Project Topic List

Pseudorandomness, Autumn 2023, University of Chicago
Instructor: William Hoza (williamhoza@uchicago.edu)

See the course webpage for project instructions.

Theorem 1 (Fooling DNFs)**.** *There is an explicit PRG for m-term DNFs with seed length $\widetilde{O}(\log m \cdot \log(m/\varepsilon))$.*

References: [DETT10; Tal17]

Theorem 2 (Fooling read-k DNFs)**.** *There is an explicit PRG for m-term read-k DNFs with seed length $(\log m) \cdot \mathrm{poly}(k, \log(1/\varepsilon)) + O(\log n)$.*

References: [KLW10; ST19]

Theorem 3 (Balanced codes)**.** *There is an explicit ε-balanced code with message length k and block length $n = k/\varepsilon^{2+o(1)}$.*

References: [Ta-17]

Theorem 4 (Fourier tail bound for ROBPs)**.** *If f is an oblivious width-w read-once branching program, then for every $k \in [n]$, we have $\sum_{|S|=k} |\widehat{f}(S)| \leq O(\log n)^{wk}$.*

References: [RSV13; CHRT18]

Theorem 5 (Fooling constant-width permutation ROBPs)**.** *There is an explicit PRG for constant-width standard-order permutation read-once branching programs with seed length $O(\log n \cdot \log(1/\varepsilon))$.*

References: [KNP11; De11; Ste12]

Theorem 6 (Fooling unbounded-width permutation ROBPs)**.** *There is an explicit PRG for unbounded-width single-accept-vertex standard-order permutation read-once branching programs with seed length $\widetilde{O}(\log n \cdot \log(1/\varepsilon))$. Furthermore, this seed length is near-optimal, i.e., every such PRG must have seed length $\widetilde{\Omega}(\log n \cdot \log(1/\varepsilon))$.*

References: [AKMPSV20; HPV21; CLTW23; CHLTW23]

Theorem 7 (Fooling combinatorial rectangles)**.** *There is an explicit PRG for combinatorial rectangles of alphabet size m and dimension n with seed length $\widetilde{O}(\log(m/\varepsilon) + \log\log n)$.*

References: [LLSZ97; Lu02; GMRTV12; GY20]

Theorem 8 (Fooling AC^0 circuits)**.** *There is an explicit PRG for depth-d size-m AC^0 circuits with seed length $\widetilde{O}(\log^{d-1} m \cdot \log(m/\varepsilon))$.*

References: [TX13; Tal17; ST22; Kel21; Lyu22]

Theorem 9 (Searching for CNF satisfying assignments)**.** *Given a polynomial-size CNF formula f and a value ε such that $\mathbb{E}[f] \geq \varepsilon$, it is possible to deterministically find a satisfying assignment to f in time $(n/\varepsilon)^{\widetilde{O}(\log\log n + \log(1/\varepsilon))}$.*

References: [GMR13; ST17; Kel21]

Theorem 10 (Fooling monotone ROBPs)**.** *There is an explicit PRG for width-w monotone standard-order read-once branching programs with seed length $\widetilde{O}(\log(n/\varepsilon))$.*

References: [DHH19; DMRTV21]

Theorem 11 (Fooling width-3 ROBPs)**.** *There is an explicit PRG for width-3 standard-order read-once branching programs with seed length $\widetilde{O}(\log n \cdot \log(1/\varepsilon))$.*

References: [GMRTV12; MRT19; CHLTW23]

Theorem 12 (Fooling linear threshold functions)**.** *There is an explicit PRG for linear threshold functions with seed length $\widetilde{O}(\log(n/\varepsilon))$.*

References: [RS10; MZ13; GKM18]

Theorem 13 (Fooling polytopes)**.** *There is an explicit PRG for m-facet polytopes with seed length $\mathrm{poly}(\log m, 1/\varepsilon) \cdot \log n$.*

References: [OST22]

Theorem 14 (Fooling de Morgan formulas)**.** *There is an explicit PRG for size-m de Morgan formulas with seed length $m^{1/3+o(1)} \cdot \mathrm{poly}(\log(1/\varepsilon))$.*

References: [IMZ19; HHTT22]

Theorem 15 (Extractors with sublinear entropy loss)**.** *For every $k \leq n$ and every $\varepsilon = 1/\operatorname{polylog}(n)$, there is an explicit (k, ε)-seeded extractor with seed length $O(\log n)$ and output length $k - o(k)$.*

References: [DKSS13; TSU12]

Theorem 16 (Two-source extractors)**.** *For every constant $\varepsilon > 0$, there exists an explicit two-source (k, ε)-extractor (outputting one bit) with entropy parameter $k = O(\log n)$.*

References: [CZ19; Li16; BDT22; Coh17; Li17; Li19; Cha20; Li23]

Theorem 17 (Weighted PRGs for ROBPs)**.** *There is an explicit weighted PRG for standard-order width-w read-once branching programs with seed length $O(\log(wn) \cdot \log n + \log(1/\varepsilon))$.*

References: [BCG20; HZ20; CL20; CDRST21; PV21; Hoz21]

Theorem 18 (Weighted PRGs for regular ROBPs)**.** *There is an explicit weighted PRG for constant-width regular standard-order read-once branching programs with seed length $\widetilde{O}(\log n \cdot \sqrt{\log(1/\varepsilon)} + \log(1/\varepsilon))$.*

References: [BHPP22; CHLTW23; CL23]

Theorem 19 (Derandomizing space-bounded computation)**.** *For every $S = S(n) \geq \log n$, we have $\mathsf{BSPACE}(S) \subseteq \mathsf{DSPACE}(o(S^{3/2}))$.*

References: [SZ99; Arm98; CL20; Hoz21; PP23]

References

[AKMPSV20] AmirMahdi Ahmadinejad, Jonathan Kelner, Jack Murtagh, John Peebles, Aaron Sidford, and Salil Vadhan. "High-precision estimation of random walks in small space". In: *Proceedings of the 61st Symposium on Foundations of Computer Science (FOCS)*. 2020, pp. 1295–1306. DOI: 10.1109/FOCS46700.2020.00123.

[Arm98] Roy Armoni. "On the Derandomization of Space-Bounded Computations". In: *Proceedings of the 2nd International Workshop on Randomization and Approximation Techniques in Computer Science (RANDOM)*. 1998, pp. 47–59. DOI: 10.1007/3-540-49543-6_5.

[BCG20] Mark Braverman, Gil Cohen, and Sumegha Garg. "Pseudorandom Pseudo-distributions with Near-Optimal Error for Read-Once Branching Programs". In: *SIAM Journal on Computing* 49.5 (2020), STOC18–242–STOC18–299. DOI: 10.1137/18M1197734.

[BDT22] Avraham Ben-Aroya, Dean Doron, and Amnon Ta-Shma. "An Efficient Reduction from Two-Source to Nonmalleable Extractors: Achieving Near-Logarithmic Min-Entropy". In: *SIAM Journal on Computing* 51.2 (2022), STOC17–31–STOC17–49. DOI: 10.1137/17M1133245.

[BHPP22] Andrej Bogdanov, William M. Hoza, Gautam Prakriya, and Edward Pyne. "Hitting Sets for Regular Branching Programs". In: *Proceedings of the 37th Computational Complexity Conference (CCC 2022)*. 2022, 3:1–3:22. ISBN: 978-3-95977-241-9. DOI: 10.4230/LIPIcs.CCC.2022.3.

[CDRST21] Gil Cohen, Dean Doron, Oren Renard, Ori Sberlo, and Amnon Ta-Shma. "Error reduction for weighted PRGs against read once branching programs". In: *Proceedings of the 36th Computational Complexity Conference (CCC)*. 2021, 22:1–22:17. DOI: 10.4230/LIPIcs.CCC.2021.22.

[Cha20] Eshan Chattopadhyay. "Guest Column: A Recipe for Constructing Two-Source Extractors". In: *SIGACT News* 51.2 (2020), 38–57. ISSN: 0163-5700. DOI: 10.1145/3406678.3406688.

[CHLTW23] Lijie Chen, William M. Hoza, Xin Lyu, Avishay Tal, and Hongxun Wu. *Weighted Pseudorandom Generators via Inverse Analysis of Random Walks and Shortcutting*. ECCC preprint TR23-114. 2023. URL: https://eccc.weizmann.ac.il/report/2023/114/.

[CHRT18] Eshan Chattopadhyay, Pooya Hatami, Omer Reingold, and Avishay Tal. "Improved pseudorandomness for unordered branching programs through local monotonicity". In: *Proceedings of the 50th Symposium on Theory of Computing (STOC)*. 2018, pp. 363–375. DOI: 10.1145/3188745.3188800.

[CL20] Eshan Chattopadhyay and Jyun-Jie Liao. "Optimal Error Pseudodistributions for Read-Once Branching Programs". In: *Proceedings of the 35th Computational Complexity Conference (CCC)*. 2020, 25:1–25:27. DOI: 10.4230/LIPIcs.CCC.2020.25.

[CL23] Eshan Chattopadhyay and Jyun-Jie Liao. *Recursive Error Reduction for Regular Branching Programs*. ECCC preprint TR23-130. 2023. URL: https://eccc.weizmann.ac.il/report/2023/130/.

[CLTW23] Lijie Chen, Xin Lyu, Avishay Tal, and Hongxun Wu. "New PRGs for Unbounded-Width/Adaptive-Order Read-Once Branching Programs". In: *50th International Colloquium on Automata, Languages, and Programming (ICALP)*. 2023, 39:1–39:20. DOI: 10.4230/LIPIcs.ICALP.2023.39.

[Coh17] Gil Cohen. "Towards Optimal Two-Source Extractors and Ramsey Graphs". In: *Proceedings of the 49th Symposium on Theory of Computing (STOC)*. 2017, 1157–1170. DOI: 10.1145/3055399.3055429. URL: https://doi.org/10.1145/3055399.3055429.

[CZ19] Eshan Chattopadhyay and David Zuckerman. "Explicit two-source extractors and resilient functions". In: *Ann. of Math. (2)* 189.3 (2019), pp. 653–705. ISSN: 0003-486X. DOI: 10.4007/annals.2019.189.3.1.

[De11] Anindya De. "Pseudorandomness for Permutation and Regular Branching Programs". In: *Proceedings of the 26th Conference on Computational Complexity (CCC)*. 2011, pp. 221–231. DOI: 10.1109/CCC.2011.23.

[DETT10] Anindya De, Omid Etesami, Luca Trevisan, and Madhur Tulsiani. "Improved pseudorandom generators for depth 2 circuits". In: *14th International Conference on Randomization and Computation (RANDOM)*. 2010, pp. 504–517. DOI: 10.1007/978-3-642-15369-3_38.

[DHH19] Dean Doron, Pooya Hatami, and William M. Hoza. "Near-Optimal Pseudorandom Generators for Constant-Depth Read-Once Formulas". In: *Proceedings of the 34th Computational Complexity Conference (CCC)*. 2019, 16:1–16:34. DOI: 10.4230/LIPIcs.CCC.2019.16.

[DKSS13] Zeev Dvir, Swastik Kopparty, Shubhangi Saraf, and Madhu Sudan. "Extensions to the Method of Multiplicities, with Applications to Kakeya Sets and Mergers". In: *SIAM Journal on Computing* 42.6 (2013), pp. 2305–2328. DOI: 10.1137/100783704.

[DMRTV21] Dean Doron, Raghu Meka, Omer Reingold, Avishay Tal, and Salil Vadhan. "Pseudorandom generators for read-once monotone branching programs". In: *Proceedings of the 25th International Conference on Randomization and Computation (RANDOM)*. 2021, 58:1–58:21. DOI: 10.4230/LIPIcs.APPROX/RANDOM.2021.58.

[GKM18] Parikshit Gopalan, Daniel M. Kane, and Raghu Meka. "Pseudorandomness via the discrete Fourier transform". In: *SIAM J. Comput.* 47.6 (2018), pp. 2451–2487. ISSN: 0097-5397. DOI: 10.1137/16M1062132.

[GMR13] Parikshit Gopalan, Raghu Meka, and Omer Reingold. "DNF sparsification and a faster deterministic counting algorithm". In: *Comput. Complexity* 22.2 (2013), pp. 275–310. ISSN: 1016-3328. DOI: 10.1007/s00037-013-0068-6.

[GMRTV12] Parikshit Gopalan, Raghu Meka, Omer Reingold, Luca Trevisan, and Salil Vadhan. "Better Pseudorandom Generators from Milder Pseudorandom Restrictions". In: *Proceedings of the 53rd Symposium on Foundations of Computer Science (FOCS)*. 2012, pp. 120–129. DOI: 10.1109/FOCS.2012.77.

[GY20] Parikshit Gopalan and Amir Yehudayoff. "Concentration for limited independence via inequalities for the elementary symmetric polynomials". In: *Theory Comput.* 16 (2020), Paper No. 17, 29. DOI: 10.4086/toc.2020.v016a017.

[HHTT22] Pooya Hatami, William M. Hoza, Avishay Tal, and Roei Tell. "Fooling constant-depth threshold circuits". In: *Proceedings of the 62nd Symposium on Foundations of Computer Science (FOCS)*. 2022, pp. 104–115. DOI: 10.1109/FOCS52979.2021.00019.

[Hoz21] William M. Hoza. "Better pseudodistributions and derandomization for space-bounded computation". In: *Proceedings of the 25th International Conference on Randomization and Computation (RANDOM)*. 2021, 28:1–28:23. DOI: 10.4230/LIPIcs.APPROX/RANDOM.2021.28.

[HPV21] William M. Hoza, Edward Pyne, and Salil Vadhan. "Pseudorandom Generators for Unbounded-Width Permutation Branching Programs". In: *Proceedings of the 12th Innovations in Theoretical Computer Science Conference (ITCS)*. 2021, 7:1–7:20. DOI: 10.4230/LIPIcs.ITCS.2021.7.

[HZ20] William M. Hoza and David Zuckerman. "Simple optimal hitting sets for small-success **RL**". In: *SIAM J. Comput.* 49.4 (2020), pp. 811–820. ISSN: 0097-5397. DOI: 10.1137/19M1268707.

[IMZ19] Russell Impagliazzo, Raghu Meka, and David Zuckerman. "Pseudorandomness from shrinkage". In: *J. ACM* 66.2 (2019), Art. 11, 16. ISSN: 0004-5411. DOI: 10.1145/3230630.

[Kel21] Zander Kelley. "An Improved Derandomization of the Switching Lemma". In: *Proceedings of the 53rd Symposium on Theory of Computing (STOC)*. 2021, 272–282. DOI: 10.1145/3406325.3451054.

[KLW10] Adam R. Klivans, Homin K. Lee, and Andrew Wan. "Mansour's Conjecture is True for Random DNF Formulas". In: *Proceedings of the 23rd Conference on Learning Theory (COLT)*. 2010, pp. 368–380. URL: http://www.learningtheory.org/colt2010/papers/085Lee.pdf.

[KNP11] Michal Koucký, Prajakta Nimbhorkar, and Pavel Pudlák. "Pseudorandom Generators for Group Products". In: *Proceedings of the 43rd Symposium on Theory of Computing (STOC)*. 2011, pp. 263–272. DOI: 10.1145/1993636.1993672.

[Li16] Xin Li. "Improved Two-Source Extractors, and Affine Extractors for Polylogarithmic Entropy". In: *57th Annual Symposium on Foundations of Computer Science (FOCS)*. 2016. DOI: 10.1109/FOCS.2016.26.

[Li17] Xin Li. "Improved Non-Malleable Extractors, Non-Malleable Codes and Independent Source Extractors". In: *Proceedings of the 49th Symposium on Theory of Computing (STOC)*. 2017, 1144–1156. DOI: 10.1145/3055399.3055486.

[Li19] Xin Li. "Non-Malleable Extractors and Non-Malleable Codes: Partially Optimal Constructions". In: *34th Computational Complexity Conference (CCC)*. 2019, 28:1–28:49. DOI: 10.4230/LIPIcs.CCC.2019.28.

[Li23] Xin Li. *Two Source Extractors for Asymptotically Optimal Entropy, and (Many) More*. arXiv preprint 2303.06802. 2023. URL: https://arxiv.org/abs/2303.06802.

[LLSZ97] Nathan Linial, Michael Luby, Michael Saks, and David Zuckerman. "Efficient construction of a small hitting set for combinatorial rectangles in high dimension". In: *Combinatorica* 17.2 (1997), pp. 215–234. ISSN: 0209-9683. DOI: 10.1007/BF01200907.

[Lu02] Chi-Jen Lu. "Improved pseudorandom generators for combinatorial rectangles". In: *Combinatorica* 22.3 (2002), pp. 417–433. ISSN: 0209-9683. DOI: 10.1007/s004930200021.

[Lyu22] Xin Lyu. "Improved Pseudorandom Generators for AC^0 Circuits". In: *Proceedings of the 37th Computational Complexity Conference (CCC)*. 2022, 34:1–34:25. DOI: 10.4230/LIPIcs.CCC.2022.34.

[MRT19] Raghu Meka, Omer Reingold, and Avishay Tal. "Pseudorandom Generators for Width-3 Branching Programs". In: *Proceedings of the 51st Symposium on Theory of Computing (STOC)*. 2019, pp. 626–637. DOI: 10.1145/3313276.3316319.

[MZ13] Raghu Meka and David Zuckerman. "Pseudorandom generators for polynomial threshold functions". In: *SIAM J. Comput.* 42.3 (2013), pp. 1275–1301. ISSN: 0097-5397. DOI: 10.1137/100811623.

[OST22] Ryan O'Donnell, Rocco A. Servedio, and Li-Yang Tan. "Fooling polytopes". In: *J. ACM* 69.2 (2022), Art. 9, 37. ISSN: 0004-5411. DOI: 10.1145/3460532.

[PP23] Aaron Putterman and Edward Pyne. "Near-optimal derandomization of medium-width branching programs". In: *Proceedings of the 55th Symposium on Theory of Computing (STOC)*. 2023, pp. 23–34. DOI: 10.1145/3564246.3585108.

[PV21] Edward Pyne and Salil Vadhan. "Pseudodistributions that beat all pseudorandom generators (extended abstract)". In: *Proceedings of the 36th Computational Complexity Conference (CCC)*. 2021, 33:1–33:15. DOI: 10.4230/LIPIcs.CCC.2021.33. Full version: ECCC preprint TR21-019.

[RS10] Yuval Rabani and Amir Shpilka. "Explicit construction of a small ε-net for linear threshold functions". In: *SIAM J. Comput.* 39.8 (2010), pp. 3501–3520. ISSN: 0097-5397. DOI: 10.1137/090764190.

[RSV13] Omer Reingold, Thomas Steinke, and Salil Vadhan. "Pseudorandomness for Regular Branching Programs via Fourier Analysis". In: *Proceedings of the 17th International Workshop on Randomization and Computation (RANDOM)*. 2013, pp. 655–670. DOI: 10.1007/978-3-642-40328-6_45.

[ST17] Rocco A. Servedio and Li-Yang Tan. "Deterministic search for CNF satisfying assignments in almost polynomial time". In: *Proceedings of the 58th Symposium on Foundations of Computer Science (FOCS)*. 2017, pp. 813–823. DOI: 10.1109/FOCS.2017.80.

[ST19] Rocco A. Servedio and Li-Yang Tan. "Pseudorandomness for read-k DNF formulas". In: *Proceedings of the 30th Symposium on Discrete Algorithms (SODA)*. 2019, pp. 621–638. DOI: 10.1137/1.9781611975482.39.

[ST22] Rocco A. Servedio and Li-Yang Tan. "Improved pseudorandom generators from peudorandom multi-switching lemmas". In: *Theory Comput.* 18 (2022), Paper No. 4, 46. DOI: 10.4086/toc.2022.v018a004.

[Ste12] Thomas Steinke. *Pseudorandomness for Permutation Branching Programs Without the Group Theory*. ECCC preprint TR12-083. 2012. URL: https://eccc.weizmann.ac.il/report/2012/083/.

[SZ99] Michael Saks and Shiyu Zhou. "$\mathrm{BP_H SPACE}(S) \subseteq \mathrm{DSPACE}(S^{3/2})$". In: *J. Comput. System Sci.* 58.2 (1999), pp. 376–403. ISSN: 0022-0000. DOI: 10.1006/jcss.1998.1616.

[Ta-17] Amnon Ta-Shma. "Explicit, almost optimal, epsilon-balanced codes". In: *Proceedings of the 49th Symposium on Theory of Computing (STOC)*. 2017, pp. 238–251. DOI: 10.1145/3055399.3055408.

[Tal17] Avishay Tal. "Tight Bounds on the Fourier Spectrum of AC0". In: *Proceedings of the 32nd Computational Complexity Conference (CCC)*. 2017, 15:1–15:31. DOI: 10.4230/LIPIcs.CCC.2017.15.

[TSU12] Amnon Ta-Shma and Christopher Umans. "Better Condensers and New Extractors from Parvaresh-Vardy Codes". In: *Proceedings of the 27th Conference on Computational Complexity (CCC)*. 2012, pp. 309–315. DOI: 10.1109/CCC.2012.25.

[TX13] Luca Trevisan and Tongke Xue. "A Derandomized Switching Lemma and an Improved Derandomization of AC0". In: *Proceedings of the 28th Conference on Computational Complexity (CCC)*. 2013, pp. 242–247. DOI: 10.1109/CCC.2013.32.