

Near-Optimal Pseudorandom Generators for Constant-Depth Read-Once Formulas

Dean Doron¹ Pooya Hatami² William M. Hoza³

The University of Texas at Austin

Research Preparation Exam
May 1, 2019

¹Supported by NSF Grant CCF-1705028

²Supported by a Simons Investigator Award (#409864, David Zuckerman)

³Supported by the NSF GRFP under Grant DGE-1610403 and by a Harrington Fellowship from UT Austin

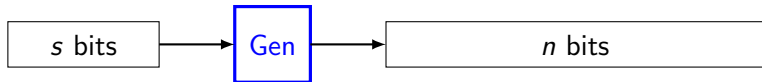
Randomness as a scarce resource

- ▶ Randomization is a popular algorithmic technique
- ▶ But randomness is **costly**

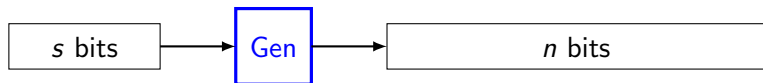
Randomness as a scarce resource

- ▶ Randomization is a popular algorithmic technique
- ▶ But randomness is **costly**
- ▶ An algorithm that uses **fewer random bits** is better

Pseudorandom generators (PRGs)



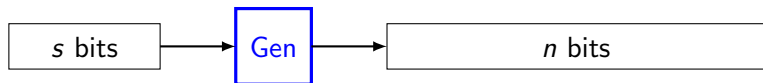
Pseudorandom generators (PRGs)



- ▶ Gen “fools” $f : \{0, 1\}^n \rightarrow \{0, 1\}$ if

$$\mathbb{E}[f(\text{Gen}(U))] = \mathbb{E}[f(U)] \pm \varepsilon$$

Pseudorandom generators (PRGs)

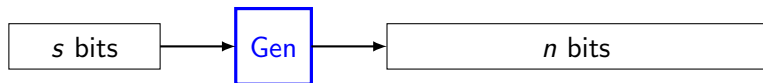


- ▶ Gen “fools” $f : \{0, 1\}^n \rightarrow \{0, 1\}$ if

$$\mathbb{E}[f(\text{Gen}(U))] = \mathbb{E}[f(U)] \pm \varepsilon$$

- ▶ Goal: Design PRG that fools an interesting **class** of functions f

Pseudorandom generators (PRGs)

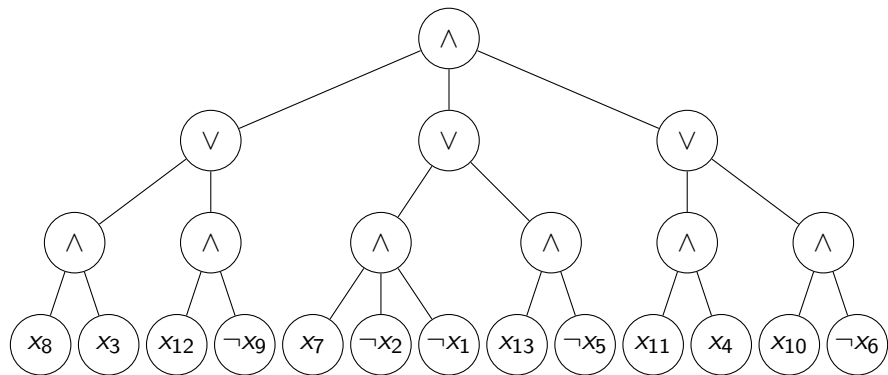


- ▶ Gen “fools” $f : \{0, 1\}^n \rightarrow \{0, 1\}$ if

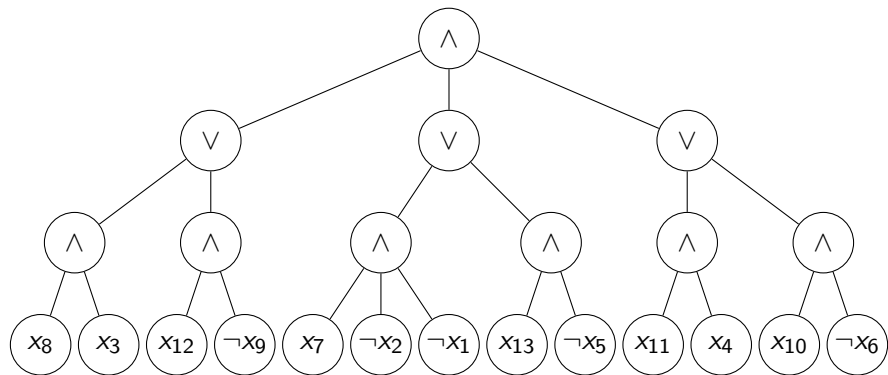
$$\mathbb{E}[f(\text{Gen}(U))] = \mathbb{E}[f(U)] \pm \varepsilon$$

- ▶ Goal: Design PRG that fools an interesting **class** of functions f
- ▶ Minimize seed length $s = s(n, \varepsilon)$

Read-once formulas

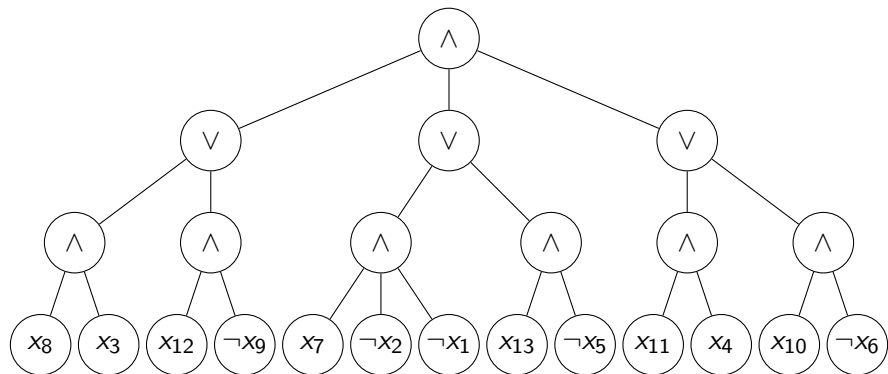


Read-once formulas



- ▶ This work: Fool depth- d read-once formulas for $d = O(1)$

Read-once formulas



- ▶ This work: Fool depth- d read-once formulas for $d = O(1)$
- ▶ Read-once version of \mathbf{AC}^0

Prior work and main result

Seed length	Model fooled	Reference
$O(n^{0.001})$	AC^0	Ajtai, Wigderson '89

Prior work and main result

Seed length	Model fooled	Reference
$O(n^{0.001})$	AC⁰	Ajtai, Wigderson '89
$O(\log^{2d+6} n)$	AC⁰	Nisan '91

Prior work and main result

Seed length	Model fooled	Reference
$O(n^{0.001})$	AC⁰	Ajtai, Wigderson '89
$O(\log^{2d+6} n)$	AC⁰	Nisan '91
$\tilde{O}(\log^{d+4} n)$	AC⁰	Trevisan, Xue '13

Prior work and main result

Seed length	Model fooled	Reference
$O(n^{0.001})$	AC ⁰	Ajtai, Wigderson '89
$O(\log^{2d+6} n)$	AC ⁰	Nisan '91
$\tilde{O}(\log^{d+4} n)$	AC ⁰	Trevisan, Xue '13
$\tilde{O}(\log^{d+1} n)$	Read-once AC ⁰	Chen, Steinke, Vadhan '15

Prior work and main result

Seed length	Model fooled	Reference
$O(n^{0.001})$	\mathbf{AC}^0	Ajtai, Wigderson '89
$O(\log^{2d+6} n)$	\mathbf{AC}^0	Nisan '91
$\tilde{O}(\log^{d+4} n)$	\mathbf{AC}^0	Trevisan, Xue '13
$\tilde{O}(\log^{d+1} n)$	Read-once \mathbf{AC}^0	Chen, Steinke, Vadhan '15
$\tilde{O}(\log^2 n)$	Arbitrary-order width- $O(1)$ ROBPs	Forbes, Kelley '18

Prior work and main result

Seed length	Model fooled	Reference
$O(n^{0.001})$	AC ⁰	Ajtai, Wigderson '89
$O(\log^{2d+6} n)$	AC ⁰	Nisan '91
$\tilde{O}(\log^{d+4} n)$	AC ⁰	Trevisan, Xue '13
$\tilde{O}(\log^{d+1} n)$	Read-once AC ⁰	Chen, Steinke, Vadhan '15
$\tilde{O}(\log^2 n)$	Arbitrary-order width- $O(1)$ ROBPs	Forbes, Kelley '18
$\tilde{O}(\log n)$	Read-once AC ⁰	This work

Prior work and main result

Seed length	Model fooled	Reference
$O(n^{0.001})$	\mathbf{AC}^0	Ajtai, Wigderson '89
$O(\log^{2d+6} n)$	\mathbf{AC}^0	Nisan '91
$\tilde{O}(\log^{d+4} n)$	\mathbf{AC}^0	Trevisan, Xue '13
$\tilde{O}(\log^{d+1} n)$	Read-once \mathbf{AC}^0	Chen, Steinke, Vadhan '15
$\tilde{O}(\log^2 n)$	Arbitrary-order width- $O(1)$ ROBPs	Forbes, Kelley '18
$\tilde{O}(\log n)$	Read-once \mathbf{AC}^0	This work

► **Main result:** PRG for read-once \mathbf{AC}^0 with seed length

$$\log(n/\varepsilon) \cdot O(d \log \log(n/\varepsilon))^{2d+2}.$$

Motivation: **L** vs. **BPL**

- ▶ Big open problem: Prove **L = BPL**

Motivation: **L** vs. **BPL**

- ▶ Big open problem: Prove **L = BPL**
 - ▶ “Randomness is not necessary for space-efficient computation”

Motivation: **L** vs. **BPL**

- ▶ Big open problem: Prove **L = BPL**
 - ▶ “Randomness is not necessary for space-efficient computation”
- ▶ Main approach: Design optimal PRG for “ROBPs”

Motivation: **L** vs. **BPL**

- ▶ Big open problem: Prove **L = BPL**
 - ▶ “Randomness is not necessary for space-efficient computation”
- ▶ Main approach: Design optimal PRG for “ROBPs”
- ▶ Bad news: Seed length $O(\log^2 n)$ has not been improved for decades [Nisan '92]

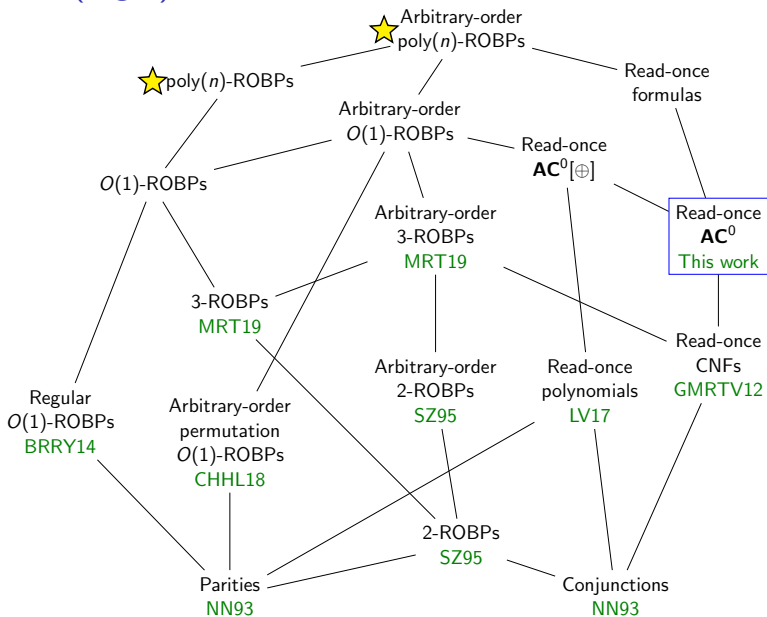
Motivation: **L** vs. **BPL**

- ▶ Big open problem: Prove **L = BPL**
 - ▶ “Randomness is not necessary for space-efficient computation”
- ▶ Main approach: Design optimal PRG for “ROBPs”
- ▶ Bad news: Seed length $O(\log^2 n)$ has not been improved for decades [Nisan '92]
- ▶ Good news: Can achieve seed length $\tilde{O}(\log n)$ for increasingly powerful **restricted models**

Motivation: **L** vs. **BPL**

- ▶ Big open problem: Prove **L** = **BPL**
 - ▶ “Randomness is not necessary for space-efficient computation”
- ▶ Main approach: Design optimal PRG for “ROBPs”
- ▶ Bad news: Seed length $O(\log^2 n)$ has not been improved for decades [Nisan '92]
- ▶ Good news: Can achieve seed length $\tilde{O}(\log n)$ for increasingly powerful **restricted models**
- ▶ Read-once **AC**⁰ is one of the **frontiers** of this progress

Seed length $\tilde{O}(\log n)$



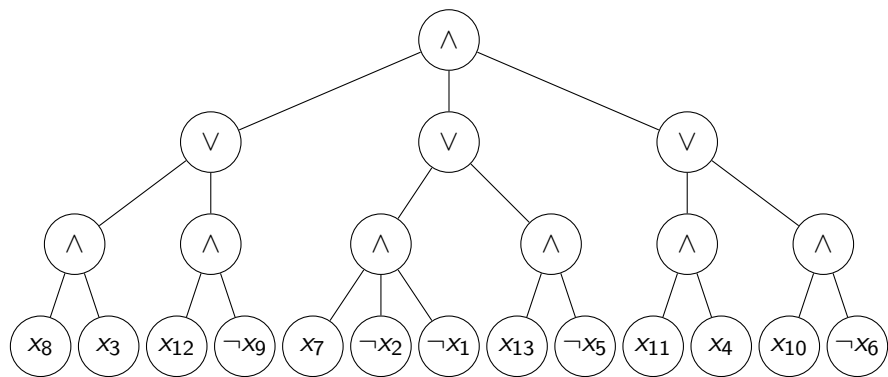
Starting point: Forbes-Kelley PRG

Seed length	Model fooled	Reference
$O(n^{0.001})$	AC ⁰	Ajtai, Wigderson '89
$O(\log^{2d+6} n)$	AC ⁰	Nisan '91
$\tilde{O}(\log^{d+4} n)$	AC ⁰	Trevisan, Xue '13
$\tilde{O}(\log^{d+1} n)$	Read-once AC ⁰	Chen, Steinke, Vadhan '15
$\tilde{O}(\log^2 n)$	Arbitrary-order width- $O(1)$ ROBPs	Forbes, Kelley '18
$\tilde{O}(\log n)$	Read-once AC ⁰	This work

Starting point: Forbes-Kelley PRG

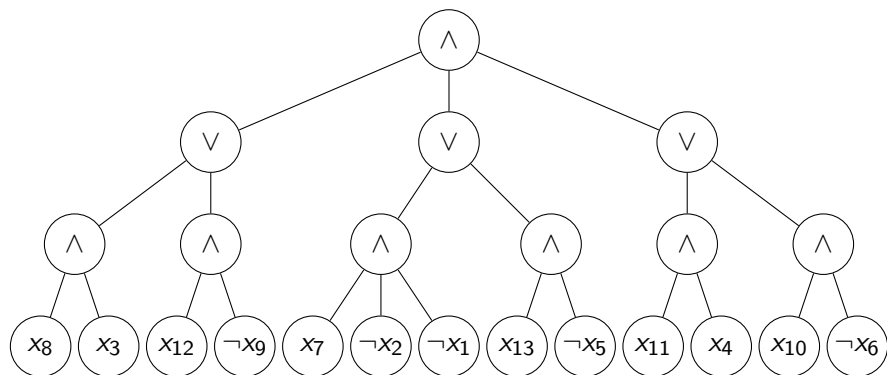
Seed length	Model fooled	Reference
$O(n^{0.001})$	\mathbf{AC}^0	Ajtai, Wigderson '89
$O(\log^{2d+6} n)$	\mathbf{AC}^0	Nisan '91
$\tilde{O}(\log^{d+4} n)$	\mathbf{AC}^0	Trevisan, Xue '13
$\tilde{O}(\log^{d+1} n)$	Read-once \mathbf{AC}^0	Chen, Steinke, Vadhan '15
$\tilde{O}(\log^2 n)$	Arbitrary-order width- $O(1)$ ROBPs	Forbes, Kelley '18
$\tilde{O}(\log n)$	Read-once \mathbf{AC}^0	This work

PRGs via pseudorandom restrictions [AW89]



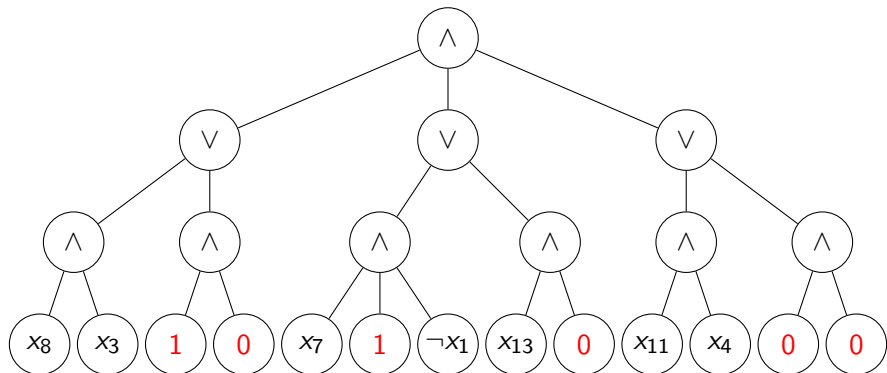
PRGs via pseudorandom restrictions [AW89]

- ▶ Start by sampling a **pseudorandom restriction** $X \in \{0, 1, \star\}^n$



PRGs via pseudorandom restrictions [AW89]

- ▶ Start by sampling a **pseudorandom restriction** $X \in \{0, 1, \star\}^n$



Restriction notation

- ▶ Define Res: $\{0, 1\}^n \times \{0, 1\}^n \rightarrow \{0, 1, \star\}^n$ by

$$\text{Res}(y, z)_i = \begin{cases} \star & \text{if } y_i = 1 \\ z_i & \text{if } y_i = 0 \end{cases}$$

Restriction notation

- Define Res: $\{0, 1\}^n \times \{0, 1\}^n \rightarrow \{0, 1, \star\}^n$ by

$$\text{Res}(y, z)_i = \begin{cases} \star & \text{if } y_i = 1 \\ z_i & \text{if } y_i = 0 \end{cases}$$

$$y = 0 \ 1 \ 1 \ 0 \ 0 \ 1 \ 0 \ 0$$

$$z = 0 \ 0 \ 1 \ 1 \ 1 \ 1 \ 0 \ 1$$

$$\text{Res}(y, z) = 0 \ \star \ \star \ 1 \ 1 \ \star \ 0 \ 1$$

Forbes-Kelley pseudorandom restriction

- ▶ A distribution D over $\{0, 1\}^n$ is ϵ -biased if it fools parities:

$$S \neq \emptyset \implies \left| \mathbb{E} \left[\bigoplus_{i \in S} D_i \right] - \frac{1}{2} \right| \leq \epsilon$$

Forbes-Kelley pseudorandom restriction

- ▶ A distribution D over $\{0, 1\}^n$ is ϵ -biased if it fools parities:

$$S \neq \emptyset \implies \left| \mathbb{E} \left[\bigoplus_{i \in S} D_i \right] - \frac{1}{2} \right| \leq \epsilon$$

- ▶ Let D, D' be independent small-bias strings

Forbes-Kelley pseudorandom restriction

- ▶ A distribution D over $\{0, 1\}^n$ is ϵ -biased if it fools parities:

$$S \neq \emptyset \implies \left| \mathbb{E} \left[\bigoplus_{i \in S} D_i \right] - \frac{1}{2} \right| \leq \epsilon$$

- ▶ Let D, D' be independent small-bias strings
- ▶ Let $X = \text{Res}(D, D')$ (seed length $\tilde{O}(\log n)$)

Forbes-Kelley pseudorandom restriction

- ▶ A distribution D over $\{0, 1\}^n$ is ϵ -biased if it fools parities:

$$S \neq \emptyset \implies \left| \mathbb{E} \left[\bigoplus_{i \in S} D_i \right] - \frac{1}{2} \right| \leq \epsilon$$

- ▶ Let D, D' be independent small-bias strings
- ▶ Let $X = \text{Res}(D, D')$ (seed length $\tilde{O}(\log n)$)
- ▶ **Theorem** [Forbes, Kelley '18]: For any $O(1)$ -width ROBP f ,

$$\mathbb{E}_{X,U} [f|_X(U)] \approx \mathbb{E}_U [f(U)]$$

Forbes-Kelley pseudorandom restriction

- ▶ A distribution D over $\{0, 1\}^n$ is ϵ -biased if it fools parities:

$$S \neq \emptyset \implies \left| \mathbb{E} \left[\bigoplus_{i \in S} D_i \right] - \frac{1}{2} \right| \leq \epsilon$$

- ▶ Let D, D' be independent small-bias strings
- ▶ Let $X = \text{Res}(D, D')$ (seed length $\tilde{O}(\log n)$)
- ▶ **Theorem** [Forbes, Kelley '18]: For any $O(1)$ -width ROBP f ,

$$\mathbb{E}_{X,U} [f|_X(U)] \approx \mathbb{E}_U [f(U)]$$

- ▶ In words, X preserves expectation of f

Forbes-Kelley pseudorandom restriction

- ▶ A distribution D over $\{0, 1\}^n$ is ϵ -biased if it fools parities:

$$S \neq \emptyset \implies \left| \mathbb{E} \left[\bigoplus_{i \in S} D_i \right] - \frac{1}{2} \right| \leq \epsilon$$

- ▶ Let D, D' be independent small-bias strings
- ▶ Let $X = \text{Res}(D, D')$ (seed length $\tilde{O}(\log n)$)
- ▶ **Theorem** [Forbes, Kelley '18]: For any $O(1)$ -width ROBP f ,

$$\mathbb{E}_{X,U} [f|_X(U)] \approx \mathbb{E}_U [f(U)]$$

- ▶ In words, X preserves expectation of f
- ▶ (Proof involves clever Fourier analysis, building on [RSV13, HLV18, CHRT18])

Forbes-Kelley pseudorandom generator

- ▶ So [FK18] can assign values to **half** the inputs using $\tilde{O}(\log n)$ truly random bits

Forbes-Kelley pseudorandom generator

- ▶ So [FK18] can assign values to **half** the inputs using $\tilde{O}(\log n)$ truly random bits
- ▶ After restricting, $f|_X$ is **another ROBP**

Forbes-Kelley pseudorandom generator

- ▶ So [FK18] can assign values to **half** the inputs using $\tilde{O}(\log n)$ truly random bits
- ▶ After restricting, $f|_X$ is **another ROBP**
- ▶ So we can apply **another pseudorandom restriction**

Forbes-Kelley pseudorandom generator

- ▶ So [FK18] can assign values to **half** the inputs using $\tilde{O}(\log n)$ truly random bits
- ▶ After restricting, $f|_X$ is **another ROBP**
- ▶ So we can apply **another pseudorandom restriction**
- ▶ Let $X^{\circ t}$ denote **composition** of t independent copies of X

Forbes-Kelley pseudorandom generator

- ▶ So [FK18] can assign values to **half** the inputs using $\tilde{O}(\log n)$ truly random bits
- ▶ After restricting, $f|_X$ is **another ROBP**
- ▶ So we can apply **another pseudorandom restriction**
- ▶ Let $X^{\circ t}$ denote **composition** of t independent copies of X
- ▶ Let $t = O(\log n)$

Forbes-Kelley pseudorandom generator

- ▶ So [FK18] can assign values to **half** the inputs using $\tilde{O}(\log n)$ truly random bits
- ▶ After restricting, $f|_X$ is **another ROBP**
- ▶ So we can apply **another pseudorandom restriction**
- ▶ Let $X^{\circ t}$ denote **composition** of t independent copies of X
- ▶ Let $t = O(\log n)$
- ▶ With high probability, $X^{\circ t} \in \{0, 1\}^n$ (no \star)

Forbes-Kelley pseudorandom generator

- ▶ So [FK18] can assign values to **half** the inputs using $\tilde{O}(\log n)$ truly random bits
- ▶ After restricting, $f|_X$ is **another ROBP**
- ▶ So we can apply **another pseudorandom restriction**
- ▶ Let $X^{\circ t}$ denote **composition** of t independent copies of X
- ▶ Let $t = O(\log n)$
- ▶ With high probability, $X^{\circ t} \in \{0, 1\}^n$ (no \star)
- ▶ Expectation preserved at every step, so total error is low:

$$\mathbb{E}_{X^{\circ t}}[f(X^{\circ t})] \approx \mathbb{E}_U[f(U)]$$

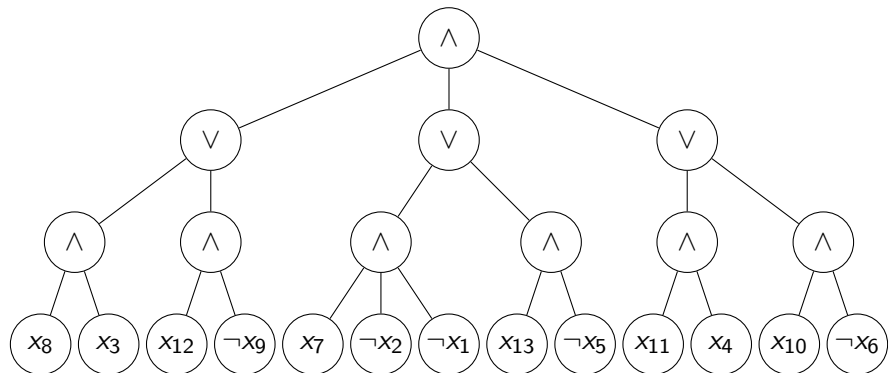
Forbes-Kelley pseudorandom generator

- ▶ So [FK18] can assign values to **half** the inputs using $\tilde{O}(\log n)$ truly random bits
- ▶ After restricting, $f|_X$ is **another ROBP**
- ▶ So we can apply **another pseudorandom restriction**
- ▶ Let $X^{\circ t}$ denote **composition** of t independent copies of X
- ▶ Let $t = O(\log n)$
- ▶ With high probability, $X^{\circ t} \in \{0, 1\}^n$ (no \star)
- ▶ Expectation preserved at every step, so total error is low:

$$\mathbb{E}_{X^{\circ t}}[f(X^{\circ t})] \approx \mathbb{E}_U[f(U)]$$

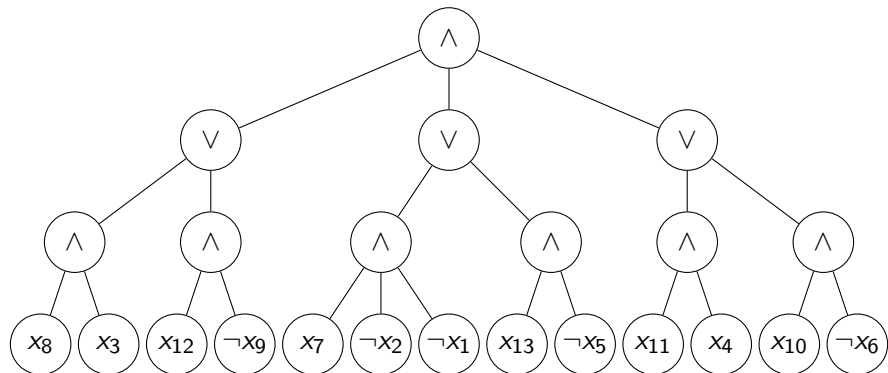
- ▶ Total cost: $\tilde{O}(\log^2 n)$ truly random bits

Improved PRGs via simplification [GMRTV12]



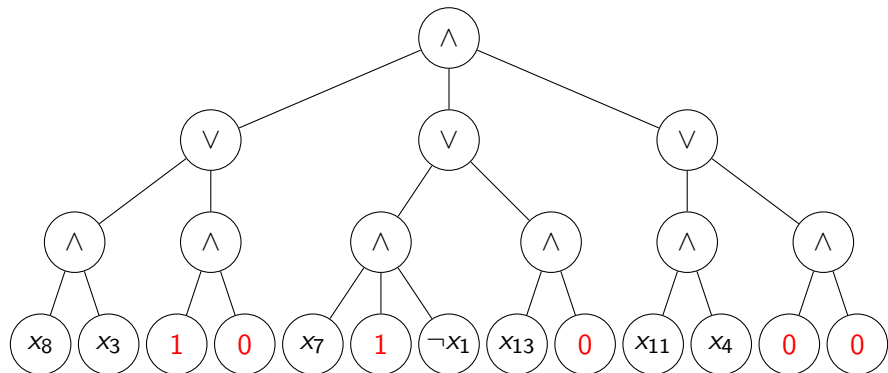
Improved PRGs via simplification [GMRTV12]

- ▶ Step 1: Apply pseudorandom restriction $X \in \{0, 1, \star\}^n$



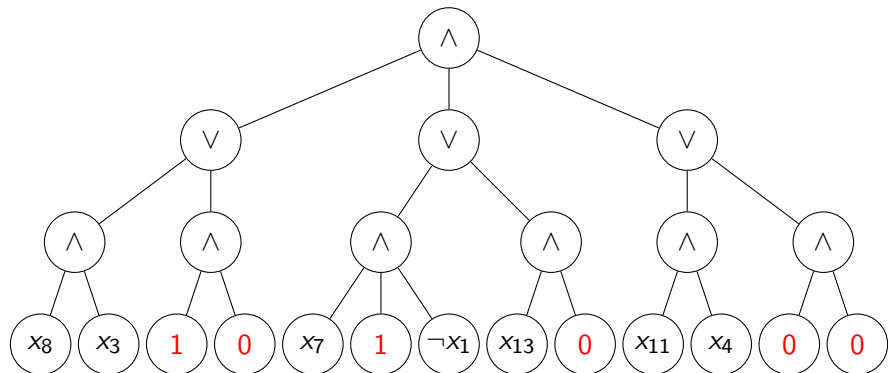
Improved PRGs via simplification [GMRTV12]

- ▶ Step 1: Apply pseudorandom restriction $X \in \{0, 1, \star\}^n$



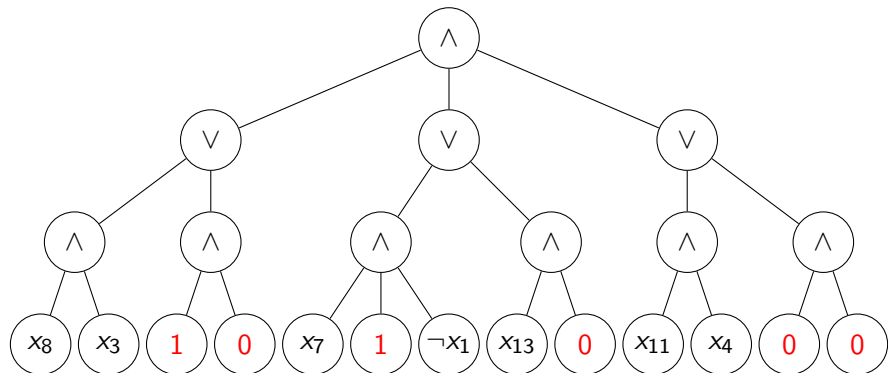
Improved PRGs via simplification [GMRTV12]

- ▶ Step 1: Apply pseudorandom restriction $X \in \{0, 1, \star\}^n$
- ▶ Design X to preserve expectation



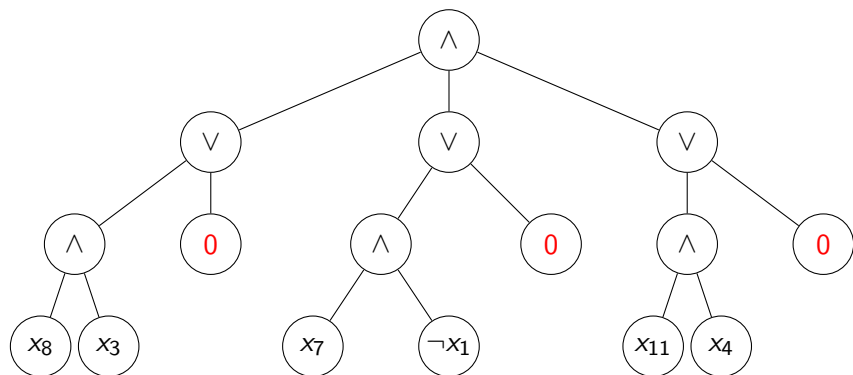
Improved PRGs via simplification [GMRTV12]

- ▶ Step 1: Apply pseudorandom restriction $X \in \{0, 1, \star\}^n$
- ▶ Design X to preserve expectation
- ▶ Design X so that $X^{\circ t}$ also **simplifies** formula, for $t \ll \log n$



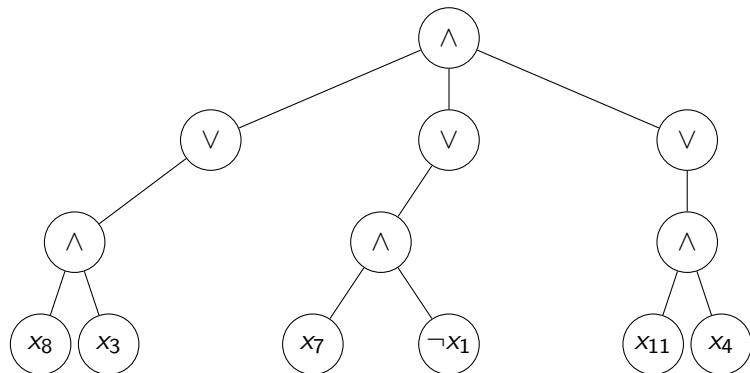
Improved PRGs via simplification [GMRTV12]

- ▶ Step 1: Apply pseudorandom restriction $X \in \{0, 1, \star\}^n$
- ▶ Design X to preserve expectation
- ▶ Design X so that $X^{\circ t}$ also **simplifies** formula, for $t \ll \log n$



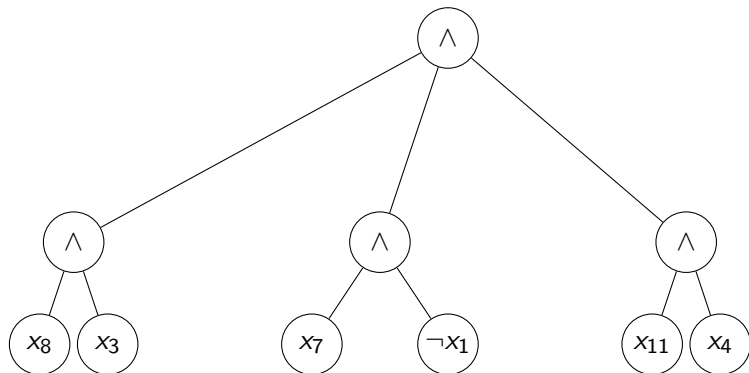
Improved PRGs via simplification [GMRTV12]

- ▶ Step 1: Apply pseudorandom restriction $X \in \{0, 1, \star\}^n$
- ▶ Design X to preserve expectation
- ▶ Design X so that $X^{\circ t}$ also **simplifies** formula, for $t \ll \log n$



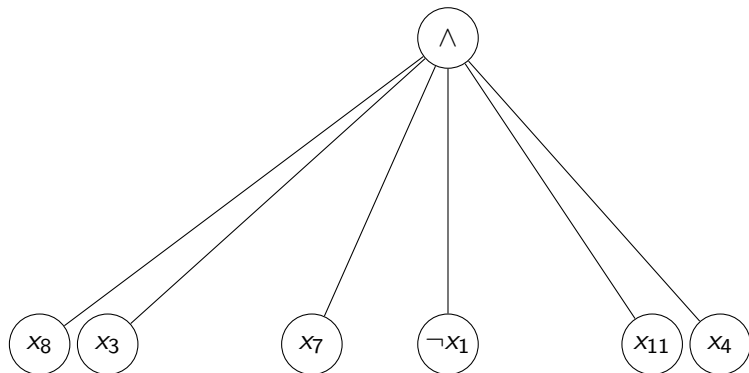
Improved PRGs via simplification [GMRTV12]

- ▶ Step 1: Apply pseudorandom restriction $X \in \{0, 1, \star\}^n$
- ▶ Design X to preserve expectation
- ▶ Design X so that $X^{\circ t}$ also **simplifies** formula, for $t \ll \log n$



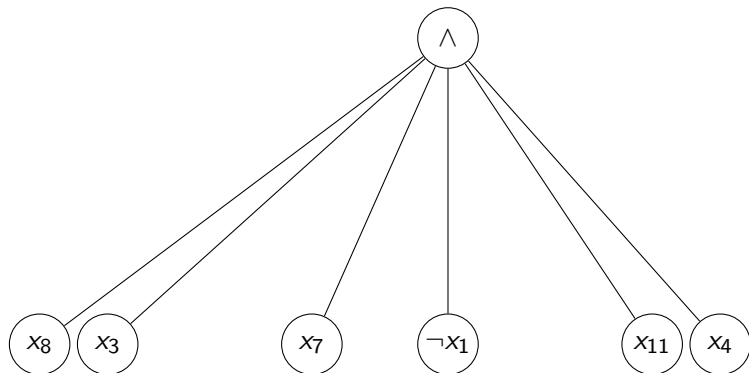
Improved PRGs via simplification [GMRTV12]

- ▶ Step 1: Apply pseudorandom restriction $X \in \{0, 1, \star\}^n$
- ▶ Design X to preserve expectation
- ▶ Design X so that $X^{\circ t}$ also **simplifies** formula, for $t \ll \log n$



Improved PRGs via simplification [GMRTV12]

- ▶ Step 1: Apply pseudorandom restriction $X \in \{0, 1, \star\}^n$
- ▶ Design X to preserve expectation
- ▶ Design X so that $X^{\circ t}$ also **simplifies** formula, for $t \ll \log n$



- ▶ Step 2: Fool restricted formula, **taking advantage of simplicity**

Our pseudorandom restriction

- ▶ Assume by **recursion**: PRG for depth d with seed length $\tilde{O}(\log n)$

Our pseudorandom restriction

- ▶ Assume by **recursion**: PRG for depth d with seed length $\tilde{O}(\log n)$
- ▶ Let's sample $X \in \{0, 1, \star\}^n$ for depth $d + 1$

Our pseudorandom restriction

- ▶ Assume by **recursion**: PRG for depth d with seed length $\tilde{O}(\log n)$
- ▶ Let's sample $X \in \{0, 1, \star\}^n$ for depth $d + 1$

1. Recursively sample $G_d, G'_d \in \{0, 1\}^n$

Our pseudorandom restriction

- ▶ Assume by recursion: PRG for depth d with seed length $\tilde{O}(\log n)$
 - ▶ Let's sample $X \in \{0, 1, \star\}^n$ for depth $d + 1$
1. Recursively sample $G_d, G'_d \in \{0, 1\}^n$
 2. Sample $D, D' \in \{0, 1\}^n$ with small bias

Our pseudorandom restriction

- ▶ Assume by **recursion**: PRG for depth d with seed length $\tilde{O}(\log n)$
 - ▶ Let's sample $X \in \{0, 1, \star\}^n$ for depth $d + 1$
1. Recursively sample $G_d, G'_d \in \{0, 1\}^n$
 2. Sample $D, D' \in \{0, 1\}^n$ with small bias
 3. $X = \text{Res}(G_d \oplus D, G'_d \oplus D')$

Preserving expectation

- ▶ **Claim:** For any depth- $(d + 1)$ read-once \mathbf{AC}^0 formula f ,

$$\mathbb{E}_{X,U}[f|_X(U)] \approx \mathbb{E}_U[f(U)]$$

Preserving expectation

- ▶ **Claim:** For any depth- $(d + 1)$ read-once \mathbf{AC}^0 formula f ,

$$\mathbb{E}_{X,U}[f|_X(U)] \approx \mathbb{E}_U[f(U)]$$

- ▶ **Proof:** Read-once \mathbf{AC}^0 can be simulated by constant-width ROBPs [CSV15]

Preserving expectation

- ▶ **Claim:** For any depth- $(d + 1)$ read-once \mathbf{AC}^0 formula f ,

$$\mathbb{E}_{X,U}[f|_X(U)] \approx \mathbb{E}_U[f(U)]$$

- ▶ **Proof:** Read-once \mathbf{AC}^0 can be simulated by constant-width ROBPs [CSV15]
- ▶ So we can simply apply Forbes-Kelley result:

$$X = \text{Res}(G_d \oplus D, G'_d \oplus D')$$

Simplification

- ▶ $\Delta(f) \stackrel{\text{def}}{=} \text{maximum fan-in of any gate other than root}$

Simplification

- ▶ $\Delta(f) \stackrel{\text{def}}{=} \text{maximum fan-in of any gate other than root}$
- ▶ **Main Lemma:** With high probability over X^{ot} ,

$$\Delta(f|_{X^{ot}}) \leq \text{polylog } n,$$

where $t = O((\log \log n)^2)$

Simplification

- ▶ $\Delta(f) \stackrel{\text{def}}{=} \text{maximum fan-in of any gate other than root}$
- ▶ **Main Lemma:** With high probability over $X^{\otimes t}$,

$$\Delta(f|_{X^{\otimes t}}) \leq \text{polylog } n,$$

where $t = O((\log \log n)^2)$

- ▶ Actually we only prove this statement “up to sandwiching”

$\Delta \mapsto \text{polylog } n$: Proof outline

- ▶ Chen, Steinke, Vadhan '15: Read-once **AC**⁰ simplifies under truly random restrictions

$\Delta \mapsto \text{polylog } n$: Proof outline

- ▶ Chen, Steinke, Vadhan '15: Read-once \mathbf{AC}^0 simplifies under **truly** random restrictions
- ▶ Testing for simplification is **another read-once \mathbf{AC}^0** problem

$\Delta \mapsto \text{polylog } n$: Proof outline

- ▶ Chen, Steinke, Vadhan '15: Read-once \mathbf{AC}^0 simplifies under **truly** random restrictions
- ▶ Testing for simplification is **another read-once \mathbf{AC}^0** problem
- ▶ So we can derandomize the [CSV15] analysis:

$$X = \text{Res}(G_d \oplus D, G'_d \oplus D')$$

Collapse under truly random restrictions

- ▶ Assume f is a **biased** read-once **AC⁰** formula:

$$\mathbb{E}[f] \leq \rho \text{ or } \mathbb{E}[f] \geq 1 - \rho$$

Collapse under truly random restrictions

- ▶ Assume f is a **biased** read-once \mathbf{AC}^0 formula:

$$\mathbb{E}[f] \leq \rho \text{ or } \mathbb{E}[f] \geq 1 - \rho$$

- ▶ Let $R = \text{Res}(U, U')$ (truly random restriction)

Collapse under truly random restrictions

- ▶ Assume f is a **biased** read-once \mathbf{AC}^0 formula:

$$\mathbb{E}[f] \leq \rho \text{ or } \mathbb{E}[f] \geq 1 - \rho$$

- ▶ Let $R = \text{Res}(U, U')$ (truly random restriction)
- ▶ **Theorem** [CSV '15]:

$$\Pr_{R^{os}}[f|_{R^{os}} \text{ nonconstant}] \leq \rho + \frac{1}{n^{100}},$$

where $s = O(\log \log n)$

Collapse under truly random restrictions

- ▶ Assume f is a **biased** read-once \mathbf{AC}^0 formula:

$$\mathbb{E}[f] \leq \rho \text{ or } \mathbb{E}[f] \geq 1 - \rho$$

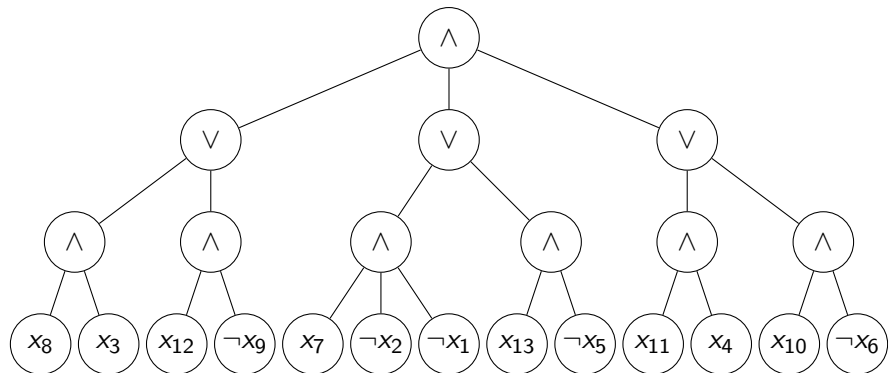
- ▶ Let $R = \text{Res}(U, U')$ (truly random restriction)
- ▶ **Theorem** [CSV '15]:

$$\Pr_{R^{\text{os}}} [f|_{R^{\text{os}}} \text{ nonconstant}] \leq \rho + \frac{1}{n^{100}},$$

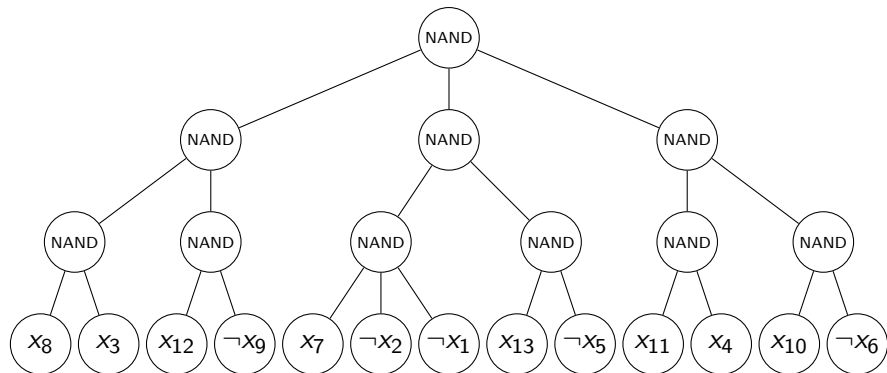
where $s = O(\log \log n)$

- ▶ (Proof uses Fourier analysis)

NAND formulas



NAND formulas



Collapse under truly random restrictions (continued)

► **Corollary:** If $\mathbb{E}[f] \geq 1 - \rho$, then

$$\Pr_{R^{\text{os}}}[f|_{R^{\text{os}}} \neq 1] \leq 2\rho + \frac{1}{n^{100}}$$

Collapse under truly random restrictions (continued)

- ▶ **Corollary:** If $\mathbb{E}[f] \geq 1 - \rho$, then

$$\Pr_{R^{os}}[f|_{R^{os}} \neq 1] \leq 2\rho + \frac{1}{n^{100}}$$

- ▶ Let \mathcal{F} be a **set** of formulas on disjoint variable sets

Collapse under truly random restrictions (continued)

- ▶ **Corollary:** If $\mathbb{E}[f] \geq 1 - \rho$, then

$$\Pr_{R^{\text{os}}}[f|_{R^{\text{os}}} \neq 1] \leq 2\rho + \frac{1}{n^{100}}$$

- ▶ Let \mathcal{F} be a **set** of formulas on disjoint variable sets
- ▶ Assume $\forall f \in \mathcal{F}, \mathbb{E}[f] \geq 1 - \rho$

Collapse under truly random restrictions (continued)

- ▶ **Corollary:** If $\mathbb{E}[f] \geq 1 - \rho$, then

$$\Pr_{R^{os}}[f|_{R^{os}} \neq 1] \leq 2\rho + \frac{1}{n^{100}}$$

- ▶ Let \mathcal{F} be a **set** of formulas on disjoint variable sets
- ▶ Assume $\forall f \in \mathcal{F}, \mathbb{E}[f] \geq 1 - \rho$
- ▶ **Corollary:**

$$\Pr_{R^{os}}[\forall f \in \mathcal{F}, f|_{R^{os}} \neq 1] \leq \left(2\rho + \frac{1}{n^{100}}\right)^{|\mathcal{F}|}.$$

Derandomizing collapse

- ▶ Let \mathcal{F} be a set of depth- $(d - 1)$ formulas on disjoint variables

Derandomizing collapse

- ▶ Let \mathcal{F} be a set of depth- $(d - 1)$ formulas on disjoint variables
- ▶ Computational problem: Given $y, z \in \{0, 1\}^n$, decide whether

$$\exists f \in \mathcal{F}, f|_{\text{Res}(y,z)} \equiv 1$$

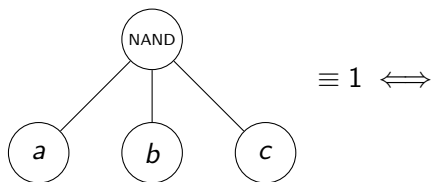
Derandomizing collapse

- ▶ Let \mathcal{F} be a set of depth- $(d - 1)$ formulas on disjoint variables
- ▶ Computational problem: Given $y, z \in \{0, 1\}^n$, decide whether

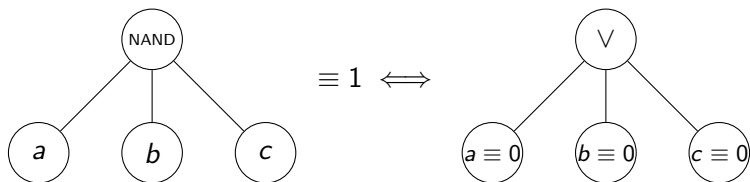
$$\exists f \in \mathcal{F}, f|_{\text{Res}(y,z)} \equiv 1$$

- ▶ **Lemma:** Can be decided in **depth- d read-once \mathbf{AC}^0**

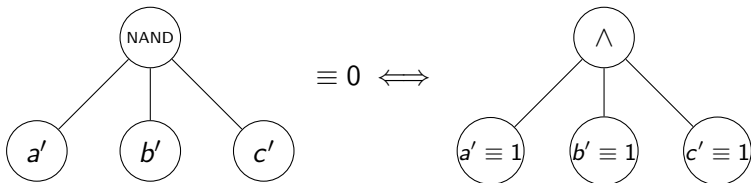
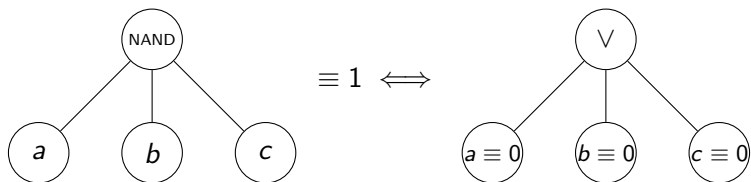
Deciding whether $\exists f \in \mathcal{F}, f|_{\text{Res}(y,z)} \equiv 1$



Deciding whether $\exists f \in \mathcal{F}, f|_{\text{Res}(y,z)} \equiv 1$



Deciding whether $\exists f \in \mathcal{F}, f|_{\text{Res}(y,z)} \equiv 1$



Deciding whether $\exists f \in \mathcal{F}, f|_{\text{Res}(y,z)} \equiv 1$ (continued)

- ▶ At bottom, we get one additional layer:

$$(\text{Res}(y, z)_i \equiv b) \iff (y_i = 0 \wedge z_i = b)$$

$$(\neg \text{Res}(y, z)_i \equiv b) \iff (y_i = 0 \wedge z_i = 1 - b)$$

Deciding whether $\exists f \in \mathcal{F}, f|_{\text{Res}(y,z)} \equiv 1$ (continued)

- ▶ At bottom, we get one additional layer:

$$(\text{Res}(y, z)_i \equiv b) \iff (y_i = 0 \wedge z_i = b)$$

$$(\neg \text{Res}(y, z)_i \equiv b) \iff (y_i = 0 \wedge z_i = 1 - b)$$

- ▶ At top: “ $\exists f \in \mathcal{F}$ ” is one more \vee gate (merge with top \vee gates)

Collapse under pseudorandom restrictions

- ▶ Let \mathcal{F} be a set of depth- $(d - 1)$ formulas on disjoint variables
- ▶ Assume $\forall f \in \mathcal{F}, \mathbb{E}[f] \geq 1 - \rho$

Collapse under pseudorandom restrictions

- ▶ Let \mathcal{F} be a set of depth- $(d - 1)$ formulas on disjoint variables
- ▶ Assume $\forall f \in \mathcal{F}, \mathbb{E}[f] \geq 1 - \rho$
- ▶ $X = \text{Res}(G_d \oplus D, G'_d \oplus D')$

Collapse under pseudorandom restrictions

- ▶ Let \mathcal{F} be a set of depth- $(d - 1)$ formulas on disjoint variables
- ▶ Assume $\forall f \in \mathcal{F}, \mathbb{E}[f] \geq 1 - \rho$
- ▶ $X = \text{Res}(G_d \oplus D, G'_d \oplus D')$
- ▶ G_d, G'_d fool depth d , so

$$\Pr_X[\forall f \in \mathcal{F}, f|_X \neq 1] \approx \Pr_R[\forall f \in \mathcal{F}, f|_R \neq 1]$$

Collapse under pseudorandom restrictions

- ▶ Let \mathcal{F} be a set of depth- $(d - 1)$ formulas on disjoint variables
- ▶ Assume $\forall f \in \mathcal{F}, \mathbb{E}[f] \geq 1 - \rho$
- ▶ $X = \text{Res}(G_d \oplus D, G'_d \oplus D')$
- ▶ G_d, G'_d fool depth d , so

$$\Pr_{X^{\text{os}}}[\forall f \in \mathcal{F}, f|_X \neq 1] \approx \Pr_{R^{\text{os}}}[\forall f \in \mathcal{F}, f|_R \neq 1]$$

- ▶ Hybrid argument:

$$\Pr_{X^{\text{os}}}[\forall f \in \mathcal{F}, f|_{X^{\text{os}}} \neq 1] \approx \Pr_{R^{\text{os}}}[\forall f \in \mathcal{F}, f|_{R^{\text{os}}} \neq 1]$$

Collapse under pseudorandom restrictions

- ▶ Let \mathcal{F} be a set of depth- $(d - 1)$ formulas on disjoint variables
- ▶ Assume $\forall f \in \mathcal{F}, \mathbb{E}[f] \geq 1 - \rho$
- ▶ $X = \text{Res}(G_d \oplus D, G'_d \oplus D')$
- ▶ G_d, G'_d fool depth d , so

$$\Pr_X[\forall f \in \mathcal{F}, f|_X \neq 1] \approx \Pr_R[\forall f \in \mathcal{F}, f|_R \neq 1]$$

- ▶ Hybrid argument:

$$\begin{aligned} \Pr_{X^{os}}[\forall f \in \mathcal{F}, f|_{X^{os}} \neq 1] &\approx \Pr_{R^{os}}[\forall f \in \mathcal{F}, f|_{R^{os}} \neq 1] \\ &\leq \left(2\rho + \frac{1}{n^{100}}\right)^{|\mathcal{F}|} \end{aligned}$$

$$\Delta \mapsto \sqrt{\Delta} \text{polylog } n$$

- ▶ So far: X^{os} causes any **biased** depth- $(d-1)$ formula to collapse

$$\Delta \mapsto \sqrt{\Delta} \text{polylog } n$$

- ▶ So far: $X^{\circ s}$ causes any **biased** depth- $(d - 1)$ formula to collapse
- ▶ What about **unbiased** depth- $(d + 1)$ formulas?

$$\Delta \mapsto \sqrt{\Delta} \text{polylog } n$$

- ▶ So far: $X^{\circ s}$ causes any **biased** depth- $(d - 1)$ formula to collapse
- ▶ What about **unbiased** depth- $(d + 1)$ formulas?

- ▶ Assume that for every gate g in f , $\mathbb{E}[\neg g] \geq 1/\text{poly}(n)$

$$\Delta \mapsto \sqrt{\Delta} \text{polylog } n$$

- ▶ So far: X^{os} causes any **biased** depth- $(d - 1)$ formula to collapse
- ▶ What about **unbiased** depth- $(d + 1)$ formulas?

- ▶ Assume that for every gate g in f , $\mathbb{E}[\neg g] \geq 1/\text{poly}(n)$
- ▶ **Lemma:** With high probability over X^{os} ,

$$\Delta(f|_{X^{\text{os}}}) \leq \sqrt{\Delta(f)} \cdot \text{polylog } n$$

Illustration: $\Delta \mapsto \sqrt{\Delta}$ polylog n

Total depth $d + 1$

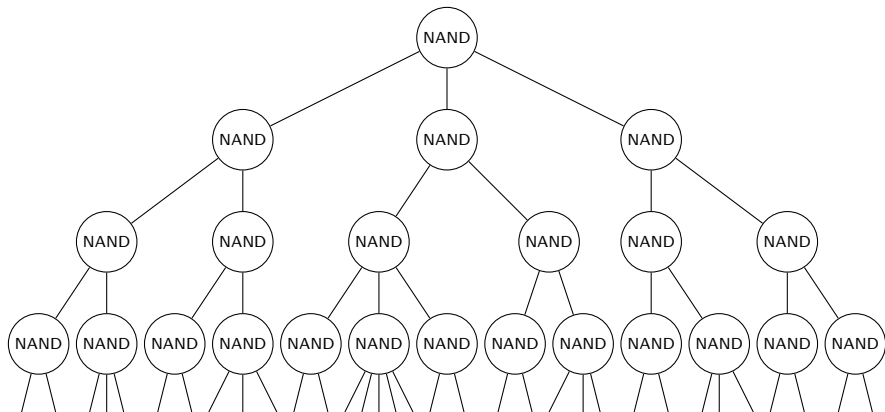


Illustration: $\Delta \mapsto \sqrt{\Delta}$ polylog n

Total depth $d + 1$

Likely to collapse
if biased

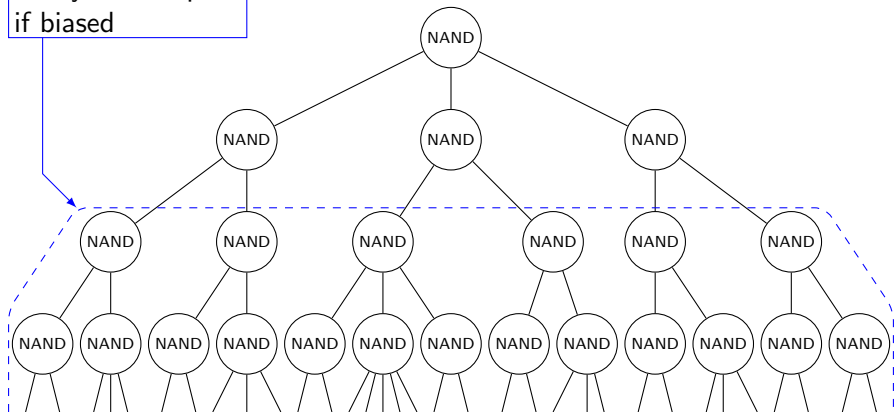
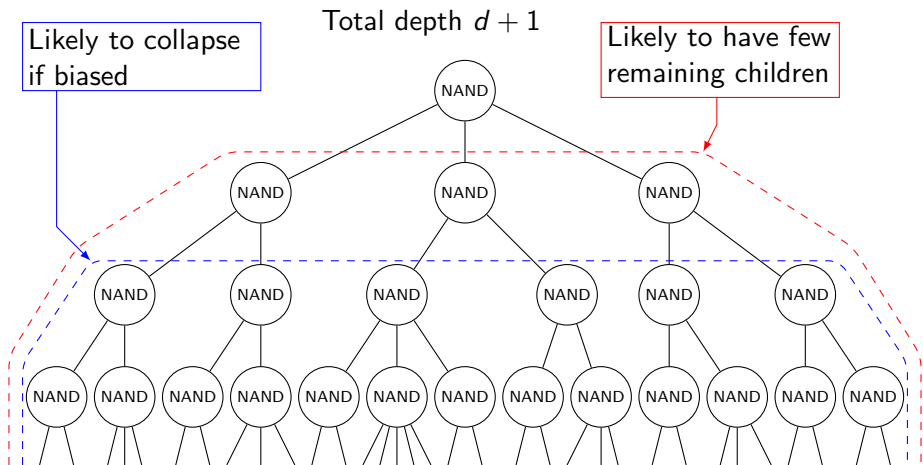


Illustration: $\Delta \mapsto \sqrt{\Delta}$ polylog n



Proof that $\Delta \mapsto \sqrt{\Delta} \text{polylog } n$

- ▶ (This analysis follows [GMRTV12, CSV15])

Proof that $\Delta \mapsto \sqrt{\Delta} \text{polylog } n$

- ▶ (This analysis follows [GMRTV12, CSV15])
- ▶ Let g be a gate, $g \neq \text{root}$

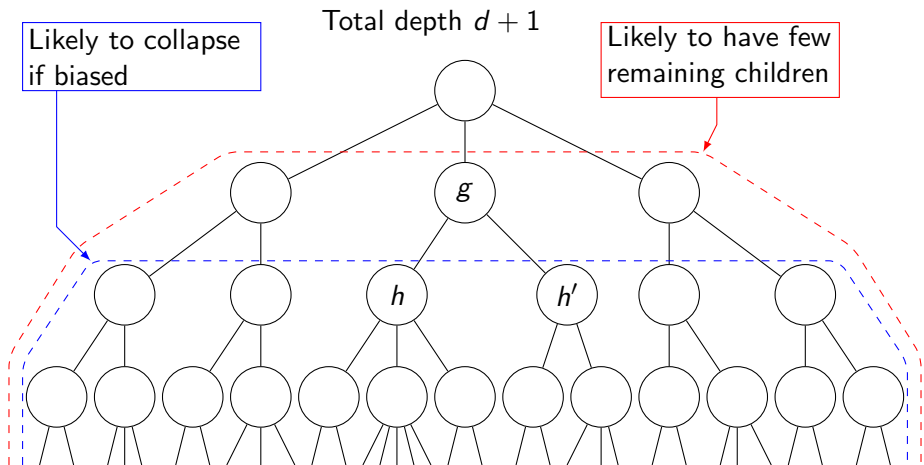
Proof that $\Delta \mapsto \sqrt{\Delta} \text{polylog } n$

- ▶ (This analysis follows [GMRTV12, CSV15])
- ▶ Let g be a gate, $g \neq \text{root}$
- ▶ Partition children h into $O(\log n)$ buckets based on $\mathbb{E}[h]$

Proof that $\Delta \mapsto \sqrt{\Delta} \text{polylog } n$

- ▶ (This analysis follows [GMRTV12, CSV15])
- ▶ Let g be a gate, $g \neq \text{root}$
- ▶ Partition children h into $O(\log n)$ buckets based on $\mathbb{E}[h]$
- ▶ Consider one bucket $\mathcal{B} = \{h : \mathbb{E}[h] \approx 1 - \rho\}$

Illustration: $\Delta \mapsto \sqrt{\Delta}$ polylog n (continued)



Proof that $\Delta \mapsto \sqrt{\Delta} \text{polylog } n$ (continued)

► $\mathcal{B} = \{h : \mathbb{E}[h] \approx 1 - \rho\}$

Proof that $\Delta \mapsto \sqrt{\Delta} \text{polylog } n$ (continued)

- ▶ $\mathcal{B} = \{h : \mathbb{E}[h] \approx 1 - \rho\}$
- ▶ How big can \mathcal{B} be?

Proof that $\Delta \mapsto \sqrt{\Delta} \text{polylog } n$ (continued)

▶ $\mathcal{B} = \{h : \mathbb{E}[h] \approx 1 - \rho\}$

▶ How big can \mathcal{B} be?



$$1/\text{poly}(n) \leq \mathbb{E}[\neg g]$$

Proof that $\Delta \mapsto \sqrt{\Delta}$ polylog n (continued)

▶ $\mathcal{B} = \{h : \mathbb{E}[h] \approx 1 - \rho\}$

▶ How big can \mathcal{B} be?



$$1/\text{poly}(n) \leq \mathbb{E}[\neg g] \leq \prod_{h \in \mathcal{B}} \mathbb{E}[h]$$

Proof that $\Delta \mapsto \sqrt{\Delta}$ polylog n (continued)

▶ $\mathcal{B} = \{h : \mathbb{E}[h] \approx 1 - \rho\}$

▶ How big can \mathcal{B} be?



$$1/\text{poly}(n) \leq \mathbb{E}[\neg g] \leq \prod_{h \in \mathcal{B}} \mathbb{E}[h] \approx (1 - \rho)^{|\mathcal{B}|}$$

Proof that $\Delta \mapsto \sqrt{\Delta} \text{polylog } n$ (continued)

▶ $\mathcal{B} = \{h : \mathbb{E}[h] \approx 1 - \rho\}$

▶ How big can \mathcal{B} be?



$$1/\text{poly}(n) \leq \mathbb{E}[\neg g] \leq \prod_{h \in \mathcal{B}} \mathbb{E}[h] \approx (1 - \rho)^{|\mathcal{B}|}$$

▶ So $|\mathcal{B}| \leq O((1/\rho) \log n)$

Proof that $\Delta \mapsto \sqrt{\Delta}$ polylog n (continued)

▶ $\mathcal{B} = \{h : \mathbb{E}[h] \approx 1 - \rho\}$

▶ How big can \mathcal{B} be?

▶

$$1/\text{poly}(n) \leq \mathbb{E}[\neg g] \leq \prod_{h \in \mathcal{B}} \mathbb{E}[h] \approx (1 - \rho)^{|\mathcal{B}|}$$

▶ So $|\mathcal{B}| \leq O((1/\rho) \log n)$

▶ We also trivially have $|\mathcal{B}| \leq \Delta$

Proof that $\Delta \mapsto \sqrt{\Delta} \text{polylog } n$ (continued)

- ▶ Let $L = \#\{h \in \mathcal{B} : h|_{X^{os}} \neq 1\}$ (number of **living** children)

Proof that $\Delta \mapsto \sqrt{\Delta} \text{polylog } n$ (continued)

- ▶ Let $L = \#\{h \in \mathcal{B} : h|_{X^{os}} \neq 1\}$ (number of **living** children)
- ▶ Let $M = \Theta(\sqrt{\Delta} \log n)$

Proof that $\Delta \mapsto \sqrt{\Delta} \text{polylog } n$ (continued)

- ▶ Let $L = \#\{h \in \mathcal{B} : h|_{X^{os}} \neq 1\}$ (number of **living** children)
- ▶ Let $M = \Theta(\sqrt{\Delta} \log n)$
- ▶ $\Pr[L \geq M] =$

Proof that $\Delta \mapsto \sqrt{\Delta} \text{polylog } n$ (continued)

- ▶ Let $L = \#\{h \in \mathcal{B} : h|_{X^{os}} \neq 1\}$ (number of **living** children)
- ▶ Let $M = \Theta(\sqrt{\Delta} \log n)$, $k =$
- ▶ $\Pr[L \geq M] = \Pr \left[\binom{L}{k} \geq \binom{M}{k} \right]$ Pascal

Proof that $\Delta \mapsto \sqrt{\Delta} \text{polylog } n$ (continued)

▶ Let $L = \#\{h \in \mathcal{B} : h|_{X^{os}} \neq 1\}$ (number of **living** children)

▶ Let $M = \Theta(\sqrt{\Delta} \log n)$, $k =$

▶ $\Pr[L \geq M] = \Pr \left[\binom{L}{k} \geq \binom{M}{k} \right]$ Pascal

$$\leq \frac{1}{\binom{M}{k}} \cdot \mathbb{E} \left[\binom{L}{k} \right]$$

Markov

Proof that $\Delta \mapsto \sqrt{\Delta}$ polylog n (continued)

► Let $L = \#\{h \in \mathcal{B} : h|_{X^{os}} \neq 1\}$ (number of **living** children)

► Let $M = \Theta(\sqrt{\Delta} \log n)$, $k =$

► $\Pr[L \geq M] = \Pr \left[\binom{L}{k} \geq \binom{M}{k} \right]$ Pascal

$$\leq \frac{1}{\binom{M}{k}} \cdot \mathbb{E} \left[\binom{L}{k} \right]$$
Markov

$$\leq \frac{1}{\binom{M}{k}} \cdot \binom{|\mathcal{B}|}{k} \cdot \left(O(\rho)^k + \frac{1}{n^{200}} \right)$$

Proof that $\Delta \mapsto \sqrt{\Delta} \text{polylog } n$ (continued)

► Let $L = \#\{h \in \mathcal{B} : h|_{X^{\text{os}}} \neq 1\}$ (number of **living** children)

► Let $M = \Theta(\sqrt{\Delta} \log n)$, $k =$

$$\begin{aligned} \text{► } \Pr[L \geq M] &= \Pr \left[\binom{L}{k} \geq \binom{M}{k} \right] && \text{Pascal} \\ &\leq \frac{1}{\binom{M}{k}} \cdot \mathbb{E} \left[\binom{L}{k} \right] && \text{Markov} \\ &\leq \frac{1}{\binom{M}{k}} \cdot \binom{|\mathcal{B}|}{k} \cdot \left(O(\rho)^k + \frac{1}{n^{200}} \right) \\ &\leq \left(\frac{|\mathcal{B}|e}{M} \right)^k \cdot \left(O(\rho)^k + \frac{1}{n^{200}} \right) && \text{Stirling} \end{aligned}$$

Proof that $\Delta \mapsto \sqrt{\Delta}$ polylog n (continued)

► Let $L = \#\{h \in \mathcal{B} : h|_{X^{os}} \neq 1\}$ (number of living children)

► Let $M = \Theta(\sqrt{\Delta} \log n)$, $k =$

► $\Pr[L \geq M] = \Pr\left[\binom{L}{k} \geq \binom{M}{k}\right]$ Pascal

$$\leq \frac{1}{\binom{M}{k}} \cdot \mathbb{E}\left[\binom{L}{k}\right]$$
Markov

$$\leq \frac{1}{\binom{M}{k}} \cdot \binom{|\mathcal{B}|}{k} \cdot \left(O(\rho)^k + \frac{1}{n^{200}}\right)$$

$$\leq \left(\frac{|\mathcal{B}|e}{M}\right)^k \cdot \left(O(\rho)^k + \frac{1}{n^{200}}\right)$$
Stirling

$$\leq \left(\frac{1}{\sqrt{\Delta}}\right)^k +$$

Proof that $\Delta \mapsto \sqrt{\Delta}$ polylog n (continued)

▶ Let $L = \#\{h \in \mathcal{B} : h|_{X^{os}} \neq 1\}$ (number of living children)

▶ Let $M = \Theta(\sqrt{\Delta} \log n)$, $k =$

▶ $\Pr[L \geq M] = \Pr \left[\binom{L}{k} \geq \binom{M}{k} \right]$ Pascal

$$\leq \frac{1}{\binom{M}{k}} \cdot \mathbb{E} \left[\binom{L}{k} \right]$$
Markov

$$\leq \frac{1}{\binom{M}{k}} \cdot \binom{|\mathcal{B}|}{k} \cdot \left(O(\rho)^k + \frac{1}{n^{200}} \right)$$

$$\leq \left(\frac{|\mathcal{B}|e}{M} \right)^k \cdot \left(O(\rho)^k + \frac{1}{n^{200}} \right)$$
Stirling

$$\leq \left(\frac{1}{\sqrt{\Delta}} \right)^k + \frac{1}{n^{200}} \cdot (\sqrt{\Delta})^k$$

Proof that $\Delta \mapsto \sqrt{\Delta}$ polylog n (continued)

▶ Let $L = \#\{h \in \mathcal{B} : h|_{X^{\text{os}}} \neq 1\}$ (number of living children)

▶ Let $M = \Theta(\sqrt{\Delta} \log n)$, $k = \Theta((\log n)/\log \Delta)$

▶ $\Pr[L \geq M] = \Pr\left[\binom{L}{k} \geq \binom{M}{k}\right]$ Pascal

$$\leq \frac{1}{\binom{M}{k}} \cdot \mathbb{E}\left[\binom{L}{k}\right]$$
Markov

$$\leq \frac{1}{\binom{M}{k}} \cdot \binom{|\mathcal{B}|}{k} \cdot \left(O(\rho)^k + \frac{1}{n^{200}}\right)$$

$$\leq \left(\frac{|\mathcal{B}|e}{M}\right)^k \cdot \left(O(\rho)^k + \frac{1}{n^{200}}\right)$$
Stirling

$$\leq \left(\frac{1}{\sqrt{\Delta}}\right)^k + \frac{1}{n^{200}} \cdot (\sqrt{\Delta})^k$$

$$\leq \frac{2}{n^{100}}$$

□

Finishing proof of main lemma

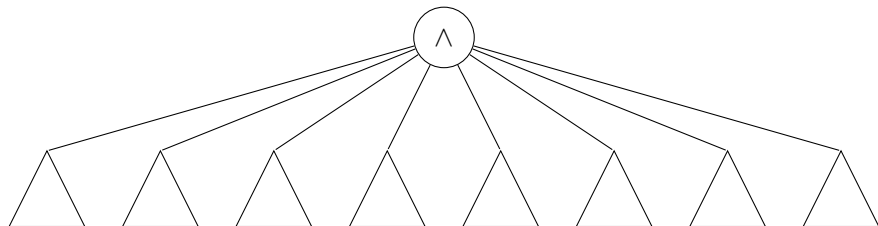
- ▶ After $s = O(\log \log n)$ restrictions, $\Delta \mapsto \sqrt{\Delta} \cdot \text{polylog } n$

Finishing proof of main lemma

- ▶ After $s = O(\log \log n)$ restrictions, $\Delta \mapsto \sqrt{\Delta} \cdot \text{polylog } n$
- ▶ Therefore, after $t = O((\log \log n)^2)$ restrictions, $\Delta = \text{polylog } n$

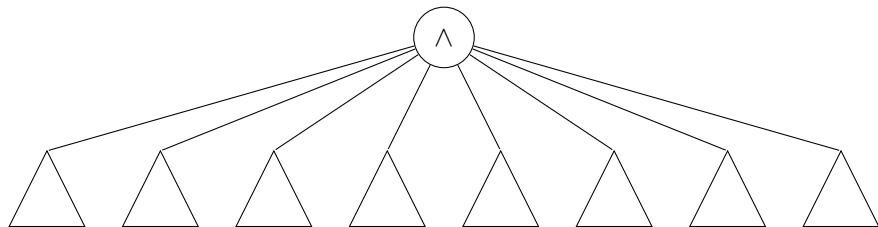
Finishing proof of main lemma

- ▶ After $s = O(\log \log n)$ restrictions, $\Delta \mapsto \sqrt{\Delta} \cdot \text{polylog } n$
- ▶ Therefore, after $t = O((\log \log n)^2)$ restrictions, $\Delta = \text{polylog } n$



Finishing proof of main lemma

- ▶ After $s = O(\log \log n)$ restrictions, $\Delta \mapsto \sqrt{\Delta} \cdot \text{polylog } n$
- ▶ Therefore, after $t = O((\log \log n)^2)$ restrictions, $\Delta = \text{polylog } n$
- ▶ Total cost so far: $\tilde{O}(\log n)$ truly random bits



Final step: MRT PRG

- ▶ **Theorem** (Meka, Reingold, Tal '19): There is an explicit PRG with seed length $\tilde{O}(\log(n/\varepsilon))$ that fools functions of the form

$$f = \bigoplus_{i=1}^m f_i,$$

Final step: MRT PRG

- ▶ **Theorem** (Meka, Reingold, Tal '19): There is an explicit PRG with seed length $\tilde{O}(\log(n/\varepsilon))$ that fools functions of the form

$$f = \bigoplus_{i=1}^m f_i,$$

where f_1, \dots, f_m are on disjoint variables and f_i can be computed by an ROBP with width $O(1)$, length polylog n

Final step: MRT PRG

- ▶ **Theorem** (Meka, Reingold, Tal '19): There is an explicit PRG with seed length $\tilde{O}(\log(n/\varepsilon))$ that fools functions of the form

$$f = \bigoplus_{i=1}^m f_i,$$

where f_1, \dots, f_m are on disjoint variables and f_i can be computed by an ROBP with width $O(1)$, length polylog n

- ▶ (Proof uses GMRTV approach, building on [GY14, CHRT18, Vio09])

Final step: MRT PRG

- ▶ **Theorem** (Meka, Reingold, Tal '19): There is an explicit PRG with seed length $\tilde{O}(\log(n/\varepsilon))$ that fools functions of the form

$$f = \bigoplus_{i=1}^m f_i,$$

where f_1, \dots, f_m are on disjoint variables and f_i can be computed by an ROBP with width $O(1)$, length polylog n

- ▶ (Proof uses GMRTV approach, building on [GY14, CHRT18, Vio09])
- ▶ In our case,

$$f = \bigwedge_{i=1}^m f_i$$

Final step: MRT PRG

- ▶ **Theorem** (Meka, Reingold, Tal '19): There is an explicit PRG with seed length $\tilde{O}(\log(n/\varepsilon))$ that fools functions of the form

$$f = \bigoplus_{i=1}^m f_i,$$

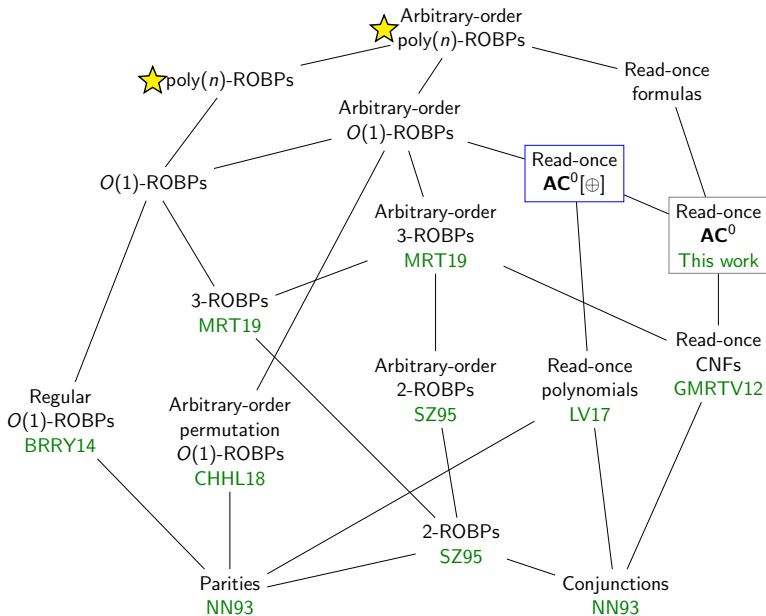
where f_1, \dots, f_m are on disjoint variables and f_i can be computed by an ROBP with width $O(1)$, length polylog n

- ▶ (Proof uses GMRTV approach, building on [GY14, CHRT18, Vio09])
- ▶ In our case,

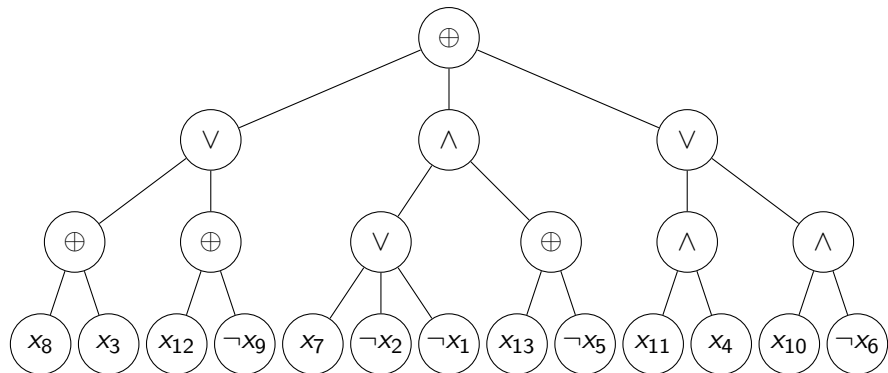
$$f = \bigwedge_{i=1}^m f_i = \sum_{S \subseteq [m]} \frac{(-1)^{|S|}}{2^m} \prod_{i \in S} (-1)^{f_i}$$

Directions for further research

Directions for further research



Read-once $AC^0[\oplus]$



Fooling read-once $\mathbf{AC}^0[\oplus]$

- ▶ Natural next step toward derandomizing **BPL**

Fooling read-once $\mathbf{AC}^0[\oplus]$

- ▶ Natural next step toward derandomizing **BPL**
- ▶ Best prior PRG: seed length $\tilde{O}(\log^2 n)$ [FK '18]

Fooling read-once $\mathbf{AC}^0[\oplus]$

- ▶ Natural next step toward derandomizing **BPL**
- ▶ Best prior PRG: seed length $\tilde{O}(\log^2 n)$ [FK '18]
- ▶ **Theorem:** Our PRG fools read-once $\mathbf{AC}^0[\oplus]$ with seed length

$$\tilde{O}(t + \log(n/\varepsilon))$$

where $t = \#$ parity gates

Fooling read-once $\mathbf{AC}^0[\oplus]$

- ▶ Natural next step toward derandomizing **BPL**
- ▶ Best prior PRG: seed length $\tilde{O}(\log^2 n)$ [FK '18]
- ▶ **Theorem:** Our PRG fools read-once $\mathbf{AC}^0[\oplus]$ with seed length

$$\tilde{O}(t + \log(n/\varepsilon))$$

where $t = \#$ parity gates

- ▶ Fool read-once $\mathbf{AC}^0[\oplus]$ with seed length $\tilde{O}(\log(n/\varepsilon))$?

Fooling read-once $\mathbf{AC}^0[\oplus]$

- ▶ Natural next step toward derandomizing **BPL**
- ▶ Best prior PRG: seed length $\tilde{O}(\log^2 n)$ [FK '18]
- ▶ **Theorem:** Our PRG fools read-once $\mathbf{AC}^0[\oplus]$ with seed length

$$\tilde{O}(t + \log(n/\varepsilon))$$

where $t = \#$ parity gates

- ▶ Fool read-once $\mathbf{AC}^0[\oplus]$ with seed length $\tilde{O}(\log(n/\varepsilon))$?
- ▶ Thanks! Questions?