)

Lower bound for Perm *on threshold circuits with depth* d*, advice* a*, size* s *s.t.*

- $d = O(1)$, $a = \text{poly-log}(n)$, s *s.t.* $s^{(O(1))}(n) < 2^n$
- $d = o(\log\log n)$, $a = \text{poly-log}(n)$, $s = n^{O(1)}$
- $d = O(1)$, $a = n^{o(1)}$, $s = n^{O(1)}$
- *Tradeoff between* d, a, s

Theorem

$\mathrm{Perm} \notin \mathsf{TC}$ *circuits of depth* $O(1)$*, advice* $n^{o(1)}$*, and poly size.*

Theorem

$\mathrm{Perm} \notin$ *TC circuits of depth $O(1)$, advice $n^{o(1)}$, and poly size.*

Theorem

Perm $\notin$ *TC circuits of depth* $O(1)$*, advice* $n^{o(1)}$*, and poly size.*

Proof

Theorem

$\mathrm{Perm} \notin$ *TC circuits of depth $O(1)$, advice $n^{o(1)}$, and poly size.*

Proof

- $\mathrm{P}^{\mathrm{Perm}} \not\subseteq \mathsf{SIZE}(n^k)$

Theorem

$\mathrm{Perm} \notin$ *TC circuits of depth $O(1)$, advice $n^{o(1)}$, and poly size.*

Proof

- $\mathrm{P}^{\mathrm{Perm}} \not\subseteq \mathsf{SIZE}(n^k)$
- theorem false $\Rightarrow \mathrm{P}^{\mathrm{Perm}} \subseteq \mathrm{TC}^0$ with $n^{o(1)}$ advice

Theorem

$\mathrm{Perm} \notin$ *TC circuits of depth* $O(1)$*, advice* $n^{o(1)}$*, and poly size.*

Proof

- $\mathrm{P}^{\mathrm{Perm}} \not\subseteq \mathsf{SIZE}(n^k)$
- theorem false $\Rightarrow \mathrm{P}^{\mathrm{Perm}} \subseteq \mathrm{TC}^0$ with $n^{o(1)}$ advice
- theorem false $\Rightarrow \mathrm{P}^{\mathrm{Perm}} \subseteq \mathsf{SIZE}(O(n))$

Theorem

$\mathrm{Perm} \notin$ *TC circuits of depth* $O(1)$*, advice* $n^{o(1)}$*, and poly size.*

Proof

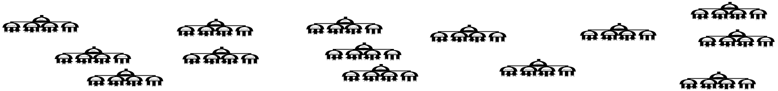
- $\mathrm{P}^{\mathrm{Perm}} \not\subseteq \mathsf{SIZE}(n^k)$
- theorem false $\Rightarrow \mathrm{P}^{\mathrm{Perm}} \subseteq \mathrm{TC}^0$ with $n^{o(1)}$ advice
- theorem false $\Rightarrow \mathrm{P}^{\mathrm{Perm}} \subseteq \mathsf{SIZE}(O(n))$

Theorem

Perm $\notin$ *TC circuits of depth* $O(1)$*, advice* $n^{o(1)}$*, and poly size.*

Proof

- $\mathrm{P}^{\mathrm{Perm}} \not\subseteq \mathsf{SIZE}(n^k)$
- theorem false $\Rightarrow \mathrm{P}^{\mathrm{Perm}} \subseteq \mathrm{TC}^0$ with $n^{o(1)}$ advice
- theorem false $\Rightarrow \mathrm{P}^{\mathrm{Perm}} \subseteq \mathsf{SIZE}(O(n))$

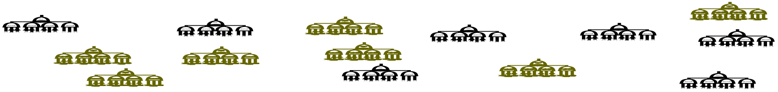


Theorem

$\mathrm{Perm} \notin$ *TC circuits of depth $O(1)$, advice $n^{o(1)}$, and poly size.*

Proof

- $\mathrm{P}^{\mathrm{Perm}} \not\subseteq \mathsf{SIZE}(n^k)$
- theorem false $\Rightarrow \mathrm{P}^{\mathrm{Perm}} \subseteq \mathrm{TC}^0$ with $n^{o(1)}$ advice
- theorem false $\Rightarrow \mathrm{P}^{\mathrm{Perm}} \subseteq \mathsf{SIZE}(O(n))$

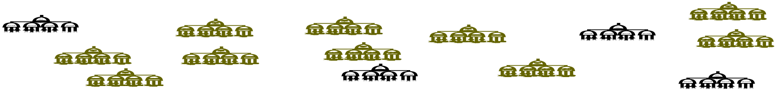


Theorem

$\mathrm{Perm} \notin$ *TC circuits of depth $O(1)$, advice $n^{o(1)}$, and poly size.*

Proof

- $\mathrm{P}^{\mathrm{Perm}} \not\subseteq \mathsf{SIZE}(n^k)$
- theorem false $\Rightarrow \mathrm{P}^{\mathrm{Perm}} \subseteq \mathrm{TC}^0$ with $n^{o(1)}$ advice
- theorem false $\Rightarrow \mathrm{P}^{\mathrm{Perm}} \subseteq \mathsf{SIZE}(O(n))$

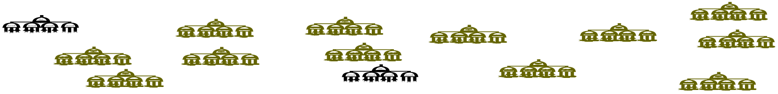


Theorem

$\mathrm{Perm} \notin$ *TC circuits of depth $O(1)$, advice $n^{o(1)}$, and poly size.*

Proof

- $\mathrm{P}^{\mathrm{Perm}} \not\subseteq \mathsf{SIZE}(n^k)$
- theorem false $\Rightarrow \mathrm{P}^{\mathrm{Perm}} \subseteq \mathrm{TC}^0$ with $n^{o(1)}$ advice
- theorem false $\Rightarrow \mathrm{P}^{\mathrm{Perm}} \subseteq \mathsf{SIZE}(O(n))$

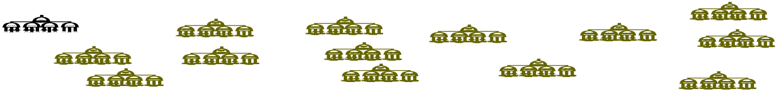


Theorem

Perm $\notin$ *TC circuits of depth* $O(1)$*, advice* $n^{o(1)}$*, and poly size.*

Proof

- $\mathrm{P}^{\mathrm{Perm}} \not\subseteq \mathsf{SIZE}(n^k)$
- theorem false $\Rightarrow \mathrm{P}^{\mathrm{Perm}} \subseteq \mathrm{TC}^0$ with $n^{o(1)}$ advice
- theorem false $\Rightarrow \mathrm{P}^{\mathrm{Perm}} \subseteq \mathsf{SIZE}(O(n))$

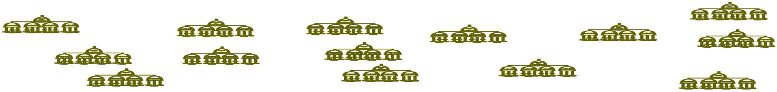


Theorem

$\mathrm{Perm} \notin$ *TC circuits of depth* $O(1)$*, advice* $n^{o(1)}$*, and poly size.*

Proof

- $\mathrm{P}^{\mathrm{Perm}} \not\subseteq \mathsf{SIZE}(n^k)$
- theorem false $\Rightarrow \mathrm{P}^{\mathrm{Perm}} \subseteq \mathrm{TC}^0$ with $n^{o(1)}$ advice
- theorem false $\Rightarrow \mathrm{P}^{\mathrm{Perm}} \subseteq \mathsf{SIZE}(O(n))$



Theorem

$\mathrm{Perm} \notin$ *TC circuits of depth $O(1)$, advice $n^{o(1)}$, and poly size.*

Proof

- $\mathrm{P}^{\mathrm{Perm}} \not\subseteq \mathsf{SIZE}(n^k)$
- theorem false $\Rightarrow \mathrm{P}^{\mathrm{Perm}} \subseteq \mathrm{TC}^0$ with $n^{o(1)}$ advice
- theorem false $\Rightarrow \mathrm{P}^{\mathrm{Perm}} \subseteq \mathsf{SIZE}(O(n))$

Theorem

$\mathrm{Perm} \notin$ *TC circuits of depth $O(1)$, advice $n^{o(1)}$, and poly size.*

Proof

- $\mathrm{P}^{\mathrm{Perm}} \not\subseteq \mathsf{SIZE}(n^k)$
- theorem false $\Rightarrow \mathrm{P}^{\mathrm{Perm}} \subseteq \mathrm{TC}^0$ with $n^{o(1)}$ advice
- theorem false $\Rightarrow \mathrm{P}^{\mathrm{Perm}} \subseteq \mathsf{SIZE}(O(n))$

theorem false:

Theorem

$\mathrm{Perm} \notin$ *TC circuits of depth $O(1)$, advice $n^{o(1)}$, and poly size.*

Proof

- $\mathrm{P}^{\mathrm{Perm}} \not\subseteq \mathsf{SIZE}(n^k)$
- theorem false $\Rightarrow \mathrm{P}^{\mathrm{Perm}} \subseteq \mathrm{TC}^0$ with $n^{o(1)}$ advice
- theorem false $\Rightarrow \mathrm{P}^{\mathrm{Perm}} \subseteq \mathsf{SIZE}(O(n))$

theorem false:

$\mathrm{P}^{\mathrm{Perm}} \quad \subseteq \mathrm{P}^{\mathrm{TC}^0} + n^{o(1)}$ advice

Theorem

$\mathrm{Perm} \notin$ *TC circuits of depth $O(1)$, advice $n^{o(1)}$, and poly size.*

Proof

- $\mathrm{P}^{\mathrm{Perm}} \not\subseteq \mathsf{SIZE}(n^k)$
- theorem false $\Rightarrow \mathrm{P}^{\mathrm{Perm}} \subseteq \mathrm{TC}^0$ with $n^{o(1)}$ advice
- theorem false $\Rightarrow \mathrm{P}^{\mathrm{Perm}} \subseteq \mathsf{SIZE}(O(n))$

theorem false:

$\mathrm{P}^{\mathrm{Perm}} \quad \subseteq \mathrm{P}^{\mathrm{TC}^0} + n^{o(1)}$ advice $\quad \subseteq \mathrm{P} + n^{o(1)}$ advice

Theorem

$\mathrm{Perm} \notin$ *TC circuits of depth $O(1)$, advice $n^{o(1)}$, and poly size.*

Proof

- $\mathrm{P}^{\mathrm{Perm}} \not\subseteq \mathsf{SIZE}(n^k)$
- theorem false $\Rightarrow \mathrm{P}^{\mathrm{Perm}} \subseteq \mathrm{TC}^0$ with $n^{o(1)}$ advice
- theorem false $\Rightarrow \mathrm{P}^{\mathrm{Perm}} \subseteq \mathsf{SIZE}(O(n))$

theorem false:

$\mathrm{P}^{\mathrm{Perm}} \subseteq \mathrm{P}^{\mathrm{TC}^0} + n^{o(1)}$ advice $\subseteq \mathrm{P} + n^{o(1)}$ advice

$\subseteq \mathrm{TC}^0 + n^{o(1)}$ advice

Theorem

$\mathrm{Perm} \notin$ *TC circuits of depth $O(1)$, advice $n^{o(1)}$, and poly size.*

Proof

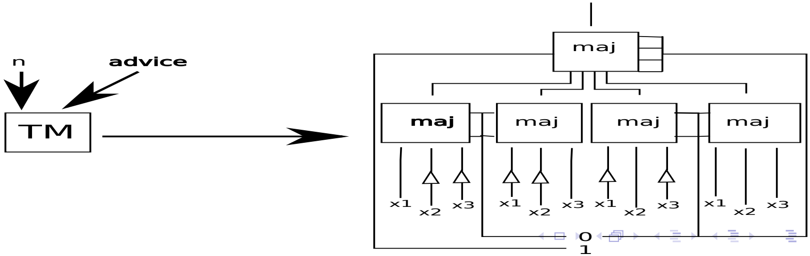
- $\mathrm{P}^{\mathrm{Perm}} \not\subseteq \mathsf{SIZE}(n^k)$
- theorem false $\Rightarrow \mathrm{P}^{\mathrm{Perm}} \subseteq \mathrm{TC}^0$ with $n^{o(1)}$ advice
- theorem false $\Rightarrow \mathrm{P}^{\mathrm{Perm}} \subseteq \mathsf{SIZE}(O(n))$

Theorem

Perm $\notin$ *TC circuits of depth $O(1)$, advice $n^{o(1)}$, and poly size.*

Proof

- $\mathrm{P}^{\mathrm{Perm}} \not\subseteq \mathsf{SIZE}(n^k)$
- theorem false $\Rightarrow \mathrm{P}^{\mathrm{Perm}} \subseteq \mathrm{TC}^0$ with $n^{o(1)}$ advice
- theorem false $\Rightarrow \mathrm{P}^{\mathrm{Perm}} \subseteq \mathsf{SIZE}(O(n))$

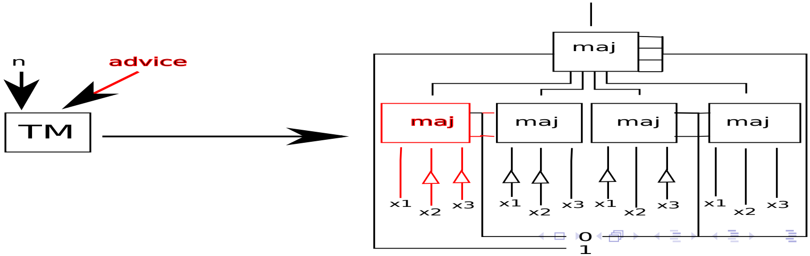


Theorem

$\mathrm{Perm} \notin$ *TC circuits of depth $O(1)$, advice $n^{o(1)}$, and poly size.*

Proof

- $\mathrm{P}^{\mathrm{Perm}} \not\subseteq \mathsf{SIZE}(n^k)$
- theorem false $\Rightarrow \mathrm{P}^{\mathrm{Perm}} \subseteq \mathrm{TC}^0$ with $n^{o(1)}$ advice
- theorem false $\Rightarrow \mathrm{P}^{\mathrm{Perm}} \subseteq \mathsf{SIZE}(O(n))$

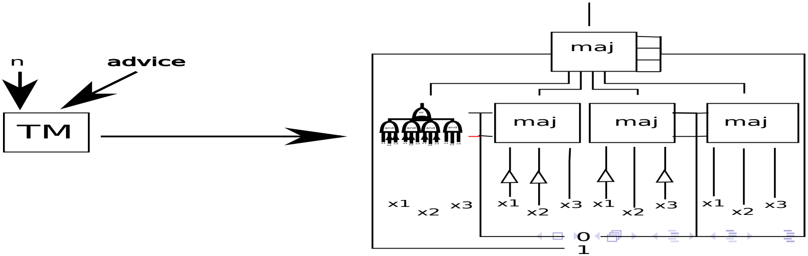


Theorem

Perm $\notin$ *TC circuits of depth $O(1)$, advice $n^{o(1)}$, and poly size.*

Proof

- $\mathrm{P}^{\mathrm{Perm}} \not\subseteq \mathsf{SIZE}(n^k)$
- theorem false $\Rightarrow \mathrm{P}^{\mathrm{Perm}} \subseteq \mathrm{TC}^0$ with $n^{o(1)}$ advice
- theorem false $\Rightarrow \mathrm{P}^{\mathrm{Perm}} \subseteq \mathsf{SIZE}(O(n))$

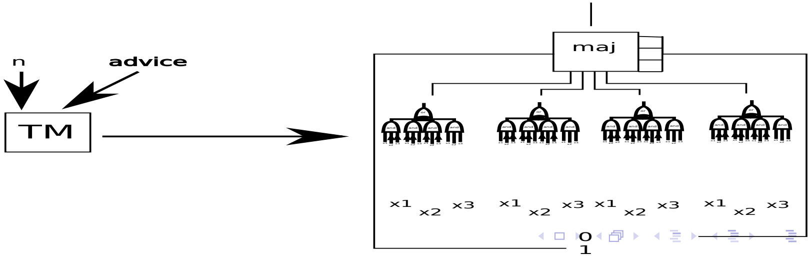


Theorem

Perm $\notin$ *TC circuits of depth $O(1)$, advice $n^{o(1)}$, and poly size.*

Proof

- $\mathrm{P}^{\mathrm{Perm}} \not\subseteq \mathsf{SIZE}(n^k)$
- theorem false $\Rightarrow \mathrm{P}^{\mathrm{Perm}} \subseteq \mathrm{TC}^0$ with $n^{o(1)}$ advice
- theorem false $\Rightarrow \mathrm{P}^{\mathrm{Perm}} \subseteq \mathsf{SIZE}(O(n))$

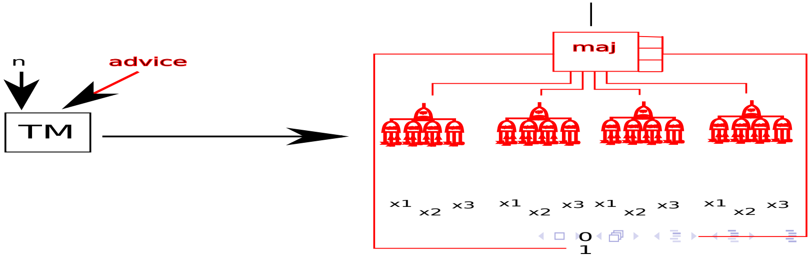


Theorem

Perm $\notin$ *TC circuits of depth* $O(1)$*, advice* $n^{o(1)}$*, and poly size.*

Proof

- $\mathrm{P}^{\mathrm{Perm}} \not\subseteq \mathsf{SIZE}(n^k)$
- theorem false $\Rightarrow \mathrm{P}^{\mathrm{Perm}} \subseteq \mathrm{TC}^0$ with $n^{o(1)}$ advice
- theorem false $\Rightarrow \mathrm{P}^{\mathrm{Perm}} \subseteq \mathsf{SIZE}(O(n))$

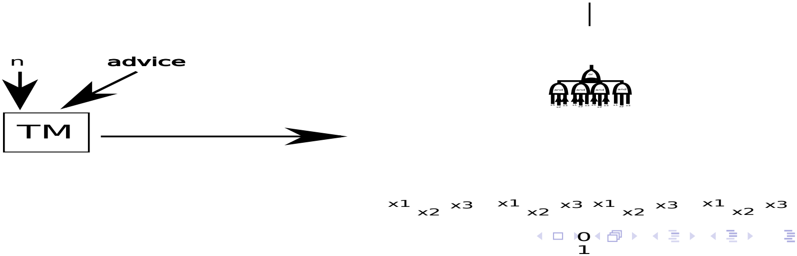


Theorem

$\mathrm{Perm} \notin$ *TC circuits of depth $O(1)$, advice $n^{o(1)}$, and poly size.*

Proof

- $\mathrm{P}^{\mathrm{Perm}} \not\subseteq \mathsf{SIZE}(n^k)$
- theorem false $\Rightarrow \mathrm{P}^{\mathrm{Perm}} \subseteq \mathrm{TC}^0$ with $n^{o(1)}$ advice
- theorem false $\Rightarrow \mathrm{P}^{\mathrm{Perm}} \subseteq \mathsf{SIZE}(O(n))$



Theorem

$\mathrm{Perm} \notin$ *TC circuits of depth $O(1)$, advice $n^{o(1)}$, and poly size.*

Proof

- $\mathrm{P}^{\mathrm{Perm}} \not\subseteq \mathsf{SIZE}(n^k)$
- theorem false $\Rightarrow \mathrm{P}^{\mathrm{Perm}} \subseteq \mathrm{TC}^0$ with $n^{o(1)}$ advice
- theorem false $\Rightarrow \mathrm{P}^{\mathrm{Perm}} \subseteq \mathsf{SIZE}(O(n))$

Level 1: PP question size $n^{o(1)} + \log(\mathrm{poly}(n))$

Theorem

$\mathrm{Perm} \notin$ *TC circuits of depth* $O(1)$*, advice* $n^{o(1)}$*, and poly size.*

Proof

- $\mathrm{P}^{\mathrm{Perm}} \not\subseteq \mathsf{SIZE}(n^k)$
- theorem false $\Rightarrow \mathrm{P}^{\mathrm{Perm}} \subseteq \mathrm{TC}^0$ with $n^{o(1)}$ advice
- theorem false $\Rightarrow \mathrm{P}^{\mathrm{Perm}} \subseteq \mathsf{SIZE}(O(n))$

$$\text{Level 1: PP question size } n^{o(1)} + \log(\mathrm{poly}(n))$$
$$\Rightarrow (n^{o(1)})^c = n^{o(1)} \text{ size circuits}$$

Theorem

Perm $\notin$ TC circuits of depth $O(1)$, advice $n^{o(1)}$, and poly size.

Proof

- $\mathrm{P}^{\mathrm{Perm}} \not\subseteq \mathsf{SIZE}(n^k)$
- theorem false $\Rightarrow \mathrm{P}^{\mathrm{Perm}} \subseteq \mathrm{TC}^0$ with $n^{o(1)}$ advice
- theorem false $\Rightarrow \mathrm{P}^{\mathrm{Perm}} \subseteq \mathsf{SIZE}(O(n))$

Level 2: PP question size $n^{o(1)} + \log(\mathrm{poly}(n) \cdot n^{o(1)})$

Theorem

$\mathrm{Perm} \notin$ *TC circuits of depth $O(1)$, advice $n^{o(1)}$, and poly size.*

Proof

- $\mathrm{P}^{\mathrm{Perm}} \not\subseteq \mathsf{SIZE}(n^k)$
- theorem false $\Rightarrow \mathrm{P}^{\mathrm{Perm}} \subseteq \mathrm{TC}^0$ with $n^{o(1)}$ advice
- theorem false $\Rightarrow \mathrm{P}^{\mathrm{Perm}} \subseteq \mathsf{SIZE}(O(n))$

Level 2: PP question size $n^{o(1)} + \log(\mathrm{poly}(n) \cdot n^{o(1)})$
$\Rightarrow (n^{o(1)})^c = n^{o(1)}$ size circuits

Theorem

$\mathrm{Perm} \notin$ TC circuits of depth $O(1)$, advice $n^{o(1)}$, and poly size.

Proof

- $\mathrm{P}^{\mathrm{Perm}} \not\subseteq \mathsf{SIZE}(n^k)$
- theorem false $\Rightarrow \mathrm{P}^{\mathrm{Perm}} \subseteq \mathrm{TC}^0$ with $n^{o(1)}$ advice
- theorem false $\Rightarrow \mathrm{P}^{\mathrm{Perm}} \subseteq \mathsf{SIZE}(O(n))$

Level d: $\Rightarrow n^{o(1)}$ size circuit

Theorem

Perm $\notin$ *TC circuits of depth* $O(1)$*, advice* $n^{o(1)}$*, and poly size.*

Proof

- $\mathrm{P}^{\mathrm{Perm}} \not\subseteq \mathsf{SIZE}(n^k)$
- theorem false $\Rightarrow \mathrm{P}^{\mathrm{Perm}} \subseteq \mathrm{TC}^0$ with $n^{o(1)}$ advice
- theorem false $\Rightarrow \mathrm{P}^{\mathrm{Perm}} \subseteq \mathsf{SIZE}(O(n))$

Level d: $\Rightarrow n^{o(1)}$ size circuit
(size $O(n)$ really)

Theorem

$\mathrm{Perm} \notin$ *TC circuits of depth* $O(1)$*, advice* $n^{o(1)}$*, and poly size.*

Theorem

Perm $\notin$ *TC circuits of depth* $O(1)$*, advice* $n^{o(1)}$*, and poly size.*

Proof of [CK12]

Theorem

Perm $\notin$ *TC circuits of depth* $O(1)$*, advice* $n^{o(1)}$*, and poly size.*

Proof of [CK12]

- TH-time-depth$(n^{k+1}, d) \not\subseteq$ TH-time-depth$(n^k, d) + o(n)$ advice

Theorem

$\mathrm{Perm} \notin$ *TC circuits of depth $O(1)$, advice $n^{o(1)}$, and poly size.*

Proof of [CK12]

- TH-time-depth$(n^{k+1}, d) \not\subseteq$ TH-time-depth$(n^k, d) + o(n)$ advice
- P has TC^0 size n^k, depth d, advice $n^{o(1)} \Rightarrow$ TH-time-depth$(n^{k+1}, d) \not\subseteq \mathrm{P} + n^{o(1)}$ advice

Theorem

Perm $\notin$ *TC circuits of depth* $O(1)$*, advice* $n^{o(1)}$*, and poly size.*

Proof of [CK12]

- TH-time-depth$(n^{k+1}, d) \not\subseteq$
  TH-time-depth$(n^k, d) + o(n)$ advice
- P has TC^0 size n^k, depth d, advice $n^{o(1)} \Rightarrow$
  TH-time-depth$(n^{k+1}, d) \not\subseteq$ P $+ n^{o(1)}$ advice
- theorem false: TH-time-depth$(n^{k+1}, d) \subseteq$ P $+ n^{o(1)}$ advice

What Next?

Extensions

- Poly advice

Extensions

- Poly advice (obstacles - natural pfs [RR97], relativization [AW09])

Extensions

- Poly advice (obstacles - natural pfs [RR97], relativization [AW09])
- Average-case, almost-everywhere hardness

Extensions

- Poly advice (obstacles - natural pfs [RR97], relativization [AW09])
- Average-case, almost-everywhere hardness
- ...

Extensions

- Poly advice (obstacles - natural pfs [RR97], relativization [AW09])
- Average-case, almost-everywhere hardness
- ...
- Make use nice properties of permanent

Extensions

- Poly advice (obstacles - natural pfs [RR97], relativization [AW09])
- Average-case, almost-everywhere hardness
- ...
- Make use nice properties of permanent
  - low-degree poly, downward/random self-reduction, ...

Thank you.

Slides online at http://www.kinnejeff.com

References I

Eric Allender.
The permanent requires large uniform threshold circuits.
Chicago Journal of Theoretical Computer Science, 1999.

Scott Aaronson and Dieter van Melkebeek.
On circuit lower bounds from derandomization.
Theory of Computing, 7(1):177–184, 2011.

Scott Aaronson and Avi Wigderson.
Algebrization: A new barrier in complexity theory.
ACM Transactions on Computation Theory, 1(1):1–54, 2009.

References II

Ruiwen Chen and Valentine Kabanets.
Lower bounds against weakly uniform circuits.
In Proceedings of the Annual International Computing and Combinatorics Conference (COCOON), pages 408–419, 2012.

Johan Håstad.
Computational Limitations of Small-Depth Circuits.
MIT Press, Cambridge, MA, USA, 1987.

Russell Impagliazzo and Avi Wigderson.
P = BPP if E requires exponential circuits: Derandomizing the XOR lemma.
In Proceedings of the ACM Symposium on Theory of Computing (STOC), pages 220–229, 1997.

References III

Maurice Jansen and Rahul Santhanam.
Marginal hitting sets imply super-polynomial lower bounds for permanent.
In Innovations in Theoretical Computer Science, 2012.

Valentine Kabanets and Russell Impagliazzo.
Derandomizing polynomial identity tests means proving circuit lower bounds.
Computational Complexity, 13(1/2):1–46, 2004.

References IV

Pascal Koiran and Sylvain Perifel.
A superpolynomial lower bound on the size of uniform non-constant-depth threshold circuits for the permanent.
In Proceedings of the IEEE Conference on Computational Complexity (CCC), pages 35–40, 2009.

Moni Naor, Omer Reingold, and Alon Rosen.
Pseudorandom functions and factoring.
SIAM Journal on Computing, 31(5):1383–1404, 2002.

Alexander A. Razborov and Steven Rudich.
Natural proofs.
Journal of Computer and System Sciences, 55(1):24–35, 1997.

References V

Ryan Williams.
Non-uniform ACC circuit lower bounds.
In Proceedings of the IEEE Conference on Computational Complexity (CCC), pages 115–125, 2011.