0368-4159: First Course in Derandomization 00 – Lecture

Syllabus - Tentative

Lecturer: Amnon Ta-Shma

Scribe:

1 Part 1 - Probabilistic Algorithms

- Parallel, probabilistic algorithm for Maximum Independent Set - derandomization using pairwise independence
- Parallel, probabilistic algorithm for Perfect Matching in RNC2 - the isolation lemma, probabilistic reduction from SAT to UniqueSAT, derandomization in QNC3 (not covered)
- Parallel, probabilistic algorithm for min-cut (Karger) and derandomization
- Probabilistic algorithm for Polynomial identity testing (PIT)
- Primality testing - classic algorithms, AKS and derandomization [AKS04]

2 Part 2 - Random Walks and Expanders

- Random walks on graphs
- Spectral analysis of graphs and the spectral gap
- USTCON $\in$ RL ([AKL$^+$79])
- Expanders and random walks on expanders

3 Error Correcting Codes and ε-bias

- Error correcting codes - intro
- Reed Solomon (RS) codes and k-wise independence
- The relation between binary codes and ε-bias
- The Hadamard (HAD) code (0-bias)
- The GV bound - $n \geqslant \frac{k}{\varepsilon^2}$
- Concatenating codes: RS $\circ$ HAD ($n = \left(\frac{k}{\varepsilon}\right)^2$)
- Justesen code (constant bias)
- Amplification using expanders, the Rozenman and Wigderson construction ($n = \frac{k}{\varepsilon^4}$)

4 Fourier Transform

- Fourier transform
- BLR linearity testing

5 (k, ε)-wise bias

- Constructing ε-biased k-wise random variables [NN93]
- ε-bias implies $2^{n/2}\varepsilon$ distance from uniformity

6 A glimpse into derandomizing space bounded computation: Bounded independence with noise fools BPL

- Intro to space bounded derandomization
- Iterative bounded independence plus noise [FK18]
- Nisan's generator

7 A glimpse into derandomizing time bounded computation: The hardness vs. randomness paradigm

- Intro to time bounded derandomization
- The Nisan-Wigderson generator [NW94]
- Derandomization implies circuit lower bounds [KI04]

8 Seminar in Spring Semester

- Complete Classification of Generalized Santha-Vazirani Sources, [BBEG17].
- Deterministic extractors for bit-fixing sources and exposure-resilient cryptography, [KZ06].
- Deterministic extractors for affine sources over large fields, [GR08].
- A WelchBerlekamp Like Algorithm for Decoding Gabidulin Codes, [Loi06]. First do Welch-Berlekamp for RS.
- Kakeya sets, new mergers and old extractors, [DW11].
- Subspace Evasive Sets, [DL11].
- Extractors with weak random seeds, [Raz05].

- (**) Explicit resilient functions matching Ajtai-Linial, [Mek17]
- Pseudorandom Generators from Polarizing Random Walks [CHHL18].
- Pseudorandom generators from the second Fourier level and applications to AC0 with parity gates, [CHLT18].
- (*) PCP proofs - truth tables approximated by low-degree polynomials
- (*) Dinur's proof of the PCP theorem using random walks on expanders [Din07].

References

[AKL$^+$79] Romas Aleliunas, Richard M Karp, Richard J Lipton, Laszlo Lovasz, and Charles Rackoff. Random walks, universal traversal sequences, and the complexity of maze problems. In *Foundations of Computer Science, 1979., 20th Annual Symposium on*, pages 218–223. IEEE, 1979.

[AKS04] Manindra Agrawal, Neeraj Kayal, and Nitin Saxena. Primes is in p. *Annals of mathematics*, pages 781–793, 2004.

[BBEG17] Salman Beigi, Andrej Bogdanov, Omid Etesami, and Siyao Guo. Complete classification of generalized santha-vazirani sources. *arXiv preprint arXiv:1709.03053*, 2017.

[CHHL18] Eshan Chattopadhyay, Pooya Hatami, Kaave Hosseini, and Shachar Lovett. Pseudorandom generators from polarizing random walks. In *LIPIcs-Leibniz International Proceedings in Informatics*, volume 102. Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik, 2018.

[CHLT18] Eshan Chattopadhyay, Pooya Hatami, Shachar Lovett, and Avishay Tal. Pseudorandom generators from the second fourier level and applications to AC0 with parity gates. *Electronic Colloquium on Computational Complexity (ECCC)*, 25:155, 2018.

[Din07] Irit Dinur. The pcp theorem by gap amplification. *Journal of the ACM (JACM)*, 54(3):12, 2007.

[DL11] Zeev Dvir and Shachar Lovett. Subspace evasive sets. *CoRR*, abs/1110.5696, 2011.

[DW11] Zeev Dvir and Avi Wigderson. Kakeya sets, new mergers, and old extractors. *SIAM Journal on Computing*, 40(3):778–792, 2011.

[FK18] Michael A Forbes and Zander Kelley. Pseudorandom generators for read-once branching programs, in any order. *arXiv preprint arXiv:1808.06265*, 2018.

[GR08] Ariel Gabizon and Ran Raz. Deterministic extractors for affine sources over large fields. *Combinatorica*, 28(4):415–440, 2008.

[KI04] Valentine Kabanets and Russell Impagliazzo. Derandomizing polynomial identity tests means proving circuit lower bounds. *Computational Complexity*, 13(1-2):1–46, 2004.

[KZ06] Jesse Kamp and David Zuckerman. Deterministic extractors for bit-fixing sources and exposure-resilient cryptography. *SIAM Journal on Computing*, 36(5):1231–1247, 2006.

[Loi06] Pierre Loidreau. A welch–berlekamp like algorithm for decoding gabidulin codes. In *Coding and cryptography*, pages 36–45. Springer, 2006.

[Mek17] Raghu Meka. Explicit resilient functions matching ajtai-linial. In *Proceedings of the Twenty-Eighth Annual ACM-SIAM Symposium on Discrete Algorithms*, pages 1132–1148. SIAM, 2017.

[NN93] Joseph Naor and Moni Naor. Small-bias probability spaces: Efficient constructions and applications. *SIAM journal on computing*, 22(4):838–856, 1993.

[NW94] Noam Nisan and Avi Wigderson. Hardness vs randomness. *Journal of computer and System Sciences*, 49(2):149–167, 1994.

[Raz05] Ran Raz. Extractors with weak random seeds. In *Proceedings of the thirty-seventh annual ACM symposium on Theory of computing*, pages 11–20. ACM, 2005.