Average case lower bounds for threshold circuits

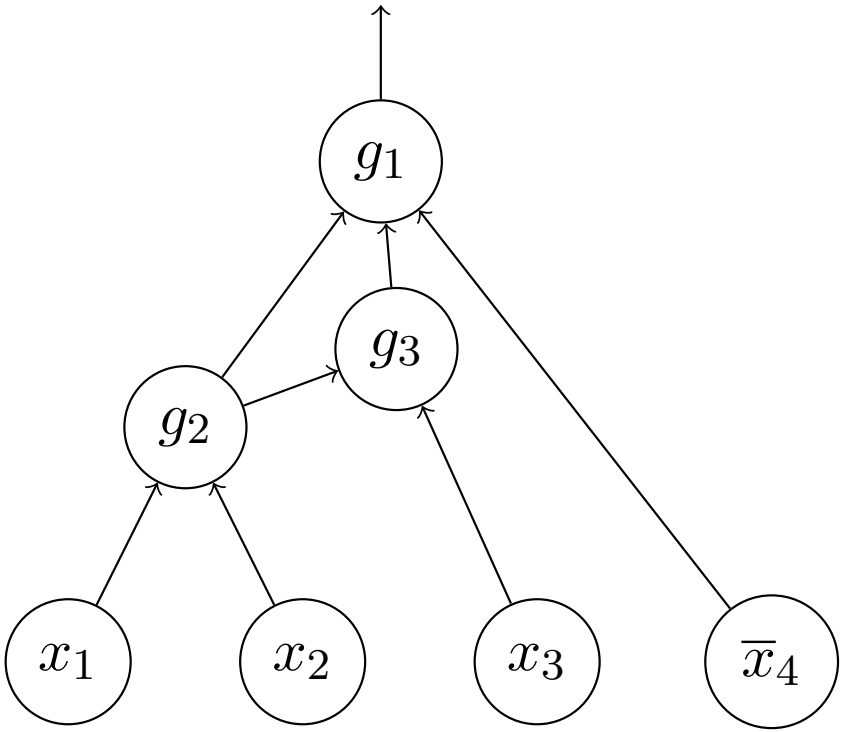
Ruiwen Chen, Rahul Santhanam and Srikanth Srinivasan

University of Oxford and Department of Mathematics, IIT Bombay

CCC 2016

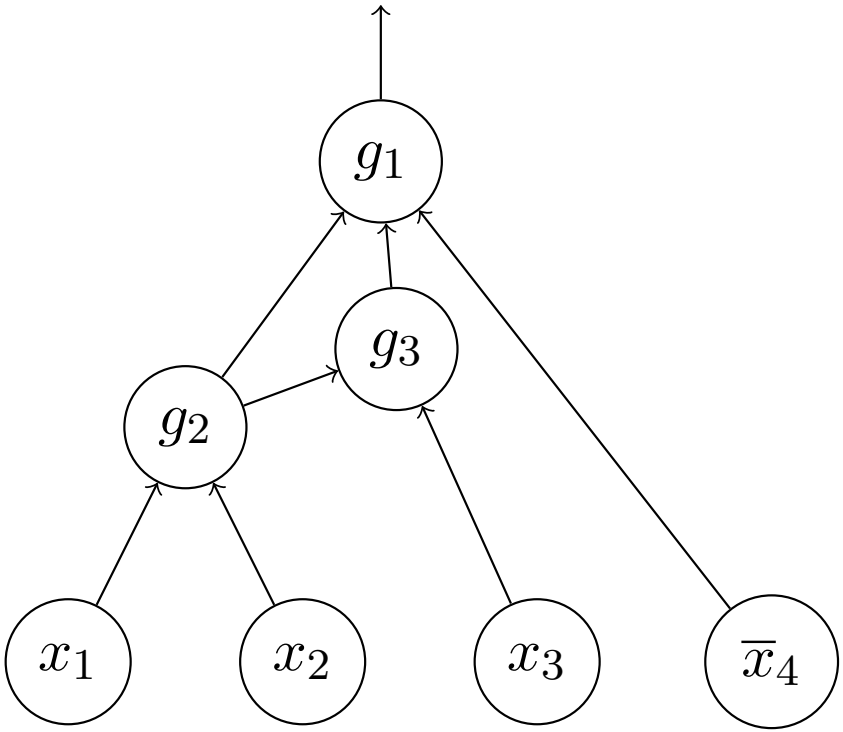
Boolean Circuits

- Circuit computing function $f : \{0,1\}^n \to \{0,1\}$.
- Computation proceeds through "simple" operations.



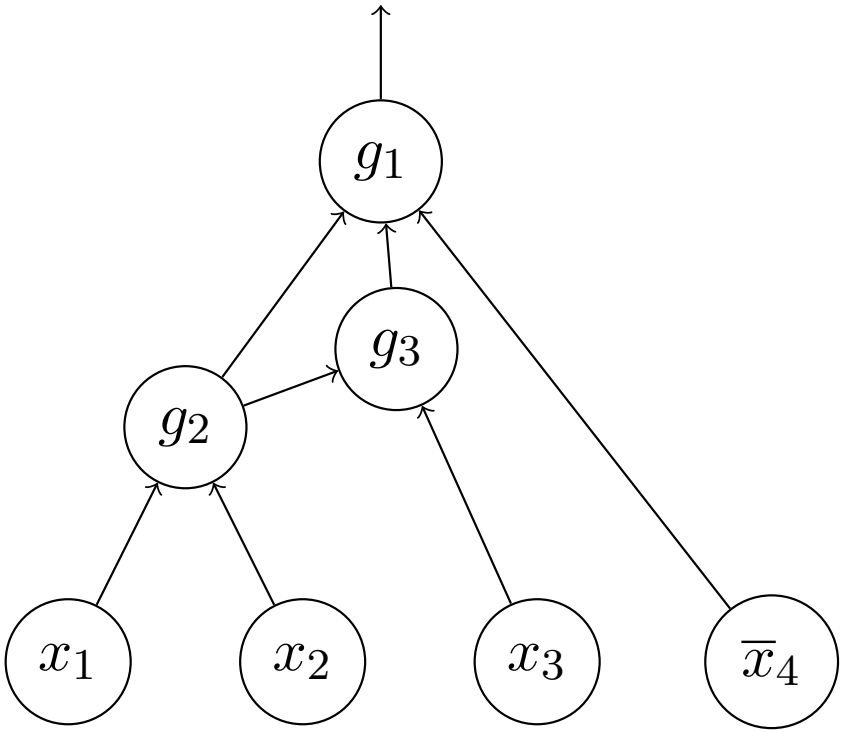
Boolean Circuits

- Circuit computing function $f : \{0,1\}^n \to \{0,1\}$.
- Computation proceeds through "simple" operations.
- $g_i \in$ "basic" operations.



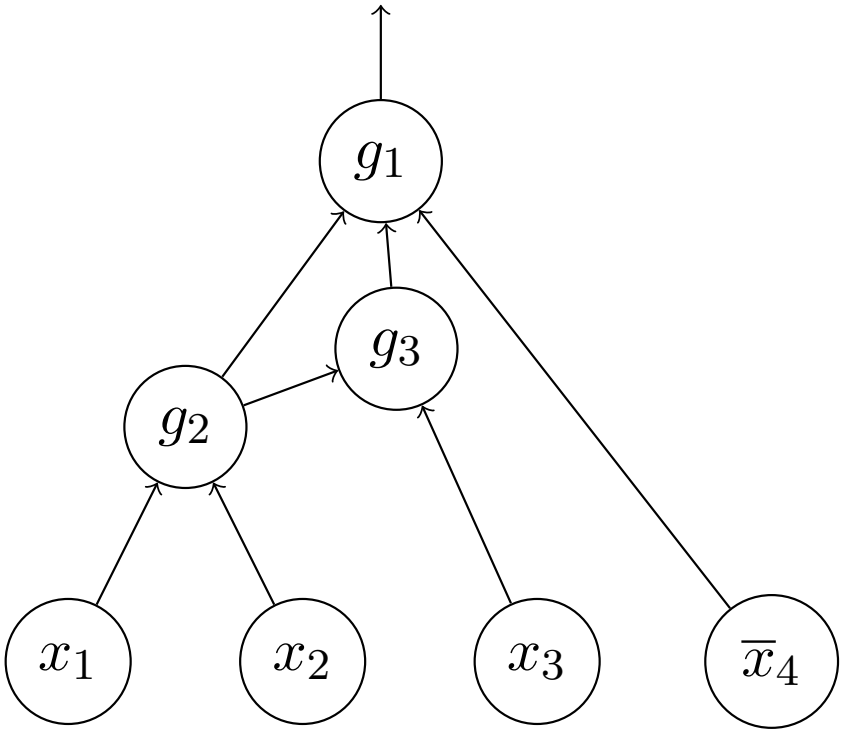
Boolean Circuits

- Circuit computing function $f : \{0,1\}^n \to \{0,1\}$.
- Computation proceeds through "simple" operations.
- $g_i \in$ "basic" operations.
- Designated output gate computes function f.



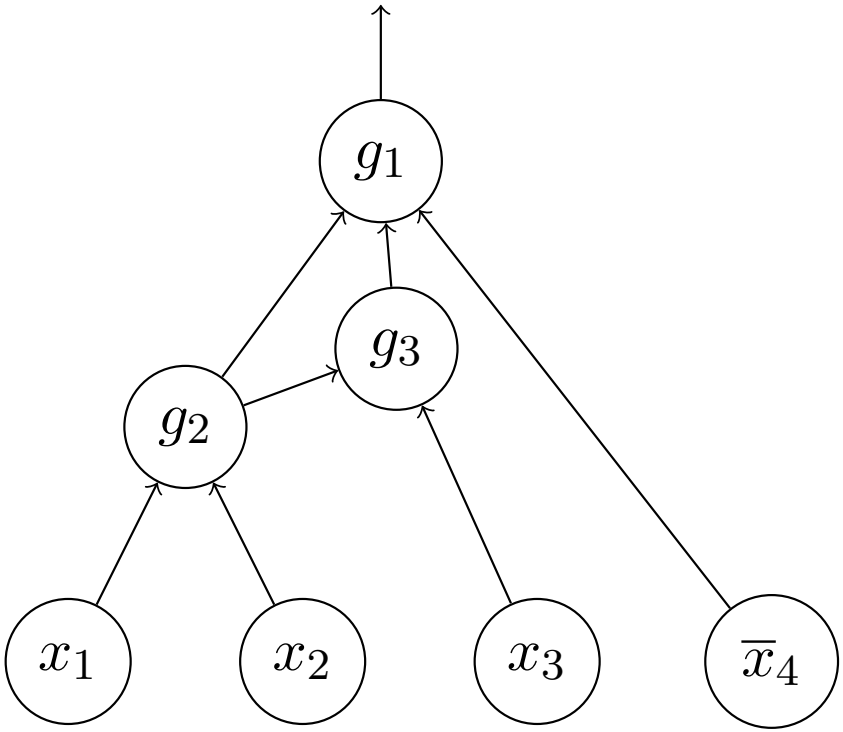
Boolean Circuits

- Size s of the circuit: time taken by algorithm.



Boolean Circuits

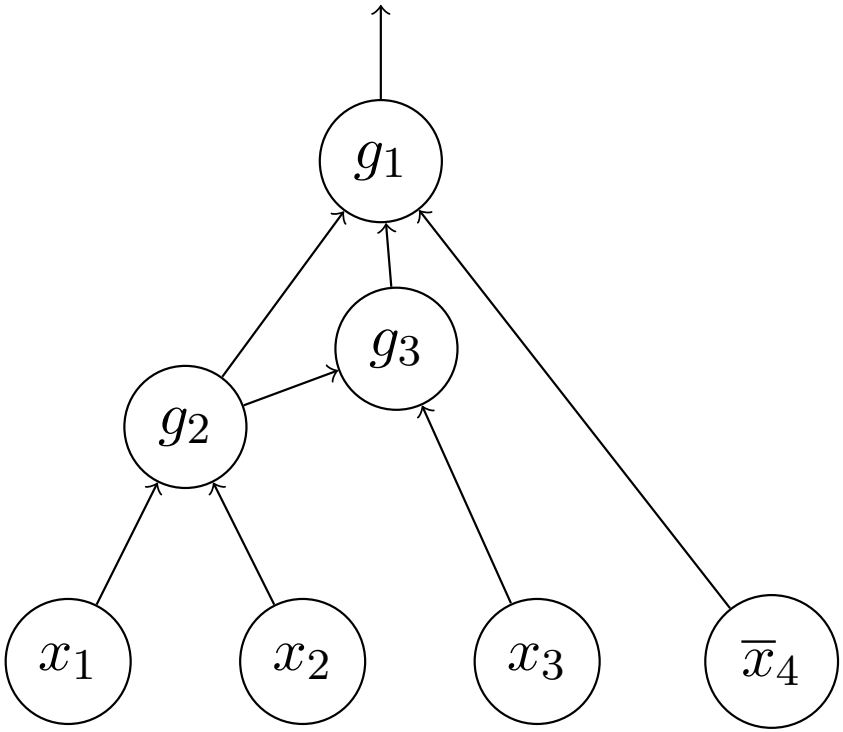
- Size s of the circuit: time taken by algorithm.
- Could be # edges/wires or # gates.



wires $= 8$, # gates $= 3$

Boolean Circuits

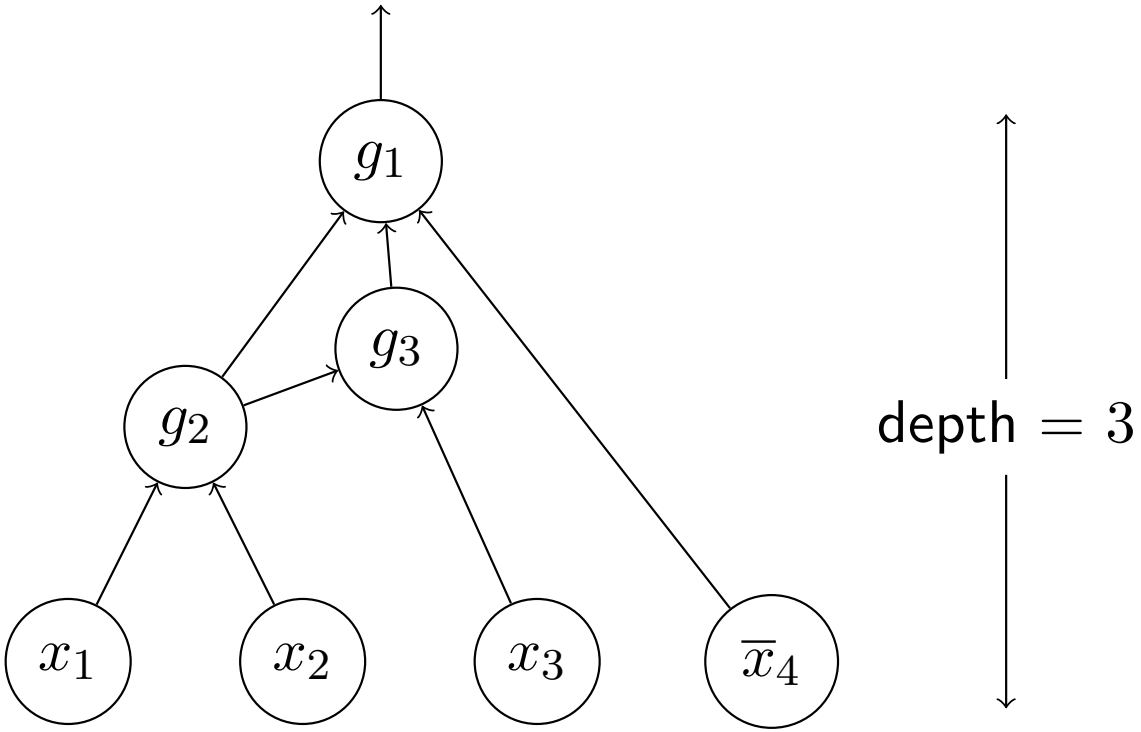
- Size s of the circuit: time taken by algorithm.
- Could be # edges/wires or # gates.
- # wires $\leq (n+$ # gates$)\cdot$ # gates.



wires $= 8$, # gates $= 3$

Boolean Circuits

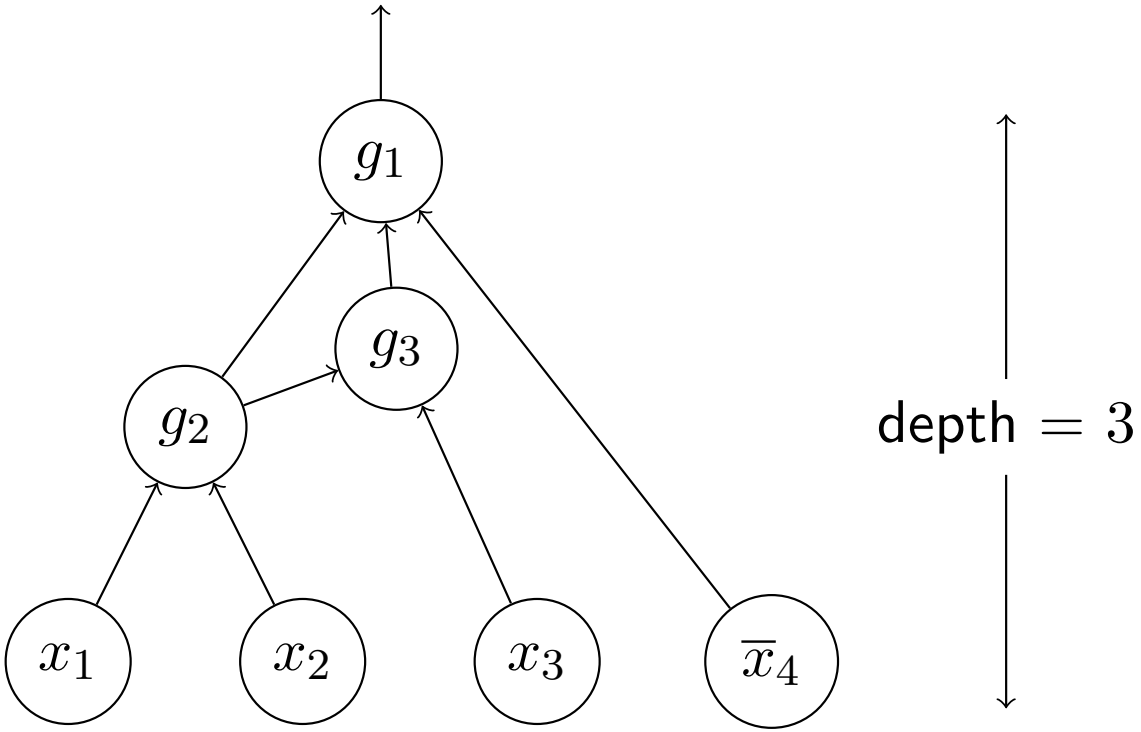
- Size s of the circuit: time taken by algorithm.
- Could be # edges/wires or # gates.
- # wires $\leq (n+$ # gates$)\cdot$ # gates.
- Depth d of the circuit: parallelism of the algorithm.



wires $= 8$, # gates $= 3$

Boolean Circuits

- Size s of the circuit: time taken by algorithm.
- Could be # edges/wires or # gates.
- # wires $\leq (n+$ # gates$)\cdot$ # gates.
- Depth d of the circuit: parallelism of the algorithm.
- $s = s(n)$, $d = O(1)$.



wires $= 8$, # gates $= 3$

Threshold circuits

- A threshold operation: $g(x) = 1$ iff $\sum_i w_i x_i \geq \theta$ for $w_i, \theta \in \mathbb{R}$.

Threshold circuits

- A threshold operation: $g(x) = 1$ iff $\sum_i w_i x_i \geq \theta$ for $w_i, \theta \in \mathbb{R}$. Some examples:
- OR function: $\mathrm{OR}(x) = 1$ iff $\sum_i x_i \geq 1$.

Threshold circuits

- A threshold operation: $g(x) = 1$ iff $\sum_i w_i x_i \geq \theta$ for $w_i, \theta \in \mathbb{R}$. Some examples:
- OR function: $\mathrm{OR}(x) = 1$ iff $\sum_i x_i \geq 1$.
- AND function: $\mathrm{AND}(x) = [\![\sum_i x_i \geq n]\!]$.

Threshold circuits

- A threshold operation: $g(x) = 1$ iff $\sum_i w_i x_i \geq \theta$ for $w_i, \theta \in \mathbb{R}$. Some examples:
- OR function: $\mathrm{OR}(x) = 1$ iff $\sum_i x_i \geq 1$.
- AND function: $\mathrm{AND}(x) = [\![\sum_i x_i \geq n]\!]$.
- MAJ function: $\mathrm{MAJ}(x) = [\![\sum_i x_i \geq n/2]\!]$.

Threshold circuits

- A threshold operation: $g(x) = 1$ iff $\sum_i w_i x_i \geq \theta$ for $w_i, \theta \in \mathbb{R}$. Some examples:
- OR function: $\mathrm{OR}(x) = 1$ iff $\sum_i x_i \geq 1$.
- AND function: $\mathrm{AND}(x) = [\![\sum_i x_i \geq n]\!]$.
- MAJ function: $\mathrm{MAJ}(x) = [\![\sum_i x_i \geq n/2]\!]$.
- GEQ function: $\mathrm{GEQ}(x, y) = [\![\sum_i 2^i (x_i - y_i) \geq 0]\!]$.

Threshold circuits

- A threshold operation: $g(x) = 1$ iff $\sum_i w_i x_i \geq \theta$ for $w_i, \theta \in \mathbb{R}$. Some examples:
- OR function: $\mathrm{OR}(x) = 1$ iff $\sum_i x_i \geq 1$.
- AND function: $\mathrm{AND}(x) = [\![\sum_i x_i \geq n]\!]$.
- MAJ function: $\mathrm{MAJ}(x) = [\![\sum_i x_i \geq n/2]\!]$.
- GEQ function: $\mathrm{GEQ}(x, y) = [\![\sum_i 2^i (x_i - y_i) \geq 0]\!]$.
- $\mathrm{TC}^0_g(s, d)$: threshold circuits with s gates and depth d.

Threshold circuits

- A threshold operation: $g(x) = 1$ iff $\sum_i w_i x_i \geq \theta$ for $w_i, \theta \in \mathbb{R}$. Some examples:
- OR function: $\mathrm{OR}(x) = 1$ iff $\sum_i x_i \geq 1$.
- AND function: $\mathrm{AND}(x) = [\![\sum_i x_i \geq n]\!]$.
- MAJ function: $\mathrm{MAJ}(x) = [\![\sum_i x_i \geq n/2]\!]$.
- GEQ function: $\mathrm{GEQ}(x, y) = [\![\sum_i 2^i (x_i - y_i) \geq 0]\!]$.
- $\mathrm{TC}^0_g(s, d)$: threshold circuits with s gates and depth d.
- $\mathrm{TC}^0_w(s, d)$: threshold circuits with s wires and depth d.

Threshold circuits

- A threshold operation: $g(x) = 1$ iff $\sum_i w_i x_i \geq \theta$ for $w_i, \theta \in \mathbb{R}$. Some examples:
- OR function: $\mathrm{OR}(x) = 1$ iff $\sum_i x_i \geq 1$.
- AND function: $\mathrm{AND}(x) = [\![\sum_i x_i \geq n]\!]$.
- MAJ function: $\mathrm{MAJ}(x) = [\![\sum_i x_i \geq n/2]\!]$.
- GEQ function: $\mathrm{GEQ}(x, y) = [\![\sum_i 2^i (x_i - y_i) \geq 0]\!]$.
- $\mathrm{TC}^0_g(s, d)$: threshold circuits with s gates and depth d.
- $\mathrm{TC}^0_w(s, d)$: threshold circuits with s wires and depth d.
- Generalize AC^0 circuits made up of AND and OR gates.

The power of threshold circuits

- $f = \mathrm{PARITY}(x_1, \ldots, x_n) = x_1 \oplus x_2 \oplus \cdots \oplus x_n$.

The power of threshold circuits

- $f = \mathrm{PARITY}(x_1, \ldots, x_n) = x_1 \oplus x_2 \oplus \cdots \oplus x_n$.
- $d \geq 2$: $f \in \mathrm{TC}^0_g(dn^{1/(d-1)}, d)$ (Siu-Roychowdhury-Kailath 1991)

The power of threshold circuits

- $f = \mathrm{PARITY}(x_1, \ldots, x_n) = x_1 \oplus x_2 \oplus \cdots \oplus x_n$.
- $d \geq 2$: $f \in \mathrm{TC}^0_g(dn^{1/(d-1)}, d)$ (Siu-Roychowdhury-Kailath 1991)
- $f \in \mathrm{TC}^0_w(n^{1+\varepsilon^d}, d)$ (Beame-Brisson-Ladner, Paturi-Saks 1991)

The power of threshold circuits

- $f = \mathrm{PARITY}(x_1, \ldots, x_n) = x_1 \oplus x_2 \oplus \cdots \oplus x_n$.
- $d \geq 2$: $f \in \mathrm{TC}^0_g(dn^{1/(d-1)}, d)$ (Siu-Roychowdhury-Kailath 1991)
- $f \in \mathrm{TC}^0_w(n^{1+\varepsilon^d}, d)$ (Beame-Brisson-Ladner, Paturi-Saks 1991)
- Compare with: PARITY does not have AC^0 circuits of subexponential size (Håstad 1986).

Circuit lower bounds

- Problem: Find explicit family of functions (say in NP) that have no TC^0 circuits of poly(n) size.

Circuit lower bounds

- Problem: Find explicit family of functions (say in NP) that have no TC^0 circuits of poly(n) size. Even open for depth 2.

Work on threshold circuits

- Hajnal Maass Pudlák Turan Szegedy 1987
- (Polynomial Approximations) Paturi Saks 1991, Siu Roychowdhury Kailath 1992; Beigel 1994; Aspnes Beigel Furst Rudich 1994, Podolskii 2012
- (Combinatorial restrictions) Impagliazzo Paturi Saks 1991
- (Communication complexity) Goldmann Hastad Razborov 1992; Nisan 1992; Hansen Miltersen 2004; Chattopadhyay Hansen 2005; Lovett, S. 2012
- (Analytic techniques) Gopalan Servedio 2010

State-of-the-art lower bounds

- (Impagliazzo-Paturi-Saks 1991) PARITY not in $\mathrm{TC}^0_g(n^{1/2(d-1)}, d)$ and $\mathrm{TC}^0_w(n^{1+\varepsilon^d}, d)$.

State-of-the-art lower bounds

- (Impagliazzo-Paturi-Saks 1991) PARITY not in $\mathrm{TC}^0_g(n^{1/2(d-1)}, d)$ and $\mathrm{TC}^0_w(n^{1+\varepsilon^d}, d)$.
- (Kane-Williams 2015) Explicit functions not in $\mathrm{TC}^0_g(n^{1.5-o(1)}, 2)$ and $\mathrm{TC}^0_w(n^{2.5-o(1)}, 2)$.

State-of-the-art lower bounds

- (Impagliazzo-Paturi-Saks 1991) PARITY not in $\mathrm{TC}^0_g(n^{1/2(d-1)}, d)$ and $\mathrm{TC}^0_w(n^{1+\varepsilon^d}, d)$.
- (Kane-Williams 2015) Explicit functions not in $\mathrm{TC}^0_g(n^{1.5-o(1)}, 2)$ and $\mathrm{TC}^0_w(n^{2.5-o(1)}, 2)$. Also extends to a special case of depth-3.

Average case lower bounds

- Want to show a function $f : \{0,1\}^n \to \{0,1\}$ hard on *average*.

Average case lower bounds

- Want to show a function $f : \{0,1\}^n \to \{0,1\}$ hard on *average*.
- Trivial to compute f on half the inputs.

Average case lower bounds

- Want to show a function $f : \{0,1\}^n \to \{0,1\}$ hard on *average*.
- Trivial to compute f on half the inputs.
- f has ε-correlation with ckt C if

$$\mathrm{Corr}(C, f) := \Pr_x[C(x) = f(x)] - \frac{1}{2} \leq \varepsilon.$$

Average case lower bounds

- Want to show a function $f : \{0,1\}^n \to \{0,1\}$ hard on *average*.
- Trivial to compute f on half the inputs.
- f has ε-correlation with ckt C if

$$\mathrm{Corr}(C, f) := \Pr_x[C(x) = f(x)] - \frac{1}{2} \leq \varepsilon.$$

- Want to show that f hard on average against $\mathrm{TC}^0(s, d)$.

Why average case lower bounds

- Improves our understanding of limitations of circuits.

Why average case lower bounds

- Improves our understanding of limitations of circuits.
- Lower bounds against slightly stronger circuit classes

Why average case lower bounds

- Improves our understanding of limitations of circuits.
- Lower bounds against slightly stronger circuit classes (E.g - Kane-Williams 2015).

Why average case lower bounds

- Improves our understanding of limitations of circuits.
- Lower bounds against slightly stronger circuit classes (E.g - Kane-Williams 2015).
- Prerequisite for constructing Pseudorandom generators (PRGs) for the circuit class.

Why average case lower bounds

- Improves our understanding of limitations of circuits.
- Lower bounds against slightly stronger circuit classes (E.g - Kane-Williams 2015).
- Prerequisite for constructing Pseudorandom generators (PRGs) for the circuit class.
- Increased understanding can lead to satisfiability algorithms, learning algorithms,...

Results

- (Impagliazzo-Paturi-Saks 1991) PARITY not in $\mathrm{TC}^0_g(n^{1/2(d-1)}, d)$ and $\mathrm{TC}^0_w(n^{1+\varepsilon^d}, d)$.

Results

- (Impagliazzo-Paturi-Saks 1991) PARITY not in $\mathrm{TC}^0_g(n^{1/2(d-1)}, d)$ and $\mathrm{TC}^0_w(n^{1+\varepsilon^d}, d)$.
- Result 1: PARITY has $o(1)$-correlation with $\mathrm{TC}^0_g(o(n^{1/2(d-1)}), d)$ and $\mathrm{TC}^0_w(n^{1+\delta^d}, d)$.

Results

- (Impagliazzo-Paturi-Saks 1991) PARITY not in $\mathrm{TC}^0_g(n^{1/2(d-1)}, d)$ and $\mathrm{TC}^0_w(n^{1+\varepsilon^d}, d)$.
- Result 1: PARITY has $o(1)$-correlation with $\mathrm{TC}^0_g(o(n^{1/2(d-1)}), d)$ and $\mathrm{TC}^0_w(n^{1+\delta^d}, d)$.
- Gates result weaker than Nisan (1992) if any explicit function allowed.

Results

- (Impagliazzo-Paturi-Saks 1991) PARITY not in $\mathrm{TC}^0_g(n^{1/2(d-1)}, d)$ and $\mathrm{TC}^0_w(n^{1+\varepsilon^d}, d)$.
- Result 1: PARITY has $o(1)$-correlation with $\mathrm{TC}^0_g(o(n^{1/2(d-1)}), d)$ and $\mathrm{TC}^0_w(n^{1+\delta^d}, d)$.
- Gates result weaker than Nisan (1992) if any explicit function allowed.
- Result 2: Different explicit function has exponentially small correlation with $\mathrm{TC}^0_w(n^{1+\delta^d}, d)$.

Random restrictions

- Restriction: setting variables to constants. Helps simplify circuit.

Random restrictions

- Restriction: setting variables to constants. Helps simplify circuit. $\rho : \{x_1, \ldots, x_n\} \to \{0, 1, *\}$.

Random restrictions

- Restriction: setting variables to constants. Helps simplify circuit. $\rho : \{x_1, \ldots, x_n\} \to \{0, 1, *\}$.
- Random restriction $\rho \sim \mathcal{R}_p$:

$$\Pr_{\rho}[\rho(x_i) = *] = p \qquad \Pr_{\rho}[\rho(x_i) = 0/1] = \frac{1-p}{2}$$

Random restrictions

- Restriction: setting variables to constants. Helps simplify circuit. $\rho : \{x_1, \ldots, x_n\} \to \{0, 1, *\}$.
- Random restriction $\rho \sim \mathcal{R}_p$:

$$\Pr_{\rho}[\rho(x_i) = *] = p \qquad \Pr_{\rho}[\rho(x_i) = 0/1] = \frac{1-p}{2}$$

- Role of Random restriction: simplify circuit, while leaving hard function (relatively) unchanged.

Key lemma

- How does the circuit simplify due to a random restriction?

Key lemma

- How does the circuit simplify due to a random restriction?
- For threshold circuits: Peres' theorem.

Peres' theorem

- Informal: if f a threshold function and $\rho \sim \mathcal{R}_p$ (small p), then $f|_\rho$ is close to constant whp.

Peres' theorem

- Informal: if f a threshold function and $\rho \sim \mathcal{R}_p$ (small p), then $f|_\rho$ is close to constant whp.
- Measure bias using $\mathrm{Var}(g) = 2\,\mathsf{Pr}_{x,y}[g(x) \neq g(y)] \in [0,1]$.

Peres' theorem

- Informal: if f a threshold function and $\rho \sim \mathcal{R}_p$ (small p), then $f|_\rho$ is close to constant whp.
- Measure bias using $\mathrm{Var}(g) = 2\,\mathsf{Pr}_{x,y}[g(x) \neq g(y)] \in [0,1]$.
- g unbiased $\Leftrightarrow \mathrm{Var}(g) = 1$.

Peres' theorem

- Informal: if f a threshold function and $\rho \sim \mathcal{R}_p$ (small p), then $f|_\rho$ is close to constant whp.
- Measure bias using $\mathrm{Var}(g) = 2\,\mathsf{Pr}_{x,y}[g(x) \neq g(y)] \in [0,1]$.
- g unbiased $\Leftrightarrow \mathrm{Var}(g) = 1$. g constant $\Leftrightarrow \mathrm{Var}(g) = 0$.

Peres' theorem

- Informal: if f a threshold function and $\rho \sim \mathcal{R}_p$ (small p), then $f|_\rho$ is close to constant whp.
- Measure bias using $\mathrm{Var}(g) = 2\,\mathrm{Pr}_{x,y}[g(x) \neq g(y)] \in [0,1]$.
- g unbiased $\Leftrightarrow \mathrm{Var}(g) = 1$. g constant $\Leftrightarrow \mathrm{Var}(g) = 0$.

Theorem (Peres 2003)

f a threshold function. $\mathbf{E}_\rho[\mathrm{Var}(f|_\rho)] = O(\sqrt{p})$.

Peres' theorem

- Informal: if f a threshold function and $\rho \sim \mathcal{R}_p$ (small p), then $f|_\rho$ is close to constant whp.
- Measure bias using $\mathrm{Var}(g) = 2\,\mathsf{Pr}_{x,y}[g(x) \neq g(y)] \in [0,1]$.
- g unbiased $\Leftrightarrow \mathrm{Var}(g) = 1$. g constant $\Leftrightarrow \mathrm{Var}(g) = 0$.

Theorem (Peres 2003)

f a threshold function. $\mathbf{E}_\rho[\mathrm{Var}(f|_\rho)] = O(\sqrt{p})$.

- Compare with PARITY: $\mathbf{E}_\rho[\mathrm{Var}(\mathrm{PARITY}|_\rho)] \approx 1$ unless $p \approx 1/n$.

Peres' theorem

- Informal: if f a threshold function and $\rho \sim \mathcal{R}_p$ (small p), then $f|_\rho$ is close to constant whp.
- Measure bias using $\mathrm{Var}(g) = 2\,\mathrm{Pr}_{x,y}[g(x) \neq g(y)] \in [0,1]$.
- g unbiased $\Leftrightarrow \mathrm{Var}(g) = 1$. g constant $\Leftrightarrow \mathrm{Var}(g) = 0$.

Theorem (Peres 2003)

f a threshold function. $\mathbf{E}_\rho[\mathrm{Var}(f|_\rho)] = O(\sqrt{p})$.

- Compare with PARITY: $\mathbf{E}_\rho[\mathrm{Var}(\mathrm{PARITY}|_\rho)] \approx 1$ unless $p \approx 1/n$.

Corollary

f a threshold function. $\mathrm{Corr}(f, \mathrm{PARITY}) \leq O(\frac{1}{\sqrt{n}})$.

Gate lower bound

Theorem

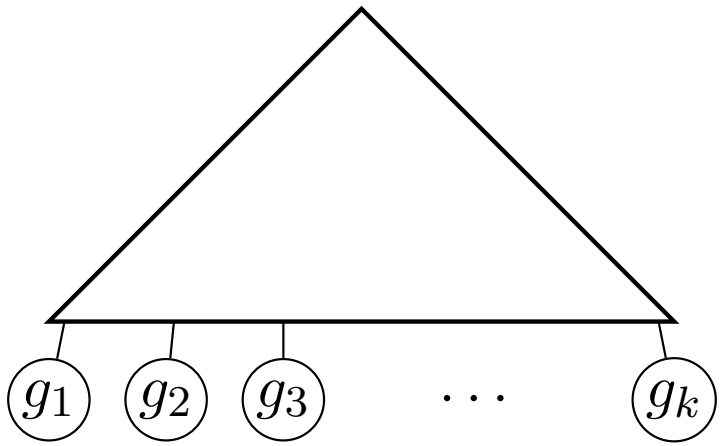
$$C \in \mathrm{TC}^0_g(o(n^{1/2(d-1)}), d) \Rightarrow \mathrm{Corr}(C, \mathrm{PARITY}) = o(1).$$

Gate lower bound

Theorem

$$C \in \mathrm{TC}^0_g(o(n^{1/2(d-1)}), d) \Rightarrow \mathrm{Corr}(C, \mathrm{PARITY}) = o(1).$$

- $C \in \mathrm{TC}^0_g(k, d)$.
- Bottom level gates: $g_1, \ldots, g_k$.

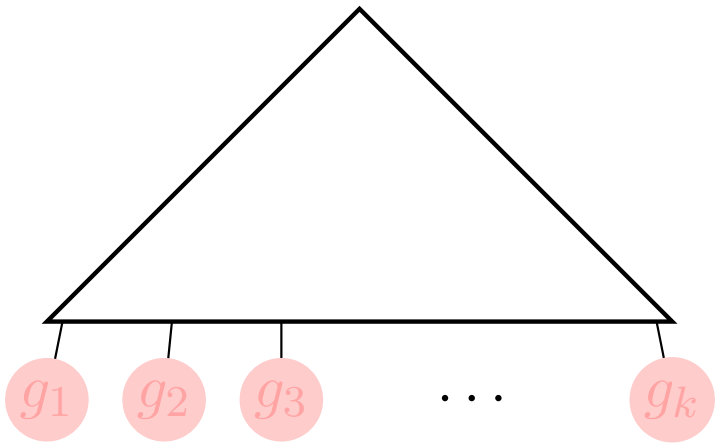


Gate lower bound

Theorem

$$C \in \mathrm{TC}^0_g(o(n^{1/2(d-1)}), d) \Rightarrow \mathrm{Corr}(C, \mathrm{PARITY}) = o(1).$$

- $C \in \mathrm{TC}^0_g(k, d)$.
- Bottom level gates: $g_1, \ldots, g_k$.
- Apply $\rho \sim \mathcal{R}_p$. Use Peres.

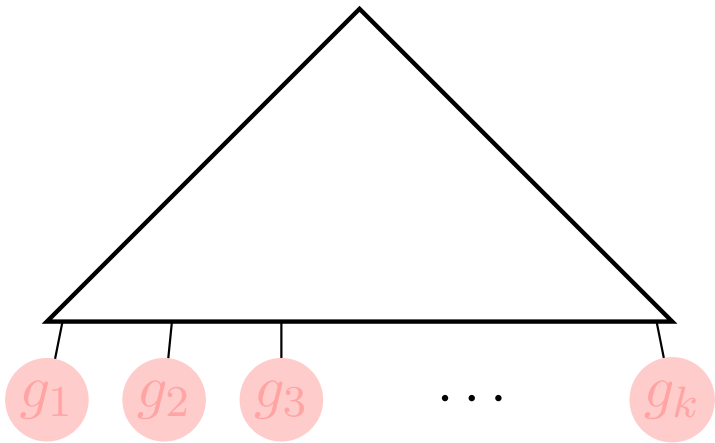


Gate lower bound

Theorem

$$C \in \mathrm{TC}^0_g(o(n^{1/2(d-1)}), d) \Rightarrow \mathrm{Corr}(C, \mathrm{PARITY}) = o(1).$$

- $C \in \mathrm{TC}^0_g(k, d)$.
- Bottom level gates: $g_1, \ldots, g_k$.
- Apply $\rho \sim \mathcal{R}_p$. Use Peres.
- $\mathbf{E}_\rho[\sum_i \mathrm{Var}(g_i)] \leq O(k\sqrt{p})$.

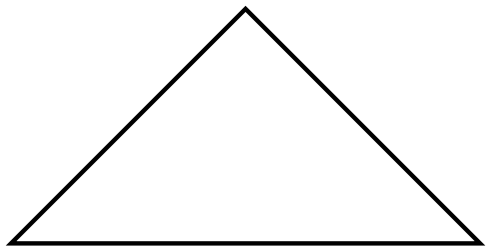


Gate lower bound

Theorem

$$C \in \mathrm{TC}^0_g(o(n^{1/2(d-1)}), d) \Rightarrow \mathrm{Corr}(C, \mathrm{PARITY}) = o(1).$$

- $C \in \mathrm{TC}^0_g(k, d)$.
- Bottom level gates: $g_1, \ldots, g_k$.
- Apply $\rho \sim \mathcal{R}_p$. Use Peres.
- $\mathbf{E}_\rho[\sum_i \mathrm{Var}(g_i)] \leq O(k\sqrt{p})$.
- Replace biased gates with constants. Depth is $d - 1$.

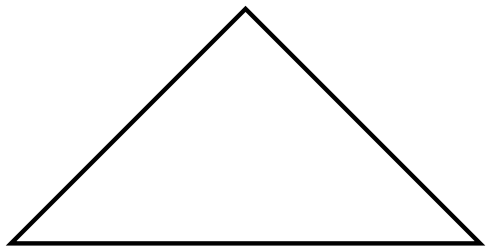


Gate lower bound

Theorem

$$C \in \mathrm{TC}^0_g(o(n^{1/2(d-1)}), d) \Rightarrow \mathrm{Corr}(C, \mathrm{PARITY}) = o(1).$$

- $C \in \mathrm{TC}^0_g(k, d)$.
- Bottom level gates: $g_1, \ldots, g_k$.
- Apply $\rho \sim \mathcal{R}_p$. Use Peres.
- $\mathbf{E}_\rho[\sum_i \mathrm{Var}(g_i)] \leq O(k\sqrt{p})$.
- Replace biased gates with constants. Depth is $d - 1$.
- Continue.



Gate lower bound (contd.)

Theorem

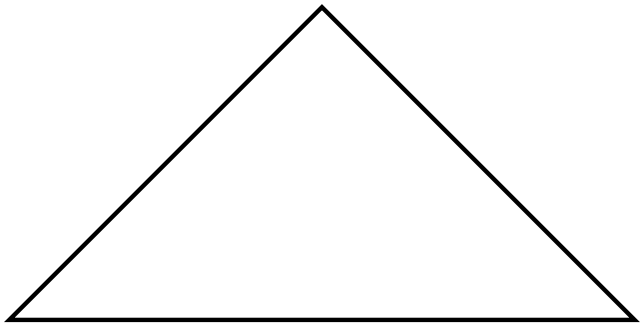
$$C \in \mathrm{TC}^0_g(o(n^{1/2(d-1)}), d) \Rightarrow \mathrm{Corr}(C, \mathrm{PARITY}) = o(1).$$

Gate lower bound (contd.)

Theorem

$C \in \mathrm{TC}^0_g(o(n^{1/2(d-1)}), d) \Rightarrow \mathrm{Corr}(C, \mathrm{PARITY}) = o(1).$

- $C \in \mathrm{TC}^0_g(k, d)$.

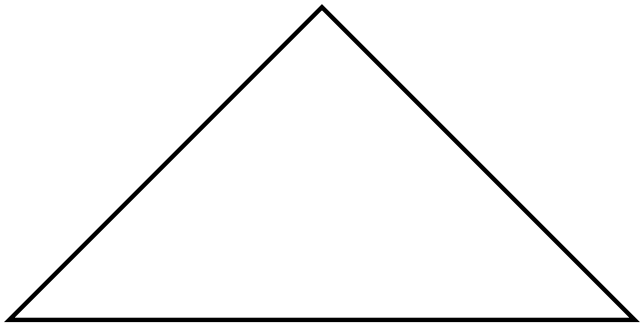


Gate lower bound (contd.)

Theorem

$$C \in \mathrm{TC}^0_g(o(n^{1/2(d-1)}), d) \Rightarrow \mathrm{Corr}(C, \mathrm{PARITY}) = o(1).$$

- $C \in \mathrm{TC}^0_g(k, d)$.
- Apply $\rho \sim \mathcal{R}_p$ d times.

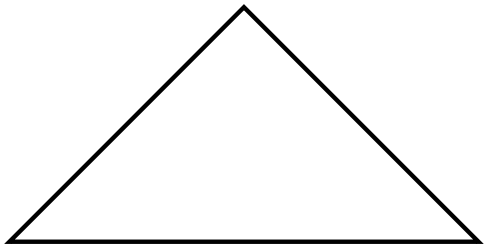


Gate lower bound (contd.)

Theorem

$$C \in \mathrm{TC}^0_g(o(n^{1/2(d-1)}), d) \Rightarrow \mathrm{Corr}(C, \mathrm{PARITY}) = o(1).$$

- $C \in \mathrm{TC}^0_g(k, d)$.
- Apply $\rho \sim \mathcal{R}_p$ d times.

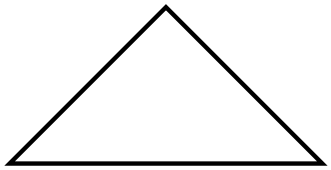


Gate lower bound (contd.)

Theorem

$$C \in \mathrm{TC}^0_g(o(n^{1/2(d-1)}), d) \Rightarrow \mathrm{Corr}(C, \mathrm{PARITY}) = o(1).$$

- $C \in \mathrm{TC}^0_g(k, d)$.
- Apply $\rho \sim \mathcal{R}_p$ d times.



Gate lower bound (contd.)

Theorem

$$C \in \mathrm{TC}^0_g(o(n^{1/2(d-1)}), d) \Rightarrow \mathrm{Corr}(C, \mathrm{PARITY}) = o(1).$$

- $C \in \mathrm{TC}^0_g(k, d)$.
- Apply $\rho \sim \mathcal{R}_p$ d times.

Gate lower bound (contd.)

Theorem

$$C \in \mathrm{TC}^0_g(o(n^{1/2(d-1)}), d) \Rightarrow \mathrm{Corr}(C, \mathrm{PARITY}) = o(1).$$

- $C \in \mathrm{TC}^0_g(k, d)$.
- Apply $\rho \sim \mathcal{R}_p$ d times.
- I.e. apply $\rho \sim \mathcal{R}_{p^d} = \mathcal{R}_q$.

Gate lower bound (contd.)

Theorem

$C \in \mathrm{TC}^0_g(o(n^{1/2(d-1)}), d) \Rightarrow \mathrm{Corr}(C, \mathrm{PARITY}) = o(1).$

- $C \in \mathrm{TC}^0_g(k, d)$.
- Apply $\rho \sim \mathcal{R}_p$ d times.
- I.e. apply $\rho \sim \mathcal{R}_{p^d} = \mathcal{R}_q$.
- $\mathbf{E}_\rho[\mathrm{Var}(C|_\rho)] \leq O(kq^{1/2d})$.

Gate lower bound (contd.)

Theorem

$C \in \mathrm{TC}^0_g(o(n^{1/2(d-1)}), d) \Rightarrow \mathrm{Corr}(C, \mathrm{PARITY}) = o(1).$

- $C \in \mathrm{TC}^0_g(k, d)$.
- Apply $\rho \sim \mathcal{R}_p$ d times.
- I.e. apply $\rho \sim \mathcal{R}_{p^d} = \mathcal{R}_q$.
- $\mathbf{E}_\rho[\mathrm{Var}(C|_\rho)] \leq O(kq^{1/2d})$.
- $\mathrm{Corr}(C, \mathrm{PARITY}) \leq o(1) = o(1)$ if $k \ll n^{1/2d}$.

Wire lower bound

Wire lower bound

Theorem

For some $\delta > 0$, *and* $C \in \mathrm{TC}^0_w(n^{1+\delta^d}, d)$, $\mathrm{Corr}(C, \mathrm{PARITY}) = o(1)$.

Wire lower bound

Theorem

For some $\delta > 0$, *and* $C \in \mathrm{TC}^0_w(n^{1+\delta^d}, d)$, $\mathrm{Corr}(C, \mathrm{PARITY}) = o(1)$.

- Why does the previous proof not work?

Wire lower bound

Theorem

For some $\delta > 0$, *and* $C \in \mathrm{TC}^0_w(n^{1+\delta^d}, d)$, $\mathrm{Corr}(C, \mathrm{PARITY}) = o(1)$.

- Why does the previous proof not work?
- Probability of failure in Peres' theorem: $O(1/\sqrt{n})$.

Wire lower bound

Theorem

For some $\delta > 0$, *and* $C \in \mathrm{TC}^0_w(n^{1+\delta^d}, d)$, $\mathrm{Corr}(C, \mathrm{PARITY}) = o(1)$.

- Why does the previous proof not work?
- Probability of failure in Peres' theorem: $O(1/\sqrt{n})$.
- Cannot handle more than $O(\sqrt{n})$ gates.

Wire lower bound

Theorem

For some $\delta > 0$, *and* $C \in \mathrm{TC}^0_w(n^{1+\delta^d}, d)$, $\mathrm{Corr}(C, \mathrm{PARITY}) = o(1)$.

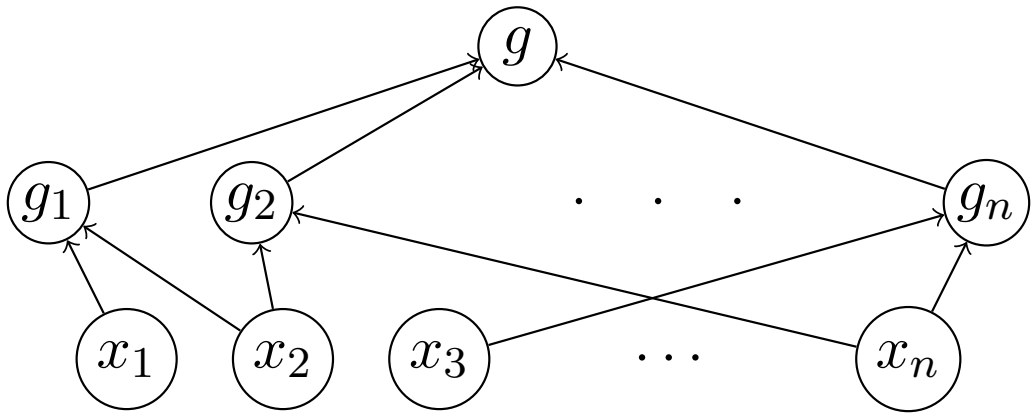
- Why does the previous proof not work?
- Probability of failure in Peres' theorem: $O(1/\sqrt{n})$.
- Cannot handle more than $O(\sqrt{n})$ gates.
- Even if $O(n)$ wires, we could have up to $O(n)$ gates.

Wire lower bound

Theorem

For some $\delta > 0$, *and* $C \in \mathrm{TC}^0_w(n^{1+\delta^d}, d)$, $\mathrm{Corr}(C, \mathrm{PARITY}) = o(1)$.

- Why does the previous proof not work?
- Probability of failure in Peres' theorem: $O(1/\sqrt{n})$.
- Cannot handle more than $O(\sqrt{n})$ gates.
- Even if $O(n)$ wires, we could have up to $O(n)$ gates.



Refining Peres' theorem

Lemma (Peres extension)

f a threshold. $Pr_\rho[\mathrm{Var}(f|_\rho)$ noticeable$] \leq p^{0.1}$.

Refining Peres' theorem

Lemma (Peres extension)

f a threshold. $Pr_\rho[\mathrm{Var}(f|_\rho)$ noticeable$] \leq p^{0.1}$.

- $\mathrm{Var}(f)$ not noticeable $\Leftrightarrow \mathrm{Var}(f) = \exp(-(1/p)^{\Omega(1)})$.

Refining Peres' theorem

Lemma (Peres extension)

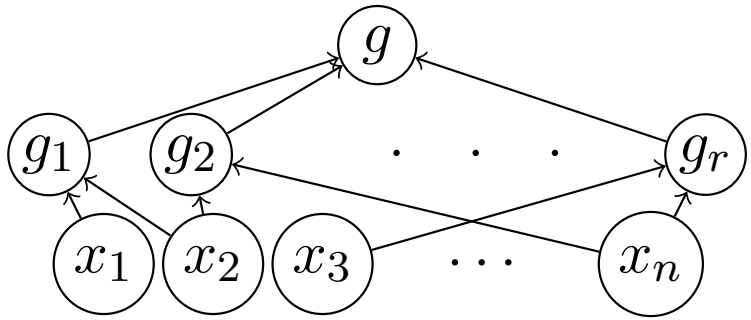
f a threshold. $Pr_\rho[\mathrm{Var}(f|_\rho)$ noticeable$] \leq p^{0.1}$.

- $\mathrm{Var}(f)$ not noticeable $\Leftrightarrow \mathrm{Var}(f) = \exp(-(1/p)^{\Omega(1)})$.
- Proof of lemma via standard CLT + critical index argument.

Back to the wires lower bound

Theorem

For some $\delta > 0$, *and* $C \in \mathrm{TC}^0_w(n^{1+\delta^d}, d)$, $\mathrm{Corr}(C, \mathrm{PARITY}) = o(1)$.

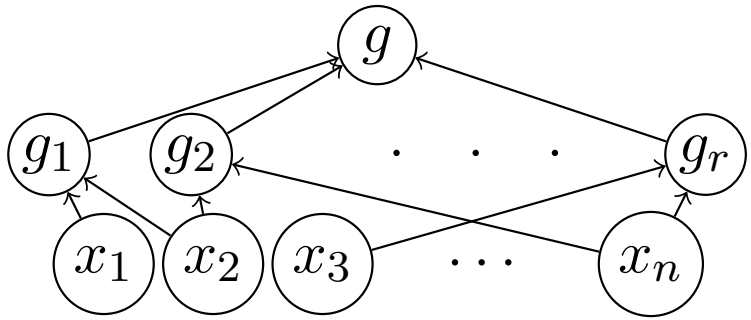


Back to the wires lower bound

Theorem

For some $\delta > 0$, and $C \in \mathrm{TC}^0_w(n^{1+\delta^d}, d)$, $\mathrm{Corr}(C, \mathrm{PARITY}) = o(1)$.

- $\sum_i \deg(g_i) \leq n^{1+\alpha}$.

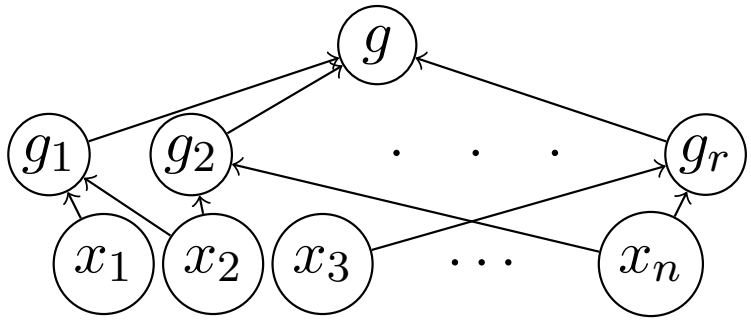


Back to the wires lower bound

Theorem

For some $\delta > 0$, *and* $C \in \mathrm{TC}^0_w(n^{1+\delta^d}, d)$, $\mathrm{Corr}(C, \mathrm{PARITY}) = o(1)$.

- $\sum_i \deg(g_i) \leq n^{1+\alpha}$.
- Apply $\rho \sim \mathcal{R}_p$, $p = n^{-O(\alpha)}$.

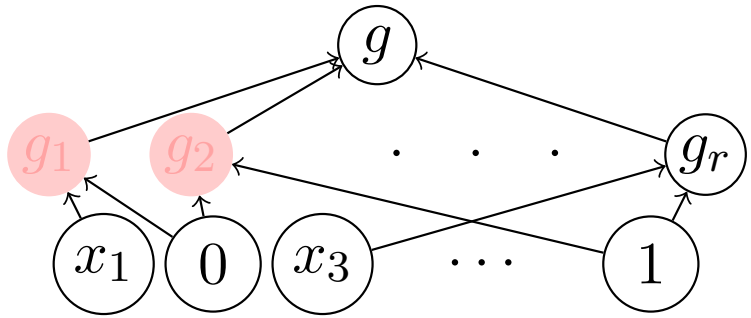


Back to the wires lower bound

Theorem

For some $\delta > 0$, *and* $C \in \mathrm{TC}^0_w(n^{1+\delta^d}, d)$, $\mathrm{Corr}(C, \mathrm{PARITY}) = o(1)$.

- $\sum_i \deg(g_i) \leq n^{1+\alpha}$.
- Apply $\rho \sim \mathcal{R}_p$, $p = n^{-O(\alpha)}$.
- New Peres: $(1 - p^{0.1})$ gates highly biased.

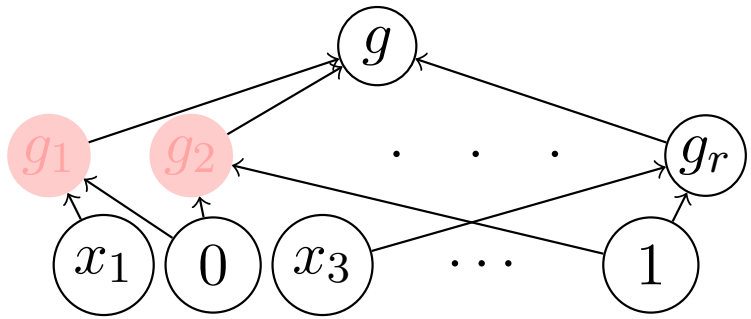


Back to the wires lower bound

Theorem

For some $\delta > 0$, *and* $C \in \mathrm{TC}^0_w(n^{1+\delta^d}, d)$, $\mathrm{Corr}(C, \mathrm{PARITY}) = o(1)$.

- $\sum_i \deg(g_i) \leq n^{1+\alpha}$.
- Apply $\rho \sim \mathcal{R}_p$, $p = n^{-O(\alpha)}$.
- New Peres: $(1 - p^{0.1})$ gates highly biased.
- Set to constants.

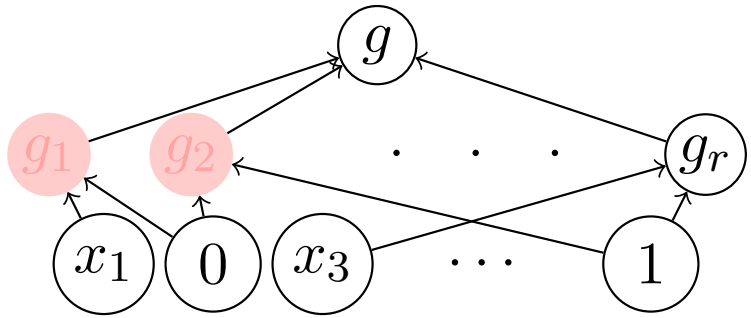


Back to the wires lower bound

Theorem

For some $\delta > 0$, *and* $C \in \mathrm{TC}^0_w(n^{1+\delta^d}, d)$, $\mathrm{Corr}(C, \mathrm{PARITY}) = o(1)$.

- $\sum_i \deg(g_i) \leq n^{1+\alpha}$.
- Apply $\rho \sim \mathcal{R}_p$, $p = n^{-O(\alpha)}$.
- New Peres: $(1 - p^{0.1})$ gates highly biased.
- Set to constants.
- $\sum_{\text{unbiased}} \deg(g_i) \leq p^{1+0.1} \cdot n^{1+\alpha} \ll pn$.

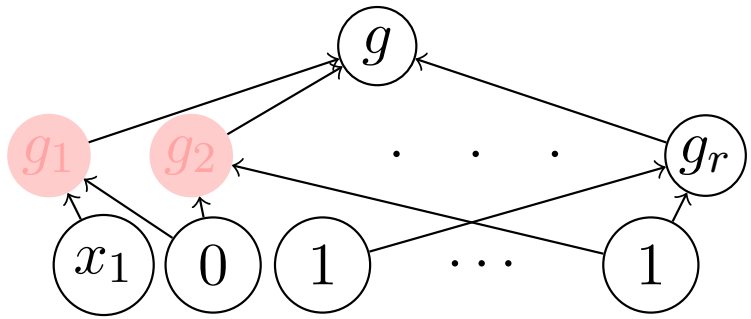


Back to the wires lower bound

Theorem

For some $\delta > 0$, *and* $C \in \mathrm{TC}^0_w(n^{1+\delta^d}, d)$, $\mathrm{Corr}(C, \mathrm{PARITY}) = o(1)$.

- $\sum_i \deg(g_i) \leq n^{1+\alpha}$.
- Apply $\rho \sim \mathcal{R}_p$, $p = n^{-O(\alpha)}$.
- New Peres: $(1 - p^{0.1})$ gates highly biased.
- Set to constants.
- $\sum_{\text{unbiased}} \deg(g_i) \leq p^{1+0.1} \cdot n^{1+\alpha} \ll pn$.
- Set all vars and continue.



More results

Theorem

For some $\delta > 0$, *and* $C \in \mathrm{TC}^0_w(n^{1+\delta^d}, d)$, $\mathrm{Corr}(C, \mathrm{PARITY}) = o(1)$.

More results

Theorem

For some $\delta > 0$, *and* $C \in \mathrm{TC}^0_w(n^{1+\delta^d}, d)$, $\mathrm{Corr}(C, \mathrm{PARITY}) = o(1)$.

- Above $o(1) = n^{-\Omega_d(1)}$.

More results

Theorem

For some $\delta > 0$, *and* $C \in \mathrm{TC}^0_w(n^{1+\delta^d}, d)$, $\mathrm{Corr}(C, \mathrm{PARITY}) = o(1)$.

- Above $o(1) = n^{-\Omega_d(1)}$.
- For a suitable other function f, $\mathrm{Corr}(f, C) \leq \exp(-n^{\Omega_d(1)})$.

More results

Theorem

For some $\delta > 0$, and $C \in \mathrm{TC}^0_w(n^{1+\delta^d}, d)$, $\mathrm{Corr}(C, \mathrm{PARITY}) = o(1)$.

- Above $o(1) = n^{-\Omega_d(1)}$.
- For a suitable other function f, $\mathrm{Corr}(f, C) \leq \exp(-n^{\Omega_d(1)})$.
- Satisfiability algorithms for $C \in \mathrm{TC}^0_w(n^{1+\delta^d}, d)$ running in time $2^{n-n^{\Omega_d(1)}}$.

More results

Theorem

For some $\delta > 0$, and $C \in \mathrm{TC}^0_w(n^{1+\delta^d}, d)$, $\mathrm{Corr}(C, \mathrm{PARITY}) = o(1)$.

- Above $o(1) = n^{-\Omega_d(1)}$.
- For a suitable other function f, $\mathrm{Corr}(f, C) \leq \exp(-n^{\Omega_d(1)})$.
- Satisfiability algorithms for $C \in \mathrm{TC}^0_w(n^{1+\delta^d}, d)$ running in time $2^{n-n^{\Omega_d(1)}}$.
- Better learning algorithms for AC^0 augmented with a few threshold gates.

Summary

- Proved correlation bounds for threshold circuits for computing PARITY and other explicit functions.

Summary

- Proved correlation bounds for threshold circuits for computing PARITY and other explicit functions.
- Bounds are close to tight for PARITY.

Summary

- Proved correlation bounds for threshold circuits for computing PARITY and other explicit functions.
- Bounds are close to tight for PARITY.
- Refined version of Peres' theorem gives more insight into the workings of threshold gates.

Summary

- Proved correlation bounds for threshold circuits for computing PARITY and other explicit functions.
- Bounds are close to tight for PARITY.
- Refined version of Peres' theorem gives more insight into the workings of threshold gates.
- More applications?
- Better lower bounds?

Summary

- Proved correlation bounds for threshold circuits for computing PARITY and other explicit functions.
- Bounds are close to tight for PARITY.
- Refined version of Peres' theorem gives more insight into the workings of threshold gates.
- More applications?
- Better lower bounds?

Thank you