Information reconciliation for multi-mode optical communication

Proposed project for UCLA Research in Industrial Projects for Students (RIPS) 2013

Industrial sponsor: HRL Laboratories, LLC

Point of contact: Jim Harrington (jwharrington@hrl.com)

Problem description

Within the realm of information theory, one active area of research is concerned with constrained communication resources. Suppose that two parties (Alice and Bob) want to share a set of data. There are many scenarios where Bob may already have a reasonable prediction of much of Alice's data. For instance, Alice may be updating a file stored in a code repository, or she may be transmitting a video stream, which typically has a large degree of similarity from one frame to the next. How can Bob make use of this *side information* (e.g., the last version of the file or the last frame) to effectively determine Alice's current data with a minimal amount of communication, in particular when Alice makes no use of Bob's knowledge? In the 1970's, this problem was cast as source coding with side information at the decoder, and there has been a renaissance over the past decade in developing practical solutions to this problem, following the publication of the classic DISCUS paper [1]. Strong candidates for syndrome source coding include low-density parity-check codes [2] and list-decodable codes [3].

HRL Laboratories, LLC, is interested in applying these information reconciliation methods between distant parties, especially for a scenario arising from a proposed multi-mode optical communication system. Suppose that Alice transmits randomly encoded single-photon signals, and then Bob's noisy measurements of these signals form his side information. They can now perform public communication to reconcile this data, but for reasons of both security and efficiency, such communication needs to be minimized. An additional twist is that Alice is transmitting in parallel over many modes (channels), and there will naturally be some amount of crosstalk between the modes, resulting in a biased error model. There is an open question of how best to reconcile information under this error model. The project can initially focus on the generic problem of source coding with side information, including a comparison of recent approaches (such as [2] and [3]), and then software simulations could be developed to address specifics of our multi-mode optical communication system. If time permits, rate-compatible code families (or rateless codes) could also be investigated for their ability to handle a wide range of channel noise with a small amount of feedback.

Detailed Task List

The suggested task list for this project follows, along with identifications of which portions of the team [coding theory, software implementation, simulation analysis] could serve as primary contributors. The first few tasks, in particular, will involve a fair amount of collaboration with both the HRL and academic mentors.

- Gain familiarity with the literature, starting with the papers referenced below [entire team].
- Investigate at least two syndrome source coding schemes as potential candidates for the information reconciliation protocol [coding theory].

- Define the basic communication model for a single channel [simulation analysis].
- Construct a set of codes that together can handle a range of channel noise [coding theory].
- Implement one or more of the syndrome source coding schemes [software implementation].
- Determine a base line of performance for syndrome source coding over the basic channel [simulation analysis].
- Extend communication model to many parallel channels with crosstalk [simulation analysis].
- Develop a strategy for joint decoding of multiple channels [coding theory and software implementation].
- Investigate performance of joint decoding versus independent decoding of the channels [simulation analysis].

Time permitting, the following optional tasks could also be incorporated. The last task could be done for any of the communication models that are developed in the course of the project.

- Introduce a small amount of feedback from the receiver into the communication model in order to adapt the source coding to the level of noise [simulation analysis].
- Construct either a rate-compatible family of codes or a rateless code (e.g., Raptor) for software implementation [coding theory and software implementation].
- Determine performance of the adaptive coding scheme over a wide range of channel noise [simulation analysis].
- Calculate communication and computational requirements of the candidate information reconciliation protocol(s), as a function of channel noise [entire team].

Desired qualifications

The mathematics background best suited for this project is covered by coursework or equivalent experience in linear algebra, probability and statistics, and discrete mathematics. One or more team members should have a strong familiarity with basic information theory, in particular Shannon entropy, communication channels, and error-correcting codes, obtained via formal coursework in electrical engineering or similar experience. At least one student should have strong software development skills (preferably in C/C++ or Python), ideally having had coursework in data structures and algorithms, or something similar.

References (and recommended reading):

[1] S. Pradhan and K. Ramchandran, "Distributed source coding using syndromes (DISCUS): Design and construction," *IEEE Transactions on Information Theory*, Vol. 49, No. 3, pp. 626—643 (2003). **See especially Section III.A (Problem Formulation).**

[2] D. Elkouss, J. Martinez-Mateo and V. Martin, "Information reconciliation for quantum key distribution," *Quantum Information and Computation*, Vol. 11, No. 3&4, pp. 226—238 (2011), (http://arXiv.org/abs/1007.1616). **See especially Section 2 (Problem Statement).**

[3] M. Ali and M. Kujiper, "An algebraic approach to source coding with side information using list decoding," (http://arXiv.org/abs/1110.6698). **See especially Section 1 (Introduction) and Section 4 (Constructive Code Design).**