IEEE European School of Information Theory

Tallinn, Estonia, April 14-18th, 2014

Abstracts of talks

Compute-and-Forward: an Explicit Link between Finite Field and Gaussian Interference Networks

Bobak Nazer
Boston University

This talk overviews the compute-and-forward strategy, which can exploit the interference property of a multi-user channel to achieve higher end-to-end rates in a network. The key idea is that users should decode linear combinations of the transmitted messages over an appropriate finite field. This is a departure from classical information-theoretic frameworks which tend to either to decode interfering messages in their entirety or treat them as noise. Structured codes (such linear or lattice codes) ensure that these linear combinations can be decoded reliably, often at far higher rates than the messages individually. Historically, codes with linear/lattice structure have been studied as a stepping stone to practical constructions. Recently, several groups have discovered network scenarios where structured codes are also useful for obtaining new achievability results. Our recent efforts have been directed towards unifying these advances under a single framework.

In the first part of the talk, we will build up the compute-and-forward framework from first principles, starting from linear codes for discrete memoryless channels and moving to nested lattice codes for Gaussian channel. We will then demonstrate applications of this framework using examples drawn from multiple-access, broadcast, interference, and MIMO channels. Finally, we will highlight some recent advances and open questions.

Algebraic Lattices and Applications to Communications

Camilla Hollanti
Aalto University

During this course, we will learn what algebraic lattices are and how they can be applied to wireless communications. We derive number-theoretic design criteria for optimizing the performance of algebraic lattice codes. In particular, we consider fading multiple-input multiple-output (MIMO) channels and space-time lattice codes arising from division algebras. Time permitting, we will demonstrate how number theory comes into play also when analyzing the (physical layer) security of communications over a wiretap channel. The relevant algebraic background will be provided during the course so that prior knowledge in algebra will not be necessary.

Information Theoretic Security and its Applications

Yingbin Liang
Syracuse University

Information theoretic security opens a promising new direction toward solving security problems in communication networks. The basic idea is to exploit the inherent randomness of communication channels to advantage legitimate receivers in order to achieve secure communications. This approach has numerous advantages including provably perfect security and significantly lower computational complexity.

In this talk, I will first introduce the idea of information theoretic security, which includes the design of secure communication schemes and the corresponding characterizations of the secrecy capacity for some basic wiretap channels. I will then present applications of information theoretic security to solving problems of secret sharing and secure communications over mobile ad hoc networks. I will finally talk about several future directions.

Spatial Coupling – What is it, why does it work, and what are the open challenges?

Rüdiger Urbanke
École Polytechnique Fédérale de Lausanne

Designing good sparse-graph codes is the problem of finding graphical structures that interact well with the message-passing decoder. Over the past 20 years many such structures have been proposed and have been found to be useful. Prominent examples of structures that work well are turbo codes, low-density parity-check codes with properly chosen degree distributions, or multi-edge ensembles.

I will talk about a further such structure which emerges if we "couple" several of our favorite graphical models along a spatial dimension. Here, "coupling" means that we connect neighboring graphical models and we do it in such a way that the local connectivity of the graphs stays undisturbed. As I will explain, due to this spatial structure, and a well chosen boundary condition, such graphical models will behave under iterative decoding as well as if one had taken one of the underlying components and decoded it in an optimal fashion. I will explain why this happens and how we can take advantage of this effect.

Although most of this talk will center on how to design good error correcting codes, the principle of spatial coupling can also be used in other areas (such as compressive sensing or constraint satisfaction problems). Time permitting, I will briefly paint the broader picture.

List Error-Correction with Information-Theoretically Minimal Redundancy

Venkatesan Guruswami
Carnegie Mellon University

This talk will be about list decoding from worst-case errors which is a relaxation of classical error-correction allowing the decoder to output a small list of messages that includes the original message in cases where unambiguous recovery is not possible. This notion is of fundamental importance in coding theory and underlies some of its powerful applications to computational complexity and cryptography.

We will show the existence of codes that enable list decoding with information-theoretically optimal redundancy that is only ϵ-higher than the worst-case error fraction, for any desired $\epsilon > 0$. We will then discuss recent work in algebraic coding theory that has led to explicit and efficiently decodable codes approaching this optimal trade-off between rate and error-correction radius. This story will begin with algorithms to decode the classical Reed-Solomon codes, and then move on to optimal rate list decoding of a folded version of Reed-Solomon codes via a simple but versatile linear-algebraic approach. We will then discuss the idea pre-coding messages to "subspace-evasive sets" as a way to reduce the list size to a constant depending only on epsilon. Time permitting, we will sketch the notion of subspace designs which enables extensions of this approach to algebraic-geometric codes over constant-sized alphabets, and discuss how, curiously, one can explicitly construct good subspace designs using variants of Reed-Solomon codes.

We will try to conclude by highlighting some of the outstanding combinatorial and algorithmic open questions in list decoding.

The Complexity of Information-Theoretic Secure Computation

Yuval Ishai
Technion

Secure computation allows two or more parties to perform a distributed computation on their local inputs while hiding the inputs from each other. In the so-called "information theoretic" setting for secure computation, the parties may communicate over secure channels and the inputs should remain hidden even from computationally unbounded parties.

It is known that every function f can be computed securely when there is a majority of honest parties, or alternatively when the parties are given access to certain forms of correlated secret randomness. However, the true cost of such secure computations remains wide open.

The talk is divided into two parts. The first part will cover the complexity of private information retrieval, a useful special case of secure computation, and discuss its relation with locally decodable error-correcting codes and related problems. The second part will cover general secure computation protocols. Both parts will survey recent progress and open questions in the area.