### Average case lower bounds for threshold circuits

Ruiwen Chen, Rahul Santhanam and Srikanth Srinivasan

Oxford University and Department of Mathematics, IIT Bombay

Low-depth complexity workshop, St. Petersburg May 25, 2016.

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



• • = • • = •

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



A B A A B A

- 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*.



-∢ ∃ ▶

• Size *s* of the circuit: time taken by algorithm.



► < Ξ ►</p>

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



-

- A 🖃

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



- Size *s* of the circuit: time taken by algorithm.
- Could be # edges/wires or # gates.
- # wires ≤ (n+ # gates)· # gates.
- Depth *d* of the circuit: parallelism of the algorithm.



# wires = 8, # gates = 3

May 25, 2016 3 / 27

- Size *s* of the circuit: time taken by algorithm.
- Could be # edges/wires or # gates.
- # wires ≤ (n+ # gates)· # gates.
- Depth *d* of the circuit: parallelism of the algorithm.

• 
$$s = s(n), d = O(1).$$



# wires = 8, # gates = 3

May 25, 2016 3 / 27

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

・ロト ・回ト ・ヨト ・ヨ

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

イロト イヨト イヨト

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

くほと くほと くほと

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

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

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

- A threshold operation: g(x) = 1 iff  $\sum_i w_i x_i \ge \theta$  for  $w_i, \theta \in \mathbb{R}$ . Some examples:
- OR function: OR(x) = 1 iff  $\sum_i x_i \ge 1$ .
- AND function:  $AND(x) = \llbracket \sum_i x_i \ge n \rrbracket$ .
- MAJ function:  $MAJ(x) = \llbracket \sum_i x_i \ge n/2 \rrbracket$ .
- GEQ function:  $\operatorname{GEQ}(x, y) = \llbracket \sum_i 2^i (x_i y_i) \ge 0 \rrbracket$ .
- $TC_g^0(s, d)$ : threshold circuits with s gates and depth d.
- $TC_w^0(s, d)$ : threshold circuits with s wires and depth d.

- A threshold operation: g(x) = 1 iff  $\sum_i w_i x_i \ge \theta$  for  $w_i, \theta \in \mathbb{R}$ . Some examples:
- OR function: OR(x) = 1 iff  $\sum_i x_i \ge 1$ .
- AND function:  $AND(x) = \llbracket \sum_i x_i \ge n \rrbracket$ .
- MAJ function:  $MAJ(x) = \llbracket \sum_i x_i \ge n/2 \rrbracket$ .
- GEQ function:  $\operatorname{GEQ}(x, y) = \llbracket \sum_i 2^i (x_i y_i) \ge 0 \rrbracket$ .
- $TC_g^0(s, d)$ : threshold circuits with s gates and depth d.
- $TC_w^0(s, d)$ : threshold circuits with s wires and depth d.
- $\bullet\,$  Generalize  $\mathsf{AC}^0$  circuits made up of AND and OR gates.

• 
$$f = PARITY(x_1, \ldots, x_n) = x_1 \oplus x_2 \oplus \cdots \oplus x_n$$
.

- K 🖻

・ロト ・回ト ・ヨト

• 
$$f = PARITY(x_1, \ldots, x_n) = x_1 \oplus x_2 \oplus \cdots \oplus x_n.$$

•  $d \ge 2$ :  $f \in TC_g^0(dn^{1/(d-1)}, d)$  (Siu-Roychowdhury-Kailath 1991)

- $f = \text{PARITY}(x_1, \dots, x_n) = x_1 \oplus x_2 \oplus \dots \oplus x_n.$
- $d \ge 2$ :  $f \in \mathrm{TC}_g^0(dn^{1/(d-1)}, d)$  (Siu-Roychowdhury-Kailath 1991)
- d = 2:  $f(x) = [[\sum_i x_i \ge 1]]$

- $f = PARITY(x_1, \ldots, x_n) = x_1 \oplus x_2 \oplus \cdots \oplus x_n.$
- $d \ge 2$ :  $f \in TC_g^0(dn^{1/(d-1)}, d)$  (Siu-Roychowdhury-Kailath 1991)
- d = 2:  $f(x) = [[\sum_i x_i \ge 1]] [[\sum_i x_i \ge 2]]$

- $f = PARITY(x_1, \ldots, x_n) = x_1 \oplus x_2 \oplus \cdots \oplus x_n.$
- $d \ge 2$ :  $f \in TC_g^0(dn^{1/(d-1)}, d)$  (Siu-Roychowdhury-Kailath 1991)
- d = 2:  $f(x) = [[\sum_i x_i \ge 1]] [[\sum_i x_i \ge 2]] + [[\sum_i x_i \ge 3]] \cdots$

- $f = \text{PARITY}(x_1, \dots, x_n) = x_1 \oplus x_2 \oplus \dots \oplus x_n$ . •  $d \ge 2$ :  $f \in \text{TC}_g^0(dn^{1/(d-1)}, d)$  (Siu-Roychowdhury-Kailath 1991)
- d = 2:  $f(x) = [[\sum_i x_i \ge 1]] [[\sum_i x_i \ge 2]] + [[\sum_i x_i \ge 3]] \cdots$



• 
$$f = \text{PARITY} \in \text{TC}_g^0(dn^{1/(d-1)}, d).$$
  
•  $d = 2$ :  $f(x) = [\![\sum_i x_i \ge 1]\!] - [\![\sum_i x_i \ge 2]\!] + [\![\sum_i x_i \ge 3]\!] \cdots$ .

- K 🕀

・ロト ・回ト ・ヨト

• 
$$f = \text{PARITY} \in \text{TC}_g^0(dn^{1/(d-1)}, d).$$
  
•  $d = 2$ :  $f(x) = [\![\sum_i x_i \ge 1]\!] - [\![\sum_i x_i \ge 2]\!] + [\![\sum_i x_i \ge 3]\!] \cdots .$   
•  $d = \log n.$ 

・ロト ・回ト ・ヨト ・ヨ

• 
$$f = \text{PARITY} \in \text{TC}_g^0(dn^{1/(d-1)}, d).$$
  
•  $d = 2$ :  $f(x) = [\![\sum_i x_i \ge 1]\!] - [\![\sum_i x_i \ge 2]\!] + [\![\sum_i x_i \ge 3]\!] \cdots .$   
•  $d = \log n.$ 

•  $g_1 = [\![\sum_i x_i \ge n/2]\!].$ 



▲ 同 ▶ → 三 ▶

∃ →

• 
$$f = \text{PARITY} \in \text{TC}_g^0(dn^{1/(d-1)}, d).$$
  
•  $d = 2$ :  $f(x) = [\![\sum_i x_i \ge 1]\!] - [\![\sum_i x_i \ge 2]\!] + [\![\sum_i x_i \ge 3]\!] \cdots .$   
•  $d = \log n.$ 

•  $g_1 = [\![\sum_i x_i \ge n/2]\!].$ •  $g_2 = \left[ \sum_i x_i - \frac{n}{2} g_1 \ge n/4 \right].$ 



- ∢ ≣ →

• 
$$f = \text{PARITY} \in \text{TC}_g^0(dn^{1/(d-1)}, d).$$
  
•  $d = 2$ :  $f(x) = [\![\sum_i x_i \ge 1]\!] - [\![\sum_i x_i \ge 2]\!] + [\![\sum_i x_i \ge 3]\!] \cdots .$   
•  $d = \log n.$ 

•  $g_1 = [\![\sum_i x_i \ge n/2]\!].$ •  $g_2 = \left[ \sum_i x_i - \frac{n}{2} g_1 \ge n/4 \right].$ ÷

• 
$$g_{\ell} = \left[ \left[ \sum_{i} x_{i} - \frac{n}{2} g_{1} - \frac{n}{4} g_{2} \cdots \ge 1 \right] \right]$$



→ < Ξ →</p>

• 
$$f = \text{PARITY} \in \text{TC}_g^0(dn^{1/(d-1)}, d).$$
  
•  $d = 2$ :  $f(x) = [\![\sum_i x_i \ge 1]\!] - [\![\sum_i x_i \ge 2]\!] + [\![\sum_i x_i \ge 3]\!] \cdots .$   
•  $d = \log n.$ 

- $g_1 = [\![\sum_i x_i \ge n/2]\!].$ •  $g_2 = [\![\sum_i x_i - \frac{n}{2}g_1 \ge n/4]\!].$ •  $\vdots$
- $g_{\ell} = \left[ \left[ \sum_{i} x_{i} \frac{n}{2} g_{1} \frac{n}{4} g_{2} \cdots \ge 1 \right] \right]$



• General d: interpolate between the above two strategies.

Chen, Santhanam, S

• PARITY  $\in \mathrm{TC}_{g}^{0}(dn^{1/(d-1)}, d).$ 

A⊒ ▶ < ∃

- PARITY  $\in \mathrm{TC}^0_q(dn^{1/(d-1)}, d).$
- Wire complexity of PARITY?

- PARITY  $\in \mathrm{TC}^0_q(dn^{1/(d-1)}, d).$
- Wire complexity of PARITY?
- Gate upper bound  $\Rightarrow$  PARITY  $\in TC_w^0(dn^{1+1/(d-1)}, d)$ .

- PARITY  $\in \mathrm{TC}_g^0(dn^{1/(d-1)}, d).$
- Wire complexity of PARITY?
- Gate upper bound  $\Rightarrow$  PARITY  $\in TC_w^0(dn^{1+1/(d-1)}, d)$ .
- Can do better (Beame-Brisson-Ladner, Paturi-Saks).

- PARITY  $\in \mathrm{TC}_g^0(dn^{1/(d-1)}, d).$
- Wire complexity of PARITY?
- Gate upper bound  $\Rightarrow$  PARITY  $\in TC_w^0(dn^{1+1/(d-1)}, d)$ .
- Can do better (Beame-Brisson-Ladner, Paturi-Saks).
- PARITY  $\in \mathrm{TC}^0_w(n^{1+\varepsilon^d}, d).$

- PARITY  $\in \mathrm{TC}_g^0(dn^{1/(d-1)}, d).$
- Wire complexity of PARITY?
- Gate upper bound  $\Rightarrow$  PARITY  $\in TC_w^0(dn^{1+1/(d-1)}, d)$ .
- Can do better (Beame-Brisson-Ladner, Paturi-Saks).
- PARITY  $\in TC_w^0(n^{1+\varepsilon^d}, d)$ .

Trick:

$$x_1 \oplus \cdots \oplus x_n = (x_1 \oplus \cdots \oplus x_m) \oplus (x_{m+1} \oplus \cdots \oplus x_{2m}) \oplus \cdots$$

## Circuit lower bounds

• How efficient are threshold circuits for computing general functions?
- How efficient are threshold circuits for computing general functions?
- Depth-2 circuits can compute every function with size  $\approx 2^n$ .

- How efficient are threshold circuits for computing general functions?
- Depth-2 circuits can compute every function with size  $\approx 2^n$ .
- Random  $f: \{0,1\}^n \to \{0,1\}$  has no threshold circuit with fewer than  $2^{0.99n}$  wires w.h.p..

- How efficient are threshold circuits for computing general functions?
- Depth-2 circuits can compute every function with size  $\approx 2^n$ .
- Random  $f:\{0,1\}^n\to \{0,1\}$  has no threshold circuit with fewer than  $2^{0.99n}$  wires w.h.p..
- Problem: Find explicit family of functions (say in NP) that have no  $TC^0$  circuits of poly(n) size.

- How efficient are threshold circuits for computing general functions?
- Depth-2 circuits can compute every function with size  $\approx 2^n$ .
- Random  $f:\{0,1\}^n\to \{0,1\}$  has no threshold circuit with fewer than  $2^{0.99n}$  wires w.h.p..
- 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 and Rudich 1994; Podolskii 2012
- (Combinatorial restrictions) Impagliazzo Paturi Saks 1991
- (Communication complexity) Nisan 1992; Hansen and Miltersen 2004; Chattopadhyay and Hansen 2005; Lovett, S. 2012
- (Analytic techniques) Gopalan and Servedio 2010

• (Furst-Saxe-Sipser, Ajtai, Yao, Håstad 80s) PARITY not in  $AC^0(2^{n^{1/(d-1)}}, d)$ .

- (Furst-Saxe-Sipser, Ajtai, Yao, Håstad 80s) PARITY not in  $AC^0(2^{n^{1/(d-1)}}, d)$ .
- (Impagliazzo-Paturi-Saks 1991) PARITY not in  $TC_g^0(n^{1/2(d-1)}, d)$  and  $TC_w^0(n^{1+\varepsilon^d}, d)$ .

- (Furst-Saxe-Sipser, Ajtai, Yao, Håstad 80s) PARITY not in  $AC^0(2^{n^{1/(d-1)}}, d)$ .
- (Impagliazzo-Paturi-Saks 1991) PARITY not in  $TC_g^0(n^{1/2(d-1)}, d)$  and  $TC_w^0(n^{1+\varepsilon^d}, d)$ .
- (Kane-Williams 2015) Explicit functions not in  $TC_g^0(n^{1.5-o(1)}, 2)$  and  $TC_w^0(n^{2.5-o(1)}, 2)$ .

- (Furst-Saxe-Sipser, Ajtai, Yao, Håstad 80s) PARITY not in  $AC^0(2^{n^{1/(d-1)}}, d)$ .
- (Impagliazzo-Paturi-Saks 1991) PARITY not in  $TC_g^0(n^{1/2(d-1)}, d)$  and  $TC_w^0(n^{1+\epsilon^d}, d)$ .
- (Kane-Williams 2015) Explicit functions not in  $\mathrm{TC}_g^0(n^{1.5-o(1)}, 2)$  and  $\mathrm{TC}_w^0(n^{2.5-o(1)}, 2)$ . Also extends to a special case of depth-3.

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

► < ∃ ►</p>

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

- 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  $\varepsilon\text{-correlation}$  with ckt C if

$$\operatorname{Corr}(C, f) := \Pr_{x}[C(x) = f(x)] - \frac{1}{2} \le \varepsilon.$$

- 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  $\varepsilon$ -correlation with ckt C if

$$\operatorname{Corr}(C, f) := \Pr_{x}[C(x) = f(x)] - \frac{1}{2} \le \varepsilon.$$

• Want to show that f hard on average against  $TC^0(s, d)$ .

• Improves our understanding of limitations of circuits.

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

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

- 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.

- 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,...

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

→ Ξ →

→ < ∃ >

### Results

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

### Results

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

### Results

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

### Random restrictions

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

► < ∃ ►</p>

### 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.  $\rho: \{x_1, \ldots, x_n\} \rightarrow \{0, 1, *\}.$
- Random restriction  $\rho \sim \mathcal{R}_p$ :

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

-1

- - E 🕨

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

- Role of Random restriction: simplify circuit, while leaving hard function (rel.) unchanged.
- Eg. with  $AC^0$  and PARITY.

- Role of Random restriction: simplify circuit, while leaving hard function (rel.) unchanged.
- Eg. with  $AC^0$  and PARITY.



 $f(x) = x_1 \oplus \cdots \oplus x_n$ 

- Role of Random restriction: simplify circuit, while leaving hard function (rel.) unchanged.
- Eg. with  $AC^0$  and PARITY.



$$f(x) = x_1 \oplus \cdots \oplus x_n$$
  $f|_{\rho_1}(x) = \bigoplus_{i \in \rho_1^{-1}(*)} x_i$ 

- Role of Random restriction: simplify circuit, while leaving hard function (rel.) unchanged.
- Eg. with AC<sup>0</sup> and PARITY.



 $f(x) = x_1 \oplus \dots \oplus x_n \qquad f|_{\rho_1}(x) = \oplus_{i \in \rho_1^{-1}(*)} x_i \qquad f|_{\rho_1 \rho_2}(x) \qquad f|_{\rho_1 \rho_2 \rho_3}(x)$ 



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

# Key lemma

- How does the circuit simplify due to a random restriction?
- Håstad's Switching lemma: If C is a small CNF (resp. DNF), then whp  $C|_{\rho}$  is a small DNF (resp. CNF).

# Key lemma

- How does the circuit simplify due to a random restriction?
- Håstad's Switching lemma: If C is a small CNF (resp. DNF), then whp  $C|_{\rho}$  is a small DNF (resp. CNF).
- 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.

► < ∃ ►</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  $\operatorname{Var}(g) = 2 \operatorname{Pr}_{x,y}[g(x) \neq g(y)] \in [0,1].$

#### 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  $\operatorname{Var}(g) = 2 \operatorname{Pr}_{x,y}[g(x) \neq g(y)] \in [0,1].$
- g unbiased  $\Leftrightarrow \operatorname{Var}(g) = 1$ .
- 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  $\operatorname{Var}(g) = 2 \operatorname{Pr}_{x,y}[g(x) \neq g(y)] \in [0,1].$
- g unbiased  $\Leftrightarrow \operatorname{Var}(g) = 1$ . g constant  $\Leftrightarrow \operatorname{Var}(g) = 0$ .

- 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  $\operatorname{Var}(g) = 2 \operatorname{Pr}_{x,y}[g(x) \neq g(y)] \in [0,1].$
- g unbiased  $\Leftrightarrow \operatorname{Var}(g) = 1$ . g constant  $\Leftrightarrow \operatorname{Var}(g) = 0$ .

### Theorem (Peres 2003)

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

- 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  $\operatorname{Var}(g) = 2 \operatorname{Pr}_{x,y}[g(x) \neq g(y)] \in [0,1].$
- g unbiased  $\Leftrightarrow \operatorname{Var}(g) = 1$ . g constant  $\Leftrightarrow \operatorname{Var}(g) = 0$ .

### Theorem (Peres 2003)

- f a threshold function.  $\mathbf{E}_{\rho}[\operatorname{Var}(f|_{\rho})] = O(\sqrt{p}).$ 
  - Compare with PARITY:  $\mathbf{E}_{\rho}[Var(PARITY|_{\rho})] \approx 1$  unless  $p \approx 1/n$ .

▲ロト ▲圖ト ▲画ト ▲画ト 三直 - のへで

- 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  $\operatorname{Var}(g) = 2 \operatorname{Pr}_{x,y}[g(x) \neq g(y)] \in [0,1].$
- g unbiased  $\Leftrightarrow \operatorname{Var}(g) = 1$ . g constant  $\Leftrightarrow \operatorname{Var}(g) = 0$ .

### Theorem (Peres 2003)

- f a threshold function.  $\mathbf{E}_{\rho}[\operatorname{Var}(f|_{\rho})] = O(\sqrt{p}).$ 
  - Compare with PARITY:  $\mathbf{E}_{\rho}[Var(PARITY|_{\rho})] \approx 1$  unless  $p \approx 1/n$ .

#### Corollary

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

▲ロト ▲圖ト ▲画ト ▲画ト 三直 - のへで

### Theorem

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

・ロト ・ 日 ト ・ ヨ ト ・ ヨ ト

#### Theorem

- $C \in \mathrm{TC}^0_a(o(n^{1/2(d-1)}), d) \Rightarrow \mathrm{Corr}(C, \mathrm{PARITY}) = o(1).$
- $C \in \mathrm{TC}^0_a(k, d).$
- Bottom level gates:  $g_1, \ldots, g_k$ .



#### Theorem

- $C \in \mathrm{TC}^0_a(o(n^{1/2(d-1)}), d) \Rightarrow \mathrm{Corr}(C, \mathrm{PARITY}) = o(1).$
- $C \in \mathrm{TC}^0_a(k, d).$
- Bottom level gates:  $g_1, \ldots, g_k$ .
- Apply  $\rho \sim \mathcal{R}_p$ . Use Peres.



#### Theorem

- $C \in \mathrm{TC}^0_a(o(n^{1/2(d-1)}), d) \Rightarrow \mathrm{Corr}(C, \mathrm{PARITY}) = o(1).$
- $C \in \mathrm{TC}^0_a(k, d).$
- Bottom level gates:  $g_1, \ldots, g_k$ .
- Apply  $\rho \sim \mathcal{R}_p$ . Use Peres.
- $\mathbf{E}_{\rho}[\sum_{i} \operatorname{Var}(g_{i})] \leq O(k\sqrt{p}).$



#### Theorem

- $C \in \mathrm{TC}_q^0(o(n^{1/2(d-1)}), d) \Rightarrow \mathrm{Corr}(C, \mathrm{PARITY}) = o(1).$
- $C \in \mathrm{TC}_g^0(k, d)$ .
- Bottom level gates:  $g_1, \ldots, g_k$ .
- Apply  $\rho \sim \mathcal{R}_p$ . Use Peres.
- $\mathbf{E}_{\rho}[\sum_{i} \operatorname{Var}(g_i)] \le O(k\sqrt{p}).$
- Replace biased gates with constants. Depth is d-1.



#### Theorem

- $C \in \mathrm{TC}^0_a(o(n^{1/2(d-1)}), d) \Rightarrow \mathrm{Corr}(C, \mathrm{PARITY}) = o(1).$
- $C \in \mathrm{TC}^0_a(k, d).$
- Bottom level gates:  $g_1, \ldots, g_k$ .
- Apply  $\rho \sim \mathcal{R}_p$ . Use Peres.
- $\mathbf{E}_{\rho}[\sum_{i} \operatorname{Var}(g_{i})] \leq O(k\sqrt{p}).$
- Replace biased gates with constants. Depth is d-1.
- Continue.



→

### Theorem

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

イロト イ団ト イヨト イヨト

### Theorem

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

•  $C \in \mathrm{TC}_g^0(k, d)$ .



э.

### Theorem

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

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



3

- ∢ ∃ ▶

### Theorem

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

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



3

- ∢ ∃ ▶

### Theorem

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

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



-

-∢ ∃ ▶

### Theorem

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

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

3

- ∢ ∃ ▶

#### Theorem

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

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

#### Theorem

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

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

∃ →

- ∢ ∃ ▶

#### Theorem

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

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

-

-∢ ∃ ▶

Chen, Santhanam, S.

<ロ> (日) (日) (日) (日) (日)

#### Theorem

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

▲ロト ▲圖ト ▲画ト ▲画ト 三直 - のへで

#### Theorem

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

• Why does the previous proof not work?

→ 3 → 4 3

#### Theorem

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

#### Theorem

- 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.

#### Theorem

- 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.

#### Theorem

- 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.



Theorem (Peres)

f a threshold.  $\mathbf{E}_{\rho \sim \mathcal{R}_p}[\operatorname{Var}(f|_{\rho})] = O(\sqrt{p}).$ 

• Why  $O(\sqrt{p})?$ 

▲□ ▶ ▲ 臣 ▶ ▲ 臣 ▶ ▲ 臣 ● の Q @

Theorem (Peres)

f a threshold.  $\mathbf{E}_{\rho \sim \mathcal{R}_p}[\operatorname{Var}(f|_{\rho})] = O(\sqrt{p}).$ 

- Why  $O(\sqrt{p})$ ?
- Eg:  $f(x) = [\![\sum_i x_i \ge n/2]\!]$ .

Theorem (Peres)

f a threshold.  $\mathbf{E}_{\rho \sim \mathcal{R}_p}[\operatorname{Var}(f|_{\rho})] = O(\sqrt{p}).$ 

- Why  $O(\sqrt{p})$ ?
- Eg:  $f(x) = [\![\sum_i x_i \ge n/2]\!].$
- $f|_{\rho}(x) = [\![\sum_{i \le m} x_i \ge n/2 \theta]\!].$

Theorem (Peres)

f a threshold.  $\mathbf{E}_{\rho \sim \mathcal{R}_p}[\operatorname{Var}(f|_{\rho})] = O(\sqrt{p}).$ 

- Why  $O(\sqrt{p})$ ?
- Eg:  $f(x) = [\![\sum_i x_i \ge n/2]\!]$ .
- $f|_{\rho}(x) = [\![\sum_{i \le m} x_i \ge n/2 \theta]\!].$



過 ト イヨ ト イヨト

Theorem (Peres)

f a threshold.  $\mathbf{E}_{\rho \sim \mathcal{R}_p}[\operatorname{Var}(f|_{\rho})] = O(\sqrt{p}).$ 

- Why  $O(\sqrt{p})$ ?
- Eg:  $f(x) = \llbracket \sum_i x_i \ge n/2 \rrbracket$ .

• 
$$f|_{\rho}(x) = [\![\sum_{i \le m} x_i \ge n/2 - \theta]\!].$$

• 
$$\theta = \text{sum of } n - m \approx n \text{ random bits.}$$



Average case bounds for TC<sup>0</sup>

Theorem (Peres)

f a threshold.  $\mathbf{E}_{\rho \sim \mathcal{R}_p}[\operatorname{Var}(f|_{\rho})] = O(\sqrt{p}).$ 

- Why  $O(\sqrt{p})$ ?
- Eg:  $f(x) = [\![\sum_i x_i \ge n/2]\!].$

• 
$$f|_{\rho}(x) = [\![\sum_{i \le m} x_i \ge n/2 - \theta]\!].$$

•  $\theta = \text{sum of } n - m \approx n \text{ random bits.}$ 

• 
$$\theta = (n-m)/2$$
:  $\operatorname{Var}(f|_{\rho}) = 1$ .



Theorem (Peres)

f a threshold.  $\mathbf{E}_{\rho \sim \mathcal{R}_p}[\operatorname{Var}(f|_{\rho})] = O(\sqrt{p}).$ 

• Why  $O(\sqrt{p})$ ? • Eg:  $f(x) = [\![\sum_i x_i \ge n/2]\!]$ . •  $f|_{\rho}(x) = [\![\sum_{i \le m} x_i \ge n/2 - \theta]\!]$ . •  $\theta = \text{sum of } n - m \approx n \text{ random bits.}$ •  $\theta = (n - m)/2$ :  $\operatorname{Var}(f|_{\rho}) = 1$ . •  $\theta = (n - m)/2 \pm O(\sqrt{m})$ :  $\operatorname{Var}(f|_{\rho}) = \Omega(1)$ .



Theorem (Peres)

f a threshold.  $\mathbf{E}_{\rho \sim \mathcal{R}_p}[\operatorname{Var}(f|_{\rho})] = O(\sqrt{p}).$ 

• Why  $O(\sqrt{p})$ ? • Eg:  $f(x) = [\sum_{i} x_i \ge n/2].$ •  $f|_{\rho}(x) = [\![\sum_{i < m} x_i \ge n/2 - \theta]\!].$ •  $\theta = \text{sum of } n - m \approx n \text{ random bits.}$ •  $\theta = (n-m)/2$ : Var $(f|_{\rho}) = 1$ . •  $\theta = (n-m)/2 \pm O(\sqrt{m})$ :  $\operatorname{Var}(f|_{\rho}) = \Omega(1).$ •  $\theta = (n-m)/2 \pm \omega(\sqrt{m})$ :  $Var(f|_{o}) = o(1).$ 



## Refining Peres' theorem (contd.)

Theorem (Peres)

f a threshold.  $\mathbf{E}_{\rho \sim \mathcal{R}_p}[\operatorname{Var}(f|_{\rho})] = O(\sqrt{p}).$ 

• Why 
$$O(\sqrt{p})$$
?  
• Eg:  $f(x) = [\![\sum_i x_i \ge n/2]\!]$ .  
•  $f|_{\rho}(x) = [\![\sum_{i \le m} x_i \ge n/2 - \theta]\!]$ .  
•  $\theta = (n - m)/2 \pm \omega(\sqrt{m})$ :  
 $\operatorname{Var}(f|_{\rho}) = o(1)$ .



 $\sum_{i < m} x_i$ 

## Refining Peres' theorem (contd.)

Theorem (Peres)

C

f a threshold.  $\mathbf{E}_{\rho \sim \mathcal{R}_p}[\operatorname{Var}(f|_{\rho})] = O(\sqrt{p}).$ 

• Why 
$$O(\sqrt{p})$$
?  
• Eg:  $f(x) = \llbracket \sum_{i \le m} x_i \ge n/2 \rrbracket$ .  
•  $f|_{\rho}(x) = \llbracket \sum_{i \le m} x_i \ge n/2 - \theta \rrbracket$ .  
•  $\theta = (n - m)/2 \pm \omega(\sqrt{m})$ :  
Var $(f|_{\rho}) = o(1)$ .  
•  $\mathbf{E}[\operatorname{Var}(f|_{\rho})] = \Omega(1)\sqrt{m}/\sqrt{n} = \Omega(\sqrt{p})$ .

・ロン ・四 ・ ・ ヨン ・ ヨン
# Refining Peres' theorem (contd.)

Lemma (Peres extension)

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

Chen, Santhanam, S.

Average case bounds for  $TC^0$ 

May 25, 2016 23 / 27

▲ロト ▲圖ト ▲画ト ▲画ト 三直 - のへで

# Refining Peres' theorem (contd.)

#### Lemma (Peres extension)

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

•  $\operatorname{Var}(f)$  not noticeable  $\Leftrightarrow \operatorname{Var}(f) = \exp(-n^{\Omega(1)}).$ 

▲ロト ▲圖ト ▲画ト ▲画ト 三直 - のへで

# Refining Peres' theorem (contd.)

#### Lemma (Peres extension)

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

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

#### Theorem

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



(日) (同) (三) (三)

#### Theorem

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

•  $\sum_i \deg(g_i) \le n^{1+\alpha}$ .



過下 イヨト イヨト ニヨ

#### Theorem

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

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



過き イヨト イヨト ニヨ

#### Theorem

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

•  $\sum_i \deg(g_i) \le n^{1+\alpha}$ .

• Apply 
$$ho \sim \mathcal{R}_p$$
,  $p = n^{-O(lpha)}$ 

• New Peres:  $(1-p^{0.1})$  gates highly biased.



過下 イヨト イヨト ニヨ

#### Theorem

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

•  $\sum_i \deg(g_i) \le n^{1+\alpha}$ .

• Apply 
$$ho \sim \mathcal{R}_p$$
,  $p = n^{-O(lpha)}$ 

- New Peres:  $(1-p^{0.1})$  gates highly biased.
- Set to constants.



#### Theorem

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

•  $\sum_i \deg(g_i) \le n^{1+\alpha}$ .

• Apply 
$$ho \sim \mathcal{R}_p$$
,  $p = n^{-O(lpha)}$ 

- New Peres:  $(1-p^{0.1})$  gates highly biased.
- Set to constants.
- $\sum_{\text{unbiased}} \deg(g_i) \le p^{1+0.1} \cdot n^{1+\alpha} \ll pn.$



伺下 イヨト イヨト ニヨ

#### Theorem

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

•  $\sum_i \deg(g_i) \le n^{1+\alpha}$ .

• Apply 
$$ho \sim \mathcal{R}_p$$
,  $p = n^{-O(lpha)}$ 

- New Peres:  $(1-p^{0.1})$  gates highly biased.
- Set to constants.
- $\sum_{\text{unbiased}} \deg(g_i) \le p^{1+0.1} \cdot n^{1+\alpha} \ll pn.$
- Set all vars and continue.



超す イヨト イヨト ニヨ

#### Theorem

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

-

Image: A matrix and a matrix

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

• • = • • = •

= 900

#### 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,  $\operatorname{Corr}(f, C) \leq \exp(-n^{\Omega_d(1)})$ .

#### Theorem

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

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

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

#### Theorem

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

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

- For a suitable other function f,  $\operatorname{Corr}(f, C) \leq \exp(-n^{\Omega_d(1)})$ .
- 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<sup>0</sup> augmented with a few threshold gates.



• 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?

Chen, Santhanam, S.

<ロ> (日) (日) (日) (日) (日)

• Optimal worst case depth 2 circuit for PARITY? Upper bound O(n)gates and lower bound  $\Omega(\sqrt{n})$ .

過 ト イヨ ト イヨト

- Optimal worst case depth 2 circuit for PARITY? Upper bound O(n) gates and lower bound  $\Omega(\sqrt{n})$ .
- Optimal version of Peres' theorem for threshold circuits with few gates? Two versions: ours and Gopalan-Servedio. Want a common generalization.

- Optimal worst case depth 2 circuit for PARITY? Upper bound O(n) gates and lower bound  $\Omega(\sqrt{n})$ .
- Optimal version of Peres' theorem for threshold circuits with few gates? Two versions: ours and Gopalan-Servedio. Want a common generalization.

# Thank you