Workshop on Complexity and Coding Theory, January 8-10, 2014

Wednesday, January 8

9:00-9:20 Coffee and Check-In
9:20-9:30 Opening Remarks
9:30-10:30 Codes and Pseudorandomness: A Survey, David Zuckerman (University of Texas at Austin)
10:30-11:00 Questions/Discussions/Break
11:00-12:00 Every List-Decodable Code for High Noise has Abundant Near-Optimal Rate Puncturings, Mary Wootters (University of Michigan)
12:00-13:00 Lunch
13:00-14:00 Direct Products in Communication Complexity, Anup Rao (University of Washington)
14:00-14:30 Questions/Discussions/Break
14:30-15:30 Exact Communication Complexity of Disjointness, Ankit Garg (Princeton University)
15:30-16:00 Questions/Discussions/Break
16:00-17:00 Optimal Unique and List Decoding for Interactive Communication, Klim Efremenko (University of Chicago)

Thursday, January 9

9:00-9:30 Coffee
9:30-10:30 One Little Edge, Michelle Effros (Caltech)
10:30-11:00 Questions/Discussions/Break
11:00-12:00 Creating Secrets Out of Erasures: a New Approach to Network Secrecy, Christina Fragouli (EPFL and UCLA)
12:00-13:00 Lunch
13:00-14:00 Constant rate PCPs for Circuit-SAT with sublinear query complexity, Swastik Kopparty (Rutgers University)
14:00-14:30 Questions/Discussions/Break
14:30-15:30 Locally Dense Codes, Daniele Micciancio (UCSD)
15:30-16:00 Questions/Discussions/Break
16:00-17:00 Incidence geometry and locally correctable codes, Shubhangi Saraf (Rutgers University)

Friday, January 10

8:30-9:00 Coffee

9:00-10:00 Semantic Security for the Wiretap Channel, Mihir Bellare (UCSD)

10:00-10:30 Questions/Discussions/Break

10:30-11:30 Private Interactive Communication Across an Adversarial Channel, Ran Gelles (UCLA)

11:30-12:00 Questions/Discussions/Break

12:00-13:00 Information Causality, Szemeredi-Trotter and Algebraic Variants of CHSH, Mohammad Bavarian (MIT)

13:00-13:30 Lunch

13:30- Excursion (location depending on weather)

Abstracts (by speaker)

Information Causality, Szemeredi-Trotter and Algebraic Variants of CHSH
Mohammad Bavarian (MIT)

CHSH_q is the following simple two-player game: two parties are given x,y in F_q uniformly at random, and each must produce an output a,b in F_q without communicating to the other. The players objective is to maximize the probability that their outputs satisfy a+b=xy in F_q. This game was introduced by Buhrman and Massar (Phys. Rev. A 72.5 (2005)) as a larger alphabet generalization of the CHSH game, which is one of the most well-studied games in quantum information theory, and which has large number of applications to quantum cryptography and quantum complexity. In this work, we obtain the first asymptotic results on the quantum and classical values of CHSH_q. The main result regarding the quantum value of CHSH_q is an upper bound of O(q^{-1/2}). Regarding the classical value of the game, we prove an upper bound O(q^{1/2-eps}) in the case of q=p^{2k-1}, and a tight lower bound of Omega(q^{-1/2}) for q=p^{2k}. A key observation that allows us to obtain the above bounds is a geometric view of CHSH_q} which reveals an intimate connection between this game and the celebrated finite field Szemeredi-Trotter theorem of Bourgain-Katz-Tao (GAFA 14.1 (2004)). This connection creates one of the first links between the study of multiplayer refereed games and arithmetic combinatorics, and may have applications to other areas. Beside the above, our work contains various other technical results of independent interest. For example, as an intermediate step in our quantum upper bound we prove a new variant of the principle of information causality, resolving an open problem of Pawlowski and Winter (Phys. Rev. A 85.2 (2012)).

Joint work with Peter W. Shor.

Semantic Security for the Wiretap Channel

Mihir Bellare (UCSD)

The wiretap channel is a setting where one aims to provide information-theoretic privacy of communicated data based solely on the assumption that the channel from sender to adversary is ``noisier'' than the channel from sender to receiver. It has developed in the Information and Coding (I&C) community over the last 30 years largely divorced from the parallel development of modern cryptography. Our work aims to bridge the gap with a cryptographic treatment involving advances on two fronts, namely definitions and schemes. On the first front (definitions), we explain that the mis-r definition in current use is weak and propose two alternatives: mis (based on mutual information) and ss (based on the classical notion of semantic security). We prove them equivalent, thereby connecting two fundamentally different ways of defining privacy and providing a new, strong and well-founded target for constructions. On the second front (schemes), we provide the first explicit scheme with all the following characteristics: it is proven to achieve both security (ss and mis, not just mis-r) and decodability; it has optimal rate; and both the encryption and decryption algorithms are proven to be polynomial-time.

Joint work with Stefano Tessaro (UCSB) and Alexander Vardy (UCSD).

Paper available at: http://cseweb.ucsd.edu/~mihir/papers/wiretap-crypto12.html

One Little Edge

Michelle Effros (Caltech)

Consider the impact of a single edge on the capacity of a network of noiseless, capacitated links. For example, if rate vector $(R_1,...,R_k)$ is achievable in a k-unicast network ${\cal N}$, is rate vector $(R_1-\delta,\ldots,R_k-\delta)$ achievable in the network ${\cal N}_\delta$ that results by removing a single edge of capacity δ from ${\cal N}$? This simple question lies at the heart of a surprising number of mysteries, a few of which will be described in this talk.

Optimal Unique and List Decoding for Interactive Communication

Klim Efremenko (University of Chicago)

In this talk, we will discuss how to encode an interactive protocol such that it will be resilient to adversarial noise. We will define an analogue of list decoding in one-way communication to the settings of interactive communication and show its limits. In particular, we will show that any protocol can be converted, with only constant stretch, to a list decoding protocol which is resilient up-to 1/2 fraction of the noise.

Then, we will study a more general model of noise where the adversary can corrupt up-to \alpha fraction of Alice's communication and up-to \beta fraction of Bob's communication. We use list decoding in order to compute the region R of pairs (\alpha, \beta) in which unique decoding is possible. The region R turns out to be quite unusual in its shape. In particular, it is bounded by a piecewise-differentiable curve with infinitely many pieces. This work improves Braverman and Rao work where they only considered a unique decoding where only the sum alpha+beta is bounded.

Joint work with Mark Braverman.

Creating Secrets Out of Erasures: a New Approach to Network Secrecy

Christina Fragouli (EPFL and UCLA)

We explore a new opportunity for security, that does not rely on the limited computational capabilities of an adversary, Eve, but instead, on her limited network presence. Current cryptographic methods rely on that Eve cannot perform sufficient fast certain operations, eg. large integer factorization. Instead, we can leverage the fact that she is not omnipresent in a wireless domain, and does not wiretap all links of a large wired network. We review and present a number of recent results, that range from information theoretical characterizations for erasure networks, to secure network coding bounds over arbitrary graphs, to testbed implementations.

Exact communication complexity of disjointness

Ankit Garg (Princeton University)

We determine the exact communication complexity of disjointness up to low order terms in the near zero-error regime. This is done by computing the exact zero-error information complexity of the 2-bit AND function. Towards this end, we develop a new local characterization of the zero-error information complexity function for two party communication problems.

Joint work with Mark Braverman, Denis Pankratov and Omri Weinstein.

Private Interactive Communication Across an Adversarial Channel

Ran Gelles (UCLA)

Say Alice and Bob hold private inputs x and y, and wish to compute a function f(x,y) privately in the information theoretic sense; that is, each party should learn nothing beyond f(x,y). However, the communication channel available to them is noisy and might introduce errors in the transmission between the two parties. Moreover, assume the channel is adversarial in the sense that it knows the protocol that Alice and Bob are running, and maliciously introduces errors to disrupt the communication, subject to some bound on the total number of errors. A fundamental question in this setting is to design a protocol that remains private in the presence of large number of errors.

If Alice and Bob are only interested in computing f(x,y) correctly, and not privately, then quite robust protocols are known that can tolerate a constant fraction of errors. However, none of these solutions is applicable in the setting of privacy, as they inherently leak information about the parties' inputs. In this talk we show that privacy and error-resilience are contradictory goals. In particular, we show that for every constant c > 0, there exists a function f(x,y) which is privately computable in the error-less setting, but for which no private and correct protocol is resilient against a c-fraction of errors.

Joint work with Amit Sahai and Akshay Wadia.

Constant rate PCPs for Circuit-SAT with sublinear query complexity

Swastik Kopparty (Rutgers University)

The PCP theorem says that every NP-proof can be encoded to another proof, namely, a probabilistically checkable proof (PCP), which can be tested by a verifier that queries only a small part of the PCP. A natural question is how large is the blow-up incurred by this encoding, i.e., how long is the PCP compared to the original NP-proof. The state-of-the-art results show that one can encode proofs for instances of size n by PCPs of length (n poly log n) that can be verified using a constant number of queries. In this work, we show that if the query complexity is relaxed to n^epsilon, then one can construct PCPs of length O(n) for circuit-SAT, and PCPs of length O(n log n) for all of NP. These PCPs have perfect completeness and constant soundness. This is the first constant-rate PCP construction that achieves constant soundness with nontrivial query complexity (o(n)).

Our proof relies on replacing the use of low-degree polynomials in PCP constructions with transitive algebraic geometry (AG) codes. In particular, we show that the automorphisms of an AG code can be used to simulate the role of affine transformations which are crucial in earlier high-rate algebraic PCP constructions. Using this observation we conclude that any asymptotically good family of transitive AG codes over a constant-sized alphabet --- like the family of AG codes presented by Stichtenoth in [Trans. Information Theory 2006] and in an appendix to this work --- leads to constant-rate PCPs with polynomially small query complexity.

Joint work with Eli Ben-Sasson, Yohay Kaplan and Or Meir, with an appendix by Henning Stichtenoth.

Locally Dense Codes

Daniele Micciancio (UCSD)

The Minimum Distance Problem (MDP), i.e., the computational task of evaluating (exactly or approximately) the minimum distance of a linear code, is a well-known NP-hard problem in coding theory. A key element in essentially all known proofs that MDP is NP-hard is the construction of a combinatorial object that we may call a "locally dense code". This is a linear code with large minimum distance d, that admits a ball of smaller radius r<d containing an exponential number of codewords, together with some auxiliary information used to map these codewords.

In this talk we provide a generic method to explicitly construct locally dense binary codes, starting from an arbitrary linear code with sufficiently large minimum distance. Instantiating our construction with well-known linear codes (e.g., Reed-Solomon codes concatenated with Hadamard codes) yields a simple proof that MDP is NP-hard to approximate within any constant factor under deterministic polynomial time reductions, simplifying and explaining recent results of Cheng and Wan (STOC 2009 / IEEE Trans. Inf. Theory 2012) and Khot and Austrin (ICALP 2011).

Our work is motivated by the construction of analogous combinatorial objects over integer lattices, which are used in NP-hardness proofs for the Shortest Vector Problem (SVP). We show that for the "max" norm, locally dense lattices can also be easily constructed. However, all currently known constructions of locally dense lattices in the standard Euclidean norm are probabilistic. Finding a deterministic construction of locally dense Euclidean lattices, would prove the NP-hardness of approximating SVP under deterministic polynomial time reductions, a long standing open problem in the computational complexity of integer lattices.

(Paper link: http://eccc.hpi-web.de/report/2013/115/)

Direct Products in Communication Complexity

Anup Rao (University of Washington)

In a given computational model, if there is a way to compute a function f on random inputs using C resources and probability of success rho, then one can usually compute the function on n independent inputs with nC resources and probability of success rho^n. But is this optimal? This kind of question is called the Direct Product question. We give new results in the setting of communication complexity. If suc(f, C) denotes the maximum success probability that can be achieved for computing f with C bits of communication, and f^n denotes the function that computes n copies of f, we show (ignoring constants) that suc(f^n, nC/polylog(nC)) is bounded by suc(f,C)^n. Prior to our work, it was known that suc(f^n,C) < suc(f,C)^n [Pernafes,Raz,Wigderson], and that suc(f^n,nC/polylog(n)) < suc(f,C), proved by [Barak,Braverman,Chen,Rao]. We give the first exponentially small bounds when the communication is allowed to increase. Our techniques involve new methods for compressing communication protocols.

Joint work with Mark Braverman, Omri Weinstein and Amir Yehudayoff.

Incidence geometry and locally correctable codes

Shubhangi Saraf (Rutgers University)

The classical Sylvester-Gallai theorem states the following: Given a finite set of points in the Euclidean plane, if the line through every pair of points passes through a third point, then all points must be collinear. Thus basically the result shows that many `local' linear dependencies implies a `global' bound on the dimension of the entire set of points. Variations of these questions have been well studied in additive combinatorics and incidence geometry. In the last few years, techniques from these areas have proven to be very useful for understanding the structure of locally decodable and locally correctable codes. In this talk I will describe several extensions to the Sylvester-Gallai theorem -quantitative versions, average case versions, approximate versions and high dimensional versions. I will also survey some recent results which use these incidence theorems to show new and strengthened lower bounds for locally correctable codes over the reals.

Based on joint works with Albert Ai, Zeev Dvir, Guangda Hu and Avi Wigderson.

Every list-decodable code for high noise has abundant near-optimal rate puncturings

Mary Wootters (University of Michigan)

We show that any q-ary code with sufficiently good distance can be randomly punctured to obtain, with high probability, a code that is list decodable with near-optimal rate and list sizes as the error rate approaches 1 - 1/q. Our results imply that "most" Reed-Solomon codes are list decodable beyond the Johnson bound; it was previously unknown whether any Reed-Solomon codes had this property. More precisely, we show that a Reed-Solomon code with random evaluation points is, with high probability, list decodable up to radius $1 - \epsilon$ with list sizes $O(1/\epsilon)$ and rate $\Omega(\epsilon)$. As a second corollary of our argument, we obtain improved bounds on the list decodability of random linear codes over large fields.

Our approach exploits techniques from high dimensional probability. Previous work used similar tools to obtain bounds on the list decodability of random linear codes, but the bounds did not scale with the size of the alphabet. In this paper, we use a chaining argument to deal with large alphabet sizes.

Joint work with Atri Rudra.

Codes and Pseudorandomness: A Survey

David Zuckerman (University of Texas at Austin)

We survey applications of error-correcting codes to the field of pseudorandomness. No knowledge of pseudorandomness will be assumed.