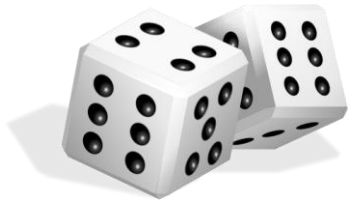
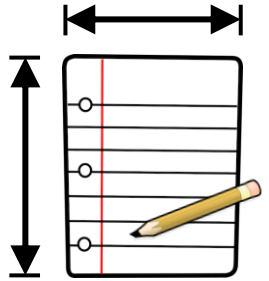
Tutorial: Derandomizing Space-Bounded Computation

Part 2

September 2, 2026



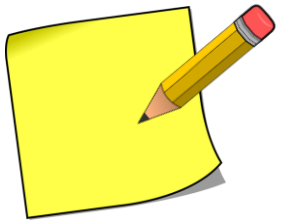


William Hoza
The University of Chicago

The complexity class BPL



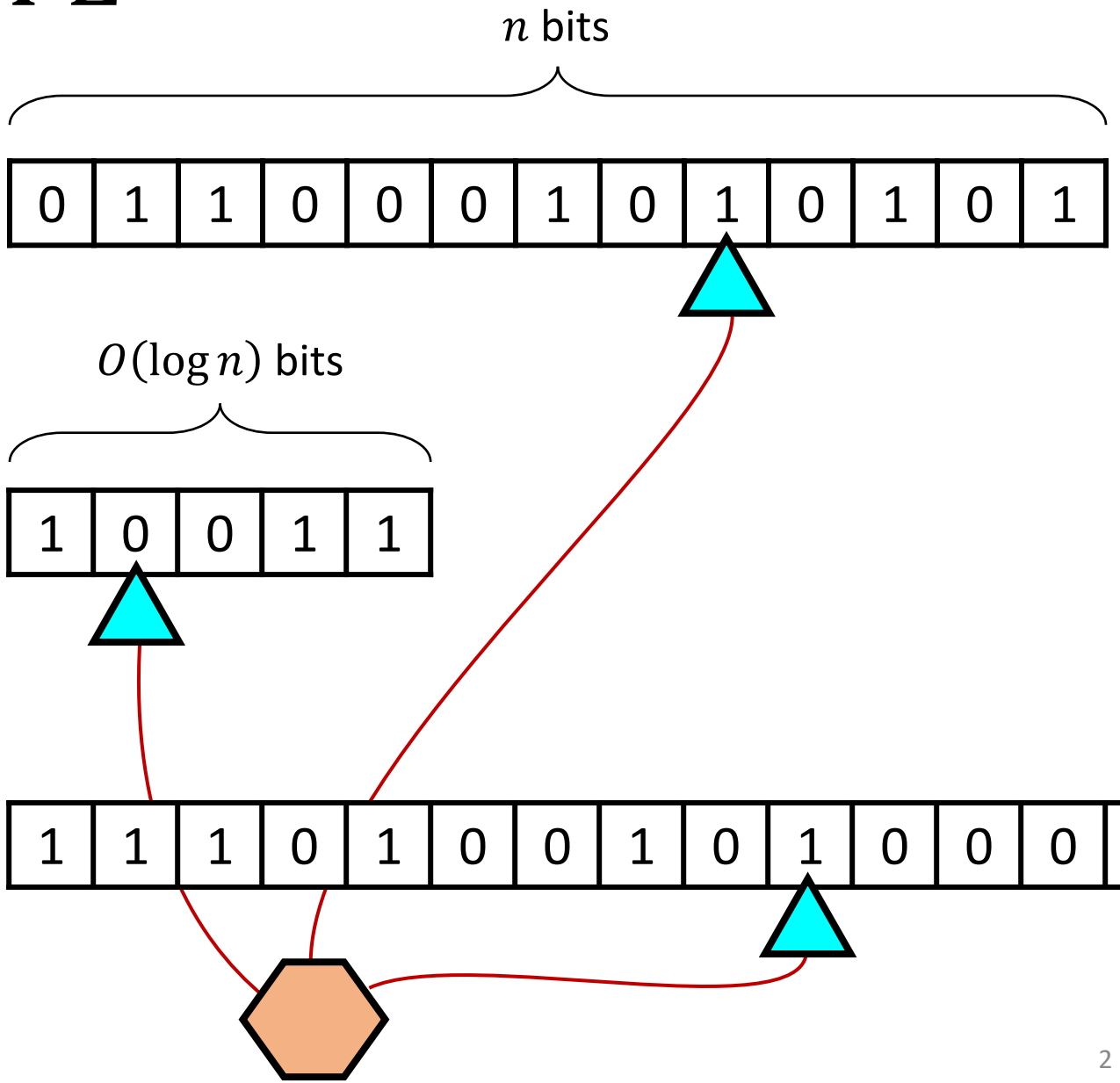
Read-only input tape



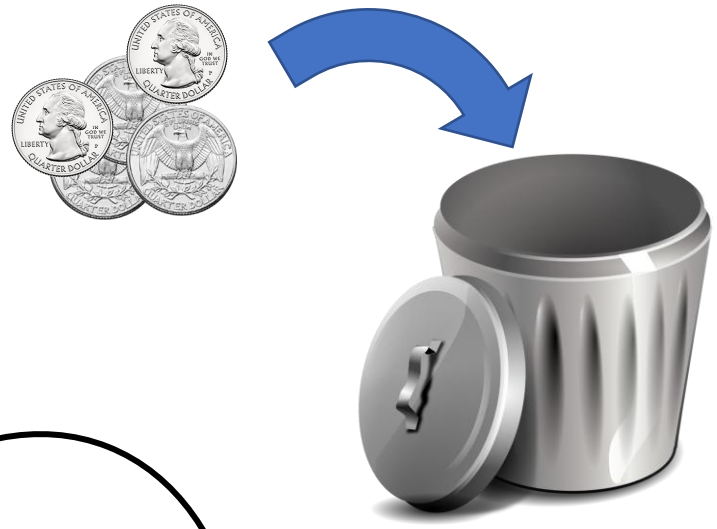
Read-write work tape



Read-once random tape



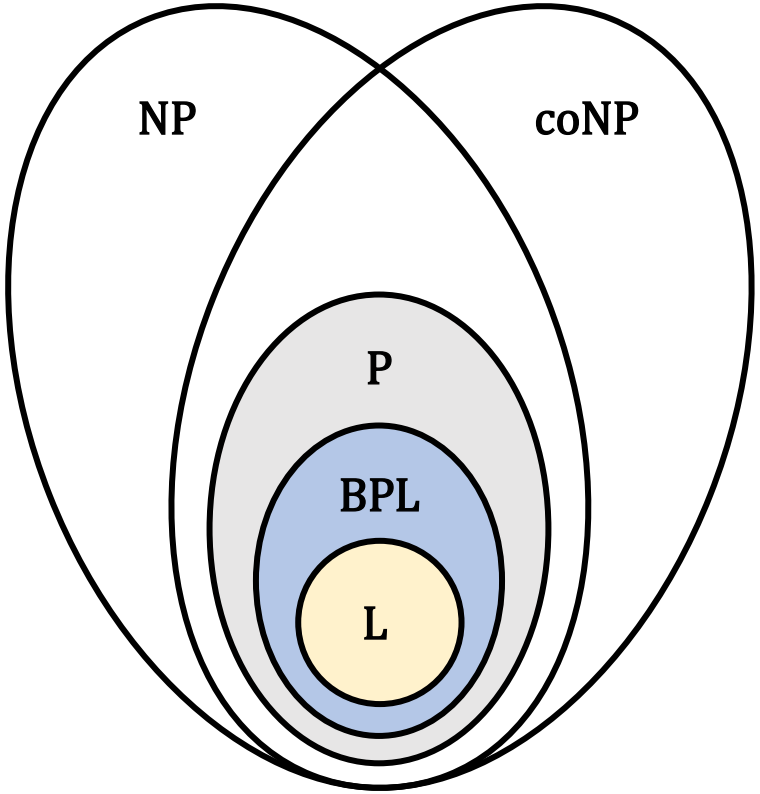
L vs. BPL



- $\mathrm{L} \subseteq \mathrm{BPL}$

Conjecture: $\mathrm{L} = \mathrm{BPL}$

- "Randomness is not necessary for space-efficient computation"



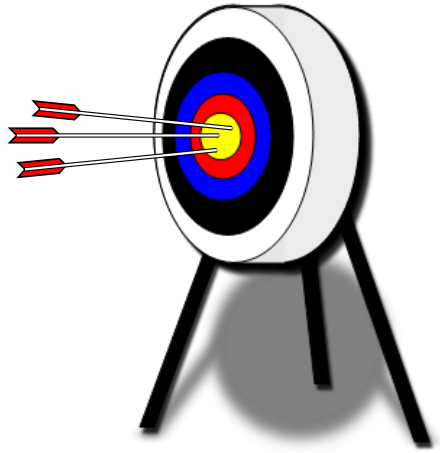
Outline

- Yesterday:
  - The INW Approach ✔️
  - The Nisan Approach ✔️
- Today:
  - The Laplacian Approach
  - The Restrictions Approach

The Laplacian Approach

Error reduction

The bottleneck in the INW/Nisan approaches is error accumulation…

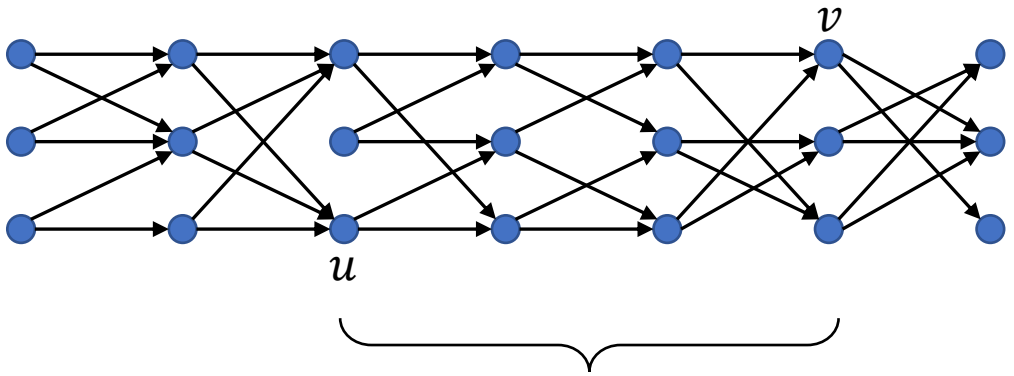


- **Assumption:** Given a width-n length-n ROBP f, one can deterministically estimate $\mathbb{E}[f]$ to within $\pm\frac{1}{n^3}$ using $S(n)$ bits of space

Theorem [Ahmadinejad, Kelner, Murtagh, Peebles, Sidford, Vadhan 2020]**:**

Given a width-n length-n ROBP f, one can deterministically estimate $\mathbb{E}[f]$ to within $\pm\varepsilon$ using $O(S(n) + \log n \cdot \log\log(1/\varepsilon))$ bits of space

Proof step 1: Subprograms

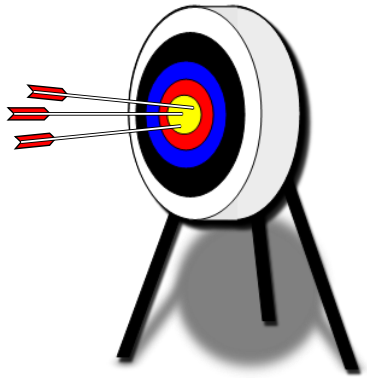


- For each subprogram $f_{u \to v}$, let $P_{u,v} = \mathbb{E}[f_{u \to v}]$
- $P \in \mathbb{R}^{N \times N}$ where N is the number of vertices, $N = (n+1) \cdot n$
- **Goal:** Approximate $\mathbb{E}[f]$
- **Strategy:** Approximate the whole matrix P

Laplacian and Richardson iteration

[Explanations on whiteboard]

1. Compute random walk matrix $W \in \mathbb{R}^{N \times N}$
2. Compute Laplacian matrix $L \coloneqq I - W$
3. Compute $\hat{P}$ such that $\left\| P - \hat{P} \right\| \leq 1/\mathrm{poly}(n)$ using assumption
4. Compute



$$\hat{\hat{P}} \coloneqq \sum_{i=0}^{m} \left(I - \hat{P}L\right)^i \cdot \hat{P}$$

"Richardson Iteration"

The Laplacian Approach:

Advanced Topics

Weighted pseudorandom generators

- **Definition:** A WPRG is a pair (G, ρ), where

  $G: \{0,1\}^s \to \{0,1\}^n$ and $\rho: \{0,1\}^s \to \mathbb{R}$

- It fools $f: \{0,1\}^n \to \{0,1\}$ with error ε if

$$\left|\mathbb{E}_x[f(x)] - \mathbb{E}_z\left[f\left(G(z)\right) \cdot \rho(z)\right]\right| \leq \varepsilon$$

- "Negative probabilities"



"Dice Illusion" by DeviantArt user Moko-m.
(License: CC BY-NC-ND 3.0)

WPRG error reduction

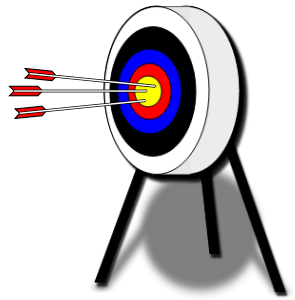
Theorem [BCG 2020] [HZ 2020] [CL 2020] [CDRST 2021] [PV 2021] [H 2021] [CW 2026] [CCDKT 2026]:

PRG that fools ROBPs with error $1/\mathrm{poly}(n)$ and seed length s



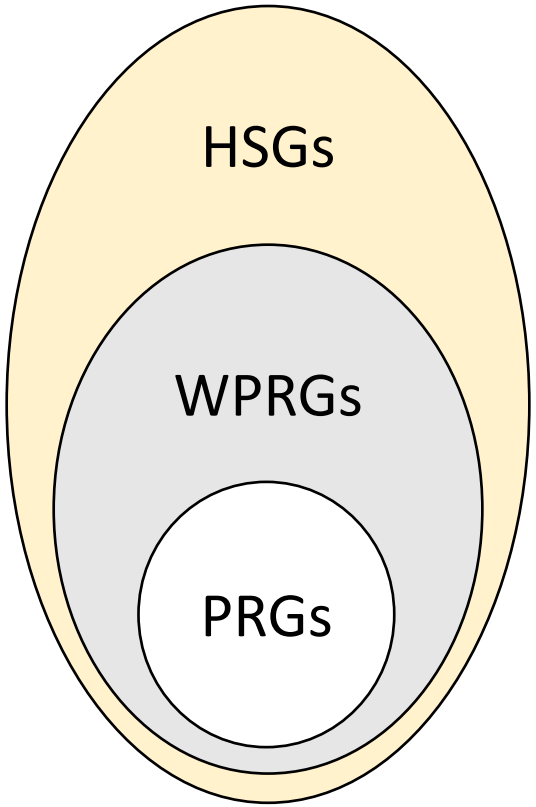
WPRG that fools ROBPs with error ε and seed length $s + O(\log(1/\varepsilon)) + \tilde{O}(\log w)$

- **Application** [H 2021]: $\mathrm{BPL} \subseteq \mathrm{DSPACE}\left(\left(\log^{3/2} n\right)/\sqrt{\log\log n}\right)$
- Proof of theorem uses a derandomized form of Richardson iteration

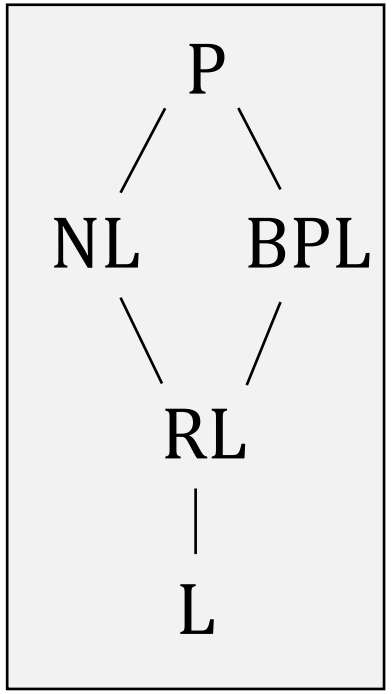


Hitting set generators

- Let $G: \{0,1\}^s \to \{0,1\}^n$
- Let $\mathcal{F}$ be a family of functions $f: \{0,1\}^n \to \{0,1\}$
- **Definition:** G is an ε-HSG for $\mathcal{F}$ if, for every $f \in \mathcal{F}$ such that $\mathbb{E}[f] > \varepsilon$, there is some $x \in \{0,1\}^s$ such that $f\big(G(x)\big) = 1$



Implications of HSGs



- **Exercise:** If there is an explicit HSG for poly-width ROBPs with seed length $O(\log n)$, then $\mathrm{L} = \mathrm{RL}$
  - RL = subset of BPL in which we insist on one-sided error

Theorem [CH 2022] [PRZ 2023]: If there is an explicit HSG for poly-width ROBPs with seed length $O(\log n)$, then $\mathrm{L} = \mathrm{BPL}$

- Proof uses Laplacian to confirm candidate probability estimates: $\hat{P}L \approx I$

Simulating random walks in undirected graphs

- **Given:** Undirected graph G, two vertices s, t, and a number $k \leq \mathrm{poly}(n)$

Theorem [AKMPSV 2020] [CHLTW 2023] [CL 2024]:

One can estimate $\Pr[k\text{-step random walk goes from } s \text{ to } t]$

deterministically to within $\pm 1/\mathrm{poly}(n)$ using $\tilde{O}(\log n)$ bits of space

- Proof uses INW approach + Richardson iteration

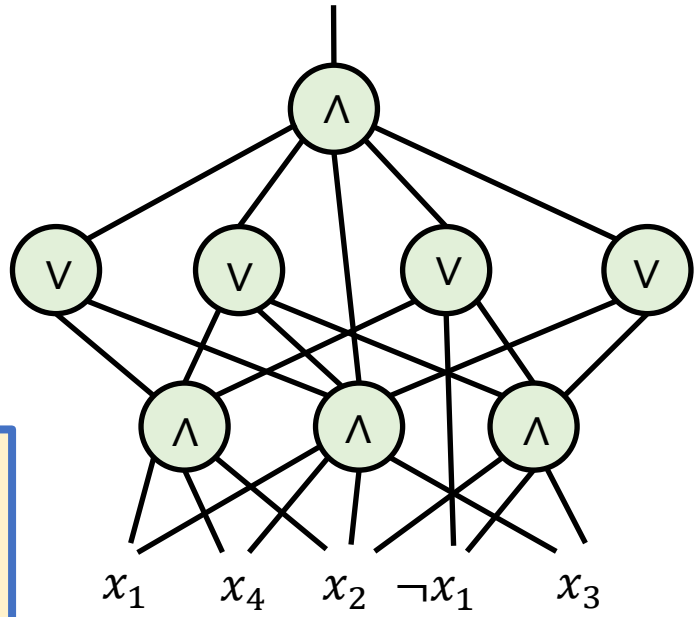
Derandomizing medium-width ROBPs

- **Problem:** Given width-w length-n ROBP f, estimate $\mathbb{E}[f]$

Space complexity	References
$\tilde{O}(\log n \cdot \log w)$	Based on [Savitch 1970]
$O\left(\log^{3/2} n + \log w \cdot \sqrt{\log n}\right)$	[Saks, Zhou 1999] [H 2021]
$\tilde{O}\left(\log n + \log w \cdot \sqrt{\log n}\right)$	[Putterman, Pyne 2023] [Cohen, Doron, Sberlo 2023]

- Proof uses Nisan approach + Richardson iteration

BPL is contained in uniform AC^1



Theorem [Cheng, Wang 2024]: For every $f \in \mathrm{BPL}$, there is a uniform family of poly-size log-depth circuits computing f, using AND/OR/NOT gates with unbounded fan-in

- Proof uses approximate counting + a variant of Richardson iteration

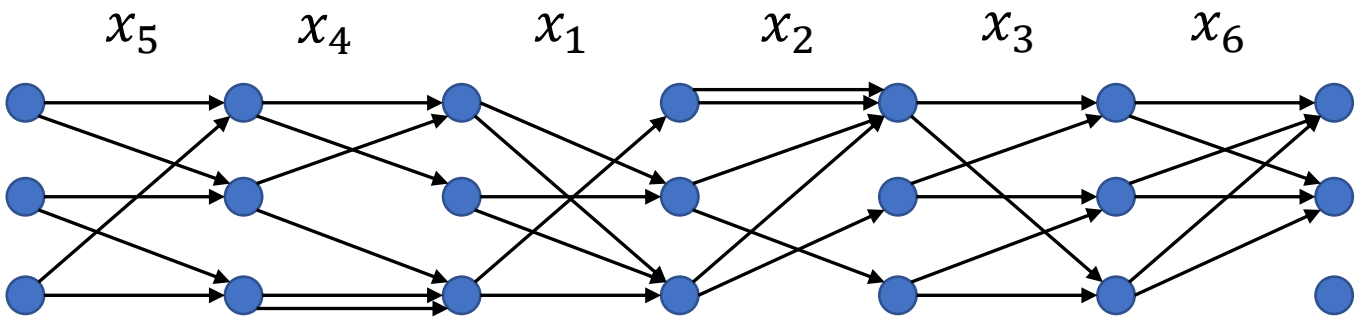
The Restrictions Approach

Forbes-Kelley PRG



Theorem [Forbes, Kelley 2018]:

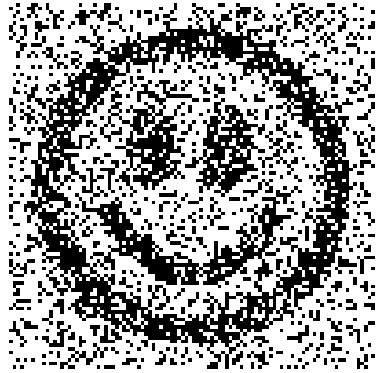
There exists an explicit PRG with seed length $O(\log^3 n)$ that fools width-n length-n ROBPs, even if the output bits are permuted



Nisan/INW provably don't work!

[Tzur 2009] [H, Lv 2025]

Step 1: Pseudorandomness plus noise



Key Lemma [Forbes, Kelley 2018]: Sample $X, Z, U \in \{0,1\}^n$ independently, where X, Z are $(2k)$-wise uniform and U is uniform. Then $X + (Z \wedge U)$ fools width-w ROBPs with error $wn \cdot 2^{-k/2}$.

- *[Proof on whiteboard]*

Step 2: Iterated restrictions [Ajtai, Wigderson 1985]

- Just proved: $X + (Z \wedge U)$ fools f
- X and Z define a restriction $\rho \in \{0, 1, \star\}^n$



U

$\approx$ $X + (Z \wedge U)$

$\approx$ ρ

$\approx$ Full PRG!

The Restrictions Approach:

Advanced Topics

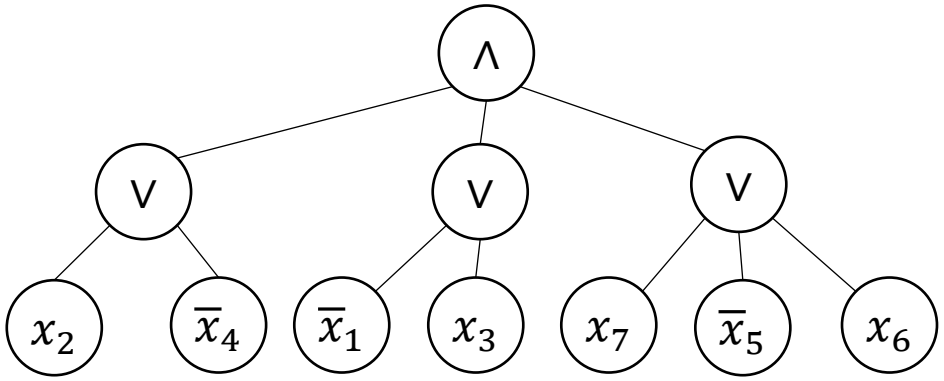
The constant-width case



Lemma [Forbes, Kelley 2018]: $\forall w, n, \varepsilon, \exists \delta = 2^{-\tilde{O}(w \cdot \log(n/\varepsilon))}$ such that if we sample $X, Z, U \in \{0,1\}^n$ independently, where X, Z are δ-biased and U is uniform, then $X + (Z \wedge U)$ fools width-w ROBPs with error ε.

- Use just $\tilde{O}(\log(n/\varepsilon))$ truly random bits to assign values to half the variables of a constant-width ROBP!
- Proof uses Fourier growth bounds [Chattopadhyay, Hatami, Reingold, Tal 2018]

Early termination



Theorem [Doron, Meka, Reingold, Tal, Vadhan 2021]: There is an explicit PRG that fools constant-width "state-monotone" ROBPs with error ε and seed length $\tilde{O}(\log(n/\varepsilon))$

- **Proof idea:** Show that after $O(\log \log n)$ iterations of Forbes-Kelley restrictions, program has simplified whp, so we can do something else

Fooling width-3 programs

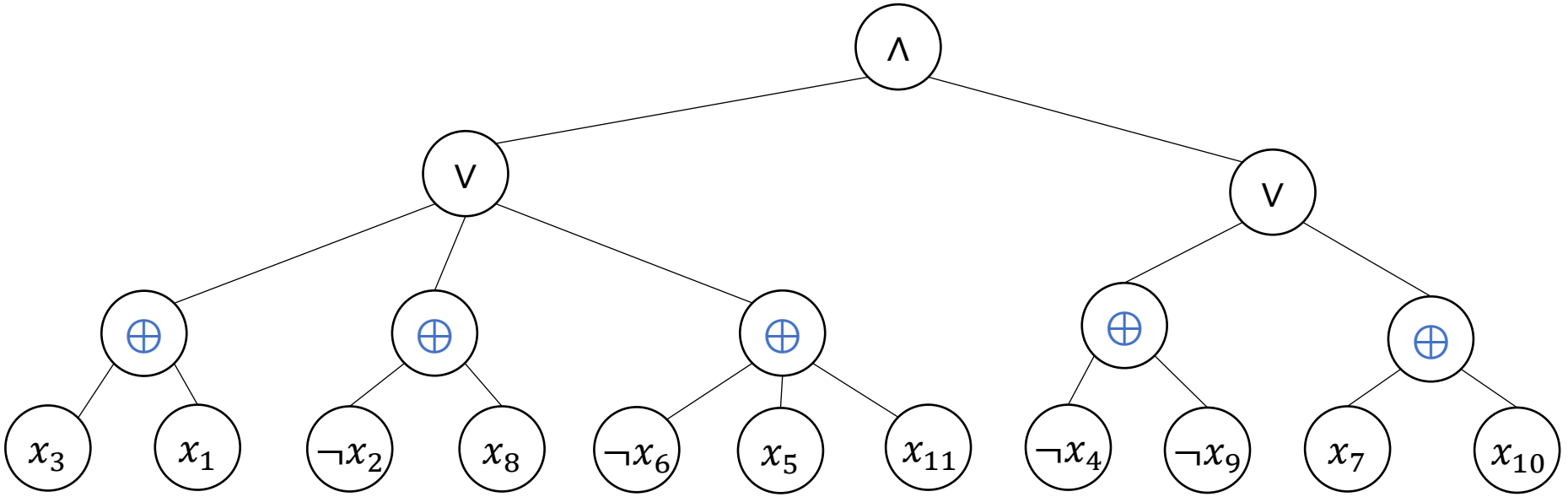
Theorem [Meka, Reingold, Tal 2019]**:** ∃ explicit PRG for width-3 ROBPs with seed length $\tilde{O}(\log n \cdot \log(1/\varepsilon))$

Theorem [CHLTW 2023] [CL 2024]**:** ∃ explicit WPRG for width-3 ROBPs with seed length $\tilde{O}\left(\log n \cdot \sqrt{\log(1/\varepsilon)} + \log(1/\varepsilon)\right)$

- **Proof idea:** Restrictions with early termination, followed by INW/Laplacian approach

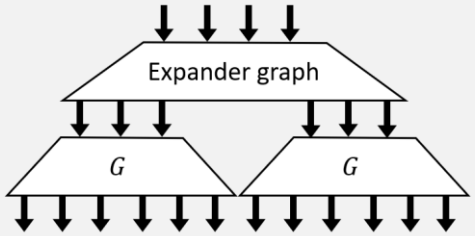
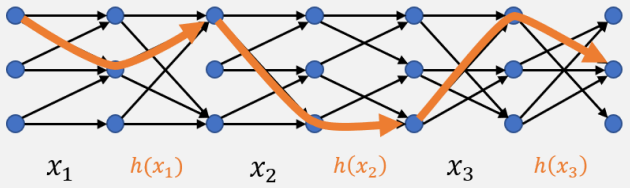
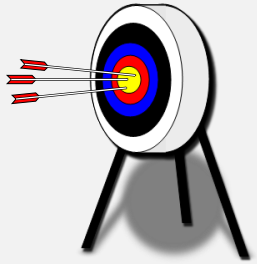
Challenge: Parity gates

- **Open problem:** Design a near-optimal PRG fooling read-once $\mathrm{AC}^0[\oplus]$



- Difficulty: It is not clear how one could justify early termination…

Conclusion

INW	Nisan
	
Laplacian	**Restrictions**
	



- Many successful ideas!
- You can come up with the next one!

Thanks for listening!