C&O 739 Information Theory and Applications
University of Waterloo, Winter 2024
Instructor: Ashwin Nayak
Project Suggestions

The following is a partial list of research articles related to the theme of the course. For related papers and other ideas, please talk to me.

Please confirm the topic and the scope of the project with me.

Applications of entropic quantities.

- Predecessor-search: Pranab Sen and Srinivasan Venkatesh. Lower bounds for predecessor searching in the cell probe model. Journal of Computer and System Sciences, 74(3):364–385, 2008.
- More data-structures: Mihai Patrascu and Erik Demaine. Logarithmic Lower Bounds in the Cell-Probe Model. SIAM Journal on Computing, 35(4):932–963, 2006.
- Set Disjointness and extended formulations: Mark Braverman and Ankur Moitra. An information complexity approach to extended formulations. In Proceedings of the forty-fifth Annual ACM Symposium on Theory of Computing, pp. 161–170, 2013.
- Explicit polytopes with high extension complexity: Mika Göös, Rahul Jain, and Thomas Watson. Extension Complexity of Independent Set Polytopes. SIAM Journal on Computing, 47(1):241–269, 2018.
- Communication complexity (of application to streaming algorithms): Uri Hadar, Jingbo Liu, Yury Polyanskiy, and Ofer Shayevitz. Communication complexity of estimating correlations. In Proceedings of the 51st Annual ACM SIGACT Symposium on Theory of Computing, pp. 792–803, 2019.
- Probability theory: Lampros Gavalakis and Ioannis Kontoyiannis. An Information-Theoretic Proof of a Finite de Finetti Theorem. Electronic Communications in Probability, 26:1–5, 2021.

Compression of interactive protocols.

- Compression, direct sum: Boaz Barak, Mark Braverman, Xi Chen, Anup Rao. How to Compress Interactive Communication. SIAM Journal on Computing, 42(3):1327–1363, 2013.
- Direct sum: Mark Braverman, Anup Rao. Information Equals Amortized Communication. IEEE Transactions on Information Theory, 60(10):6058–6069, Oct. 2014.
- Compression for product distributions: Gillat Kol. Interactive Compression for Product Distributions. Technical report TR15-168, ECCC, http://eccc.hpi-web.de/report/2015/168, 2015. In Proceedings of the forty-eighth annual ACM Symposium on Theory of Computing, June 2016, pages 987-998.

  OR

  Prahladh Harsha, Rahul Jain, and Jaikumar Radhakrishnan. Partition bound is quadratically tight for product distributions. In Proceedings of the 43rd International Colloquium on Automata, Languages, and Programming, 2016, LIPIcs 55, 135:1–135:13.

Coding for noisy (interactive) communication.

- Coding for interaction: Leonard J. Schulman. Coding for Interactive Communication. IEEE Transactions on Information Theory 42(6):1745–1756, 1996.

  And more in the survey

  Ran Gelles. Coding for Interactive Communication: A Survey. Foundations and Trends in Theoretical Computer Science 13(1–2):1–157, 2017. Now Publishers.

- Interactive Channel Capacity: Bernhard Haeupler. Interactive Channel Capacity Revisited. In Proceeding of the 56th Annual IEEE Symposium on Foundations of Computer Science, pp. 226–235, 2014.

- Noisy broadcast channels: Robert G. Gallager. Finding parity in a simple broadcast network. IEEE Transactions on Information Theory 34:176–180, 1988.

  And

  Navin Goyal, Guy Kindler, and Michael E. Saks. Lower Bounds for the Noisy Broadcast Problem. SIAM Journal on Computing, 37(6):1806–1841, 2008.

- Rounds in noisy broadcast protocols: Klim Efremenko, Gillat Kol, and Raghuvansh R. Saxena. Interactive coding over the noisy broadcast channel. In Proceedings of the 50th Annual ACM-SIGACT Symposium on Theory of Computing, June 2018, pp. 507–520.

- Insertion-deletion channels: Alexander A. Sherstov and Pei Wu. Optimal Interactive Coding for Insertions, Deletions, and Substitutions. In Proceedings of the 58th IEEE Annual Symposium on Foundations of Computer Science, Oct. 2017, pp. 240–251.

Parallel repetition and direct product theorems.

- Parallel Repetition theorem: Thomas Holenstein. Parallel Repetition: Simplification and the No-Signaling Case, Theory of Computing 5(8):141–172, 2009.

- Direct Product theorem, bounded rounds: Rahul Jain, Attila Pereszlenyi, Penghui Yao. A direct product theorem for bounded-round public-coin randomized communication complexity. In Proceedings of the 53rd Annual IEEE Symposium on Foundations of Computer Science, pp. 167–176, 2012.

- Direct Product theorem, general case: Mark Braverman, Anup Rao, Omri Weinstein, Amir Yehudayoff. Direct products in communication complexity. In Proceedings of the 54th Annual IEEE Symposium on Foundations of Computer Science, pp. 746-755, 2013.

- Anchoring games: Mohammad Bavarian, Thomas Vidick, and Henry Yuen. Hardness amplification for entangled games via anchoring. In Proceedings of the 49th Annual ACM SIGACT Symposium on Theory of Computing, 2017, pp. 303–316.

Error-correction codes, their applications.

- Linear-time coding/decoding: Michael Sipser and Daniel A. Spielman. Expander codes: Codes and complexity. IEEE Transactions on Information Theory, 42(6-1):1710–1722, 1996.

- List-decoding: Venkatesan Guruswami and Madhu Sudan. Improved Decoding of Reed-Solomon and Algebraic-Geometric codes. IEEE Transactions on Information Theory, 45:1757–1767, 1999.

  And more in the survey

  Venkatesan Guruswami. Algorithmic Results in List Decoding. Foundations and Trends in Theoretical Computer Science 2(2):107–195, 2006. Now Publishers.

  See also

  Venkatesan Guruswami and Atri Rudra. Concatenated codes can achieve list-decoding capacity. In Proceedings of the 19th Annual ACM-SIAM Symposium on Discrete Algorithms (SODA), spp. 258–267, 2008.

- Randomness extraction: Luca Trevisan. Extractors and Pseudorandom Generators. Journal of the ACM, 48(4):860–879, 2001.

  And more in the survey

  Salil P. Vadhan. Pseudorandomness. Foundations and Trends in Theoretical Computer Science 7(1–3):1–336, 2011. Now Publishers.

- Local decoding: Sergey Yekhanin. Locally decodable codes. Foundations and Trends in Theoretical Computer Science 6(3):139–255, 2012. Now Publishers.

- Polar codes: Erdal Arikan. Channel Polarization: A Method for Constructing Capacity-Achieving Codes for Symmetric Binary-Input Memoryless Channels. IEEE Transactions on Information Theory, 55(7):3051–3073, 2009.

- Polar codes with near-optimal convergence: Venkatesan Guruswami, Andrii Riazanov, and Min Ye. Arıkan meets Shannon: Polar codes with Near-Optimal Convergence to Channel Capacity. IEEE Transactions on Information Theory, 68(5):2877–2919, May 2022.

- Codes and epsilon-biased sets: Amnon Ta-Shma. Explicit, almost optimal, epsilon-balanced codes. In Proceedings of the 49th Annual ACM SIGACT Symposium on Theory of Computing, June 2017, pp. 238–251.

- Irit Dinur, Shai Evra, Ron Livne, Alexander Lubotzky, and Shahar Mozes. Locally Testable Codes with Constant Rate, Distance, and Locality. In Proceedings of the 54th Annual ACM SIGACT Symposium on Theory of Computing, pp. 357–374, 2022.

  OR

  Pavel Panteleev and Gleb Kalachev. Asymptotically Good Quantum and Locally Testable Classical LDPC Codes. In Proceedings of the 54th Annual ACM SIGACT Symposium on Theory of Computing, pp. 375–388, 2022.

Quantum Information Theory and Applications.

- Please discuss possible papers in quantum information with me.