Coding for Interactive Communication

FOCS 2016 Workshop: Saturday, October 8th

1 Overview

The goal of this workshop is to discuss the area of "Coding for Interactive Communictaions", which can be seen as the equivalent of error correcting codes for conversations / communication protocols. While this research direction goes back to fundamental work initiated by Schulman in '92 [Sch92, Sch93, Sch96, RS94] it has recently gained much attention and seen signifficant progress [BR11, Dru11, Bra12, BK12, KLR12, KR13, BN13, FGOS13, CPT13, Pan13, LdMM13, GHS14, GH14, Hae14, GMS14, BKN14, BE14, BNT$^+$14, MS14, LV15, HKV15, JKL15, GH15, GSW15, EGH15, ABE$^+$16, HS16, Pud16, DL16, BEGH16, GHK$^+$16, Gel16, BGMO16, AGS16]. This rapid recent progress makes it hard for non-experts (and even for experts) to keep track of outstanding open problems and interesting research directions. Despite steady interest in the topic, this makes it difficult to get into this area. The purpose of the tutorial is twofold:

1. to give a comprehensive summary of the current state-of-the-art and a primer on the most important techniques for the broader community
2. to outline and discuss new research directions and open questions and putting them in context with the most recent works and thus exposing them to a large audience of interested researchers while also lowering the barriers to working on them.

We hope that this will facilitate and inspire further progress in this new direction, particularly by researchers not currently working in the area.

2 Schedule (tentative)

The workshop will feature two talks by the organizers and a coffee break. Both talks will leave ample time for discussing (open) questions:

- **2:30-4:00 Mark Braverman: Introduction to Interactive Coding, Tree Codes, and Extensions**

  We will introduce the problem of interactive error-correcting coding, and the parameters we care about. We will discuss tree codes, their various extensions, and attempts at efficient constructions. We will then outline list-decodable interactive codes, both as a useful primitive and as a case study in applications of tree-code extensions. Time permitting, we will briefly discuss the multiparty case, as well as lower bound paradigms.

- **4:00-4:30 Coffee Break**

- **4:30-6:00 Bernhard Haeupler: Interactive Coding Schemes Efficiency and Rate**

  We will provide an overview over interactive coding techniques which lead to computationally efficient interactive coding schemes and discuss the question of communication rate. While there exists schemes whose communication rate approaches one for asymptotically small noise rates there seems to be a gap between what rates are possible in the usual one-way error correcting code setting and what interactive coding schemes can achieve. We discuss recent communication complexity lower bound results, conjectures, and open questions addressing this rate gap.

Speakers / Organizers:

- **Mark Braverman** received his PhD at the University of Toronto and is currently a professor at Princeton University. His research focuses on complexity theory and on connections between theoretical computer science and other disciplines such as information theory, dynamical systems, operations research, and mechanism design.
- **Bernhard Haeupler** received his PhD at MIT and is currently an assistant professor at Carnegie Mellon University. His research focuses on combinatorial algorithms, the theory of distributed computing, information theory, and (network) coding theory.

3 Background

In 1948 Shannon's formalized and exactly characterized the possibilities and limitations of achieving reliable information transfer over unreliable channels. It is hard to overestimate the impact of this theory of error correction. Over the last decades it was a main enabler of the digital revolution and essentially any modern telecommunications, computing or data storage system crucially relies on error correcting codes. Beyond their immeasurable practical impact their mathematical development has also lead to profound and deep connections in many sub-fields of mathematics, computer science, engineering, and beyond. It is thus not surprising that this study is continued today by hundreds of active researchers in the fields of information theory and coding theory.

Many modern communication settings however go beyond the reliable one-way information transfer enabled through error correcting codes and instead operate over many interleaved rounds of interactive communication, that are interspersed with computations. Cloud computing and other modern distributed systems are prime examples of such settings and the trend to more and more distributed and interactive systems is increasing. The problem with such interactive settings is that a single (fully) corrupted message, which itself is only a tiny fraction of the overall communication, can fatally derange a protocol and its underlying computations. Single messages might furthermore be too small to apply error correction codes (efficiently). In general, both problems make achieving reliable interactive communication by protecting messages one by one impossible and motivate the above mentioned research on interactive coding schemes. In contrast to error correcting codes, interactive coding schemes require a fundamental integration of error correction capabilities and interactive computations/communications making this research direction a rich and interesting playing field for (theoretical) computer scientists. The close ties of communication and computation in this setup make it also less surprising that research on interactive coding has already found applications and developed ties to other parts of theoretical computer science, such as, circuits [KLR12], cryptography [CPT13, FGOS13, GSW15], distributed computing [BEGH16, RS94, HS16], interactive proofs [DL16] and complexity [Dru11]. In addition, it has developed fascinating connections to questions in metric embeddings [LdMM13] and pure mathematics [MS14].

References

[ABE+16] Noga Alon, Mark Braverman, Klim Efremenko, Ran Gelles, and Bernhard Haeupler. Reliable communication over highly connected noisy networks. *ACM SIGACT-SIGOPS Symposium on Principles of Distributed Computing (PODC)*, 61, 2016.

[AGS16] Shweta Agrawal, Ran Gelles, and Amit Sahai. Adaptive protocols for interactive communication. *IEEE Internetional Symposium on Information Theory (ISIT)*, pages 595–599, 2016.

[BE14] Mark Braverman and Klim Efremenko. List and unique coding for interactive communication in the presence of adversarial noise. In *Proceedings of the IEEE Symposium on Foundations of Computer Science (FOCS)*, pages 236–245, 2014.

[BEGH16] Mark Braverman, Klim Efremenko, Ran Gelles, and Bernhard Haeupler. Constant-rate coding for multiparty interactive communication is impossible. *Proceedings of the ACM Symposium on Theory of Computing (STOC)*, pages 999–1010, 2016.

[BGMO16] Mark Braverman, Ran Gelles, Jieming Mao, and Rafail Ostrovsky. Coding for interactive communication correcting insertions and deletions. *Proceedings of the International Colloquium on Automata, Languages and Programming (ICALP)*, 2016.

[BK12] Zvika Brakerski and Yael Tauman Kalai. Efficient interactive coding against adversarial noise. *Proceedings of the IEEE Symposium on Foundations of Computer Science (FOCS)*, pages 160–166, 2012.

[BKN14] Zvika Brakerski, Yael Tauman Kalai, and Moni Naor. Fast interactive coding against adversarial noise. *Journal of the ACM (JACM)*, 61(6):35:1–35:30, 2014.

[BN13] Zvika Brakerski and Moni Naor. Fast algorithms for interactive coding. In *Proceedings of the ACM-SIAM Symposium on Discrete Algorithms (SODA)*, pages 443–456, 2013.

[BNT+14] Gilles Brassard, Amiya Nayak, Alain Tapp, Dave Touchette, and Falk Unger. Noisy interactive quantum communication. In *Proceedings of the IEEE Symposium on Foundations of Computer Science (FOCS)*, pages 296–305, 2014.

[BR11] Mark Braverman and Anup Rao. Towards coding for maximum errors in interactive communication. In *Proceedings of the ACM Symposium on Theory of Computing (STOC)*, pages 159–166, 2011.

[Bra12] Mark Braverman. Towards deterministic tree code constructions. In *Proceedings of the ACM-SIGACT Innovations in Theoretical Computer Science Conference (ITCS)*, pages 161–167, 2012.

[CPT13] Kai-Min Chung, Rafael Pass, and Sidharth Telang. Knowledge-preserving interactive coding. In *Proceedings of the IEEE Symposium on Foundations of Computer Science (FOCS)*, pages 449–458, 2013.

[DL16] Yevgeniy Dodis and Allison Bishop Lewko. Interactive coding for interactive proofs. *International Theory of Cryptography Conference (TCC)*, pages 352–366, 2016.

[Dru11] Andrew Drucker. Efficient probabilistically checkable debates. *Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques*, pages 519–529, 2011.

[EGH15] Klim Efremenko, Ran Gelles, and Bernhard Haeupler. Maximal noise in interactive communication over erasure channels and channels with feedback. In *Proceedings of the ACM-SIGACT Innovations in Theoretical Computer Science Conference (ITCS)*, pages 11–20, 2015.

[FGOS13] Matthew Franklin, Ran Gelles, Rafail Ostrovsky, and Leonard Schulman. Optimal coding for streaming authentication and interactive communication. In *Proceedings of the IACR International Cryptology Conference (CRYPTO)*, pages 258–276, 2013.

[Gel16] Ran Gelles. Coding for interactive communication: A survey. *http://www.cs.princeton.edu/r̃gelles/papers/survey.pdf*, 2016.

[GH14] Mohsen Ghaffari and Bernhard Haeupler. Optimal Error Rates for Interactive Coding II: Efficiency and List Decoding. In *Proceedings of the IEEE Symposium on Foundations of Computer Science (FOCS)*, pages 394–403, 2014.

[GH15] Ran Gelles and Bernhard Haeupler. Capacity of interactive communication over erasure channels and channels with feedback. In *Proceedings of the ACM-SIAM Symposium on Discrete Algorithms (SODA)*, pages 1296–1311, 2015.

[GHK+16] Ran Gelles, Bernhard Haeupler, Gillat Kol, Noga Ron-Zewi, and Avi Wigderson. Towards optimal deterministic coding for interactive communication. *Proceedings of the ACM-SIAM Symposium on Discrete Algorithms (SODA)*, 2016.

[GHS14] Mohsen Ghaffari, Bernhard Haeupler, and Madhu Sudan. Optimal error rates for interactive coding I: Adaptivity and other settings. In *Proceedings of the ACM Symposium on Theory of Computing (STOC)*, pages 794–803, 2014.

[GMS14] Ran Gelles, Ankur Moitra, and Amit Sahai. Efficient coding for interactive communication. *IEEE Transactions on Information Theory (TransInf)*, 60(3):1899–1913, 2014.

[GSW15] Ran Gelles, Amit Sahai, and Akshay Wadia. Private interactive communication across an adversarial channel. *IEEE Transactions on Information Theory (TransInf)*, 61(12):6860–6875, 2015.

[Hae14] Bernhard Haeupler. Interactive Channel Capacity Revisited. In *Proceedings of the IEEE Symposium on Foundations of Computer Science (FOCS)*, pages 226–235, 2014.

[HKV15] Bernhard Haeupler, Pritish Kamath, and Ameya Velingker. Communication with partial noiseless feedback. In *Proceedings of the International Workshop on Randomization and Computation (RANDOM)*, 2015.

[HS16] William M. Hoza and Leonard J. Schulman. The adversarial noise threshold for distributed protocols. *Proceedings of the ACM-SIAM Symposium on Discrete Algorithms (SODA)*, pages 240–258, 2016.

[JKL15] Abhishek Jain, Yael Tauman Kalai, and Allison Bishop Lewko. Interactive coding for multiparty protocols. In *Proceedings of the ACM Innovations in Theoretical Computer Science Conference (ITCS)*, pages 1–10, 2015.

[KLR12] Yael Tauman Kalai, Allison Lewko, and Anup Rao. Formulas resilient to short-circuit errors. In *Foundations of Computer Science (FOCS), 2012 IEEE 53rd Annual Symposium on*, pages 490–499. IEEE, 2012.

[KR13] Gillat Kol and Ran Raz. Interactive channel capacity. In *Proceedings of the ACM Symposium on Theory of Computing (STOC)*, pages 715–724, 2013.

[LdMM13] James Lee, Arnaud de Mesmay, and Mohammad Moharrami. Dimension reduction for finite trees in L1. *Discrete & Computational Geometry*, 50(4):977–1032, 2013.

[LV15] Allison Lewko and Ellen Vitercik. Balancing communication for multi-party interactive coding. *CoRR*, abs/1503.06381, 2015.

[MS14] Cristopher Moore and Leonard Schulman. Tree codes and a conjecture on exponential sums. In *Proceedings of the ACM-SIGACT Innovations in Theoretical Computer Science Conference (ITCS)*, pages 145–154, 2014.

[Pan13] Denis Pankratov. On the power of feedback in interactive channels. Technical Report: `http://people.cs.uchicago.edu/~pankratov/papers/feedback.pdf`, 2013.

[Pud16] Pavel Pudlák. Linear tree codes and the problem of explicit constructions. *Linear Algebra and its Applications*, 490:124–144, 2016.

[RS94] Sridhar Rajagopalan and Leonard Schulman. A coding theorem for distributed computation. In *Proceedings of the ACM Symposium on Theory of Computing (STOC)*, pages 790–799, 1994.

[Sch92] Leonard J. Schulman. Communication on noisy channels: a coding theorem for computation. *Proceedings of the IEEE Symposium on Foundations of Computer Science (FOCS)*, pages 724–733, 1992.

[Sch93] Leonard J. Schulman. Deterministic coding for interactive communication. In *Proceedings of the ACM Symposium on Theory of Computing (STOC)*, pages 747–756, 1993.

[Sch96] Leonard J. Schulman. Coding for interactive communication. *IEEE Transactions on Information Theory (TransInf)*, 42(6):1745–1756, 1996.