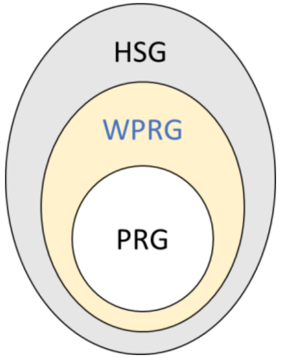
Better Pseudodistributions and Derandomization for Space-Bounded Computation

William Hoza · Simons Institute · williamhoza@berkeley.edu

Summary: We present a new construction and a new application of weighted pseudorandom generators for space-bounded computation.

Definition [Braverman, Cohen, and Garg 2018]: A *weighted pseudorandom generator* (WPRG) is a pair (G, ρ), where $G: \{0,1\}^r \to \{0,1\}^n$ and $\rho: \{0,1\}^r \to \mathbb{R}$, such that $\forall$ poly-width read-once branching program f,

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



Seed length	Type of generator	Reference
$\tilde{O}(\sqrt{n}) + O(\log(1/\varepsilon))$	HSG	Ajtai, Komlós, Szemerédi 1987
$2^{O(\sqrt{\log n})} \cdot \log(1/\varepsilon)$	PRG	Babai, Nisan, Szegedy 1989
$O(\log^2 n + \log n \cdot \log(1/\varepsilon))$	PRG	Nisan 1990, …
$\tilde{O}(\log^2 n + \log(1/\varepsilon))$	WPRG	Braverman, Cohen, Garg 2018
$O(\log^2 n + \log(1/\varepsilon))$	HSG	H, Zuckerman 2018
$\tilde{O}(\log^2 n) + O(\log(1/\varepsilon))$	WPRG	Chattopadhyay, Liao 2020
$O(\log^2 n) + \tilde{O}(\log(1/\varepsilon))$	WPRG	Cohen, Doron, Renard, Sberlo, Ta-Shma 2021 and Pyne, Vadhan 2021
$O(\log^2 n + \log(1/\varepsilon))$	WPRG	H 2021

New construction:

Theorem: $\exists$ explicit WPRG for width-n length-n ROBPs with seed length $O(\log^2 n + \log(1/\varepsilon))$

New application:

Theorem: $\forall S = S(n) \ge \log n, \quad \mathbf{BPSPACE}(S) \subseteq \mathbf{DSPACE}\left(S^{3/2}/\sqrt{\log S}\right)$

Deterministic space	Model simulated	Reference
$O(S^2)$	$\mathbf{NSPACE}(S)$	Savitch 1969
$O(S^2)$	Non-halting unbounded-error randomized space-S	Jung 1981 and Borodin, Cook, Pippenger 1983
$O(S^{3/2})$	$\mathbf{BPSPACE}(S)$	Saks, Zhou 1995
$O(S^{3/2}/\sqrt{\log S})$	$\mathbf{BPSPACE}(S)$	H 2021