Interactive Information Theory
January 15-20, 2012

MEALS

*Breakfast (Buffet): 7:00–9:30 am, Sally Borden Building, Monday–Friday
*Lunch (Buffet): 11:30 am–1:30 pm, Sally Borden Building, Monday–Friday
*Dinner (Buffet): 5:30–7:30 pm, Sally Borden Building, Sunday–Thursday
Coffee Breaks: As per daily schedule, TransCanada Pipelines Pavilion (TCPL) foyer or 2nd floor lounge, Corbett Hall
***Please remember to scan your meal card at the host/hostess station in the dining room for each meal.**

MEETING ROOMS

All lectures will be held in Room 201 of the TransCanada Pipelines Pavilion (TCPL) and not the (usual) Max Bell Building. LCD projector, overhead projectors and blackboards are available for presentations. There is a 2nd floor lounge in Corbett Hall (where we sleep) which participants may use to converse and relax in. Beverages and a small assortment of snacks are available on a cash honor system. Please respect that all other space has been contracted to other Banff Centre guests, including any Food and Beverage in those areas.
The names in italics on the right are the informal "chairs" of the sessions.

SCHEDULE

Sunday	
16:00	Check-in begins (Front Desk - Professional Development Centre - open 24 hours)
	Lecture rooms available after 16:00 (if desired)
17:30–19:30	Buffet Dinner, Sally Borden Building
20:00	Informal gathering in 2nd floor lounge, Corbett Hall (if desired)
	Beverages and a small assortment of snacks are available on a cash honor system.
Monday	**Focus Topic: Interactive Source Coding and Computing**
7:00–8:45	Breakfast
8:45–9:00	Introduction and Welcome by BIRS Station Manager
9:00	9-9:30 OPENING REMARKS and participant introductions
	9:30-10:30 Mark Braverman
	Coffee Break, TCPL foyer - 10:30-11:00
	11:00-12:00 Babak Hassibi
12:00–13:15	Lunch
13:00–14:00	Guided Tour of The Banff Centre; meet in the 2nd floor lounge, Corbett Hall
Young-Han	14:30 - 15:00 Prakash Ishwar
	15:00-15:30 Nan Ma
	Coffee Break, TCPL foyer - 15:30-16:00
Mark	16:00-16:30 Jin Meng
	16:30-17:00 Anup Rao
	17:00 - 17:45 Open Problem Session
17:30–19:30	Dinner
19:30 - 22:00	Welcome to Canada! reception hosted by Natasha Devroye and Ashish Khisti in 2nd floor lounge, Corbett Hall

Tuesday	**Focus Areas: Interactive Channel Coding and Networking**
7:00–9:00	Breakfast
9:00 *Daniela*	9-10 Young-Han Kim
	10-10:30 Yossi Steinberg
	Coffee Break, 2nd floor lounge, Corbett Hall - TCPL foyer
Petar	11:00 - 11:30 Bobak Nazer
	11:30 - 12:00 Daniela Tuninetti
	12:00 - 12:30 Holger Boche
12:30–13:30	Lunch
13:45	Group Photo; meet on the front steps of Corbett Hall
Holger	14:00-14:30 Tobias Oechtering
	14:30-15:00 Petar Popovski
	15:00-15:30 Besma Smida
	Coffee Break, TCPL foyer - 15:30-16:00
Yossi	16:00-16:30 Ramji Venkataramanan
	16:30 - 17:00 Jean-Francois Chamberland
17:30–19:30	Dinner

Wednesday	**Focus Topic: Hypothesis Testing and and Energy Efficient Communication**
7:00–9:00	Breakfast
9:00 *Stark*	9:00-10:00 Rob Nowak
	10:00-10:30 Matt Malloy
	Coffee Break, TCPL foyer - 10:30-11:00
Aylin	11:00-11:30 Te Sun Han
	11:30-12:00 Sennur Ulukus
	12:00 - 12:30 Kaya Tutuncuoglu
12:30–13:30	Lunch
	Free Afternoon
17:30–19:30	Dinner

Thursday	**Focus Topics: Interactive Information Security and Other Applications**
7:00–9:00	Breakfast
9:00 *Rob*	9-10:00 Himanshu Tyagi
	10:00-10:30 Prakash Narayan
	Coffee Break, TCPL foyer - 10:30-11:00
Sennur	11:00-11:30 Frans Willems
	11:30-12:00 Aylin Yener
	12:00 - 12:30 Ashish Khisti
12:30–13:30	Lunch
Frans	14:00 - 14:30 Pulkit Grover
	14:30 - 15:00 Stark Draper
	15:00 - 15:30 Aditya Mahajan
	Coffee Break, TCPL foyer - 15:30-16:00
Ashish	16:00-16:30 Andrew Eckford
	16:30 - 17:00 Ersen Ekrem
17:30–19:30	Dinner

Friday	**Free time, open problems and discussions**
7:00–9:00	Breakfast
9:00	9:00-9:30
	9:30-10:00
	10:00-10:30
Checkout by 12 noon.	

** 5-day workshops are welcome to use BIRS facilities (2nd Floor Lounge, Max Bell Meeting Rooms, Reading Room) until 3 pm on Friday, although participants are still required to checkout of the guest rooms by 12 noon. **

Interactive Information Theory
January 15-20, 2012

Organizers:
Natasha Devroye (University of Illinois at Chicago, USA)
Ashish Khisti (University of Toronto, Canada)
Ian Blake (University of British Columbia, Canada)

ABSTRACTS
(in alphabetic order by speaker surname)

Speaker: **Holger Boche (joint Work with Moritz Wiese and Igor Bjelakovic)** (Technische Universitt Mnchen)
Title: *Conferencing Encoders for Compound and Arbitrarily Varying Multiple-Access Channel*
Abstract: In the first part of the talk we prove two coding theorems for the compound multiple-access channel (MAC) with an arbitrary number of channel states. The channel state information at the transmitters is such that each transmitter has a finite partition of the set of states and knows which element of the partition the actual state belongs to. The receiver may have arbitrary channel state information. The first coding theorem is for the case that both transmitters have a common message and that each has an additional private message. The second coding theorem is for the case where rate-constrained, but noiseless transmitter cooperation is possible. This cooperation may be used to exchange information about channel state information as well as the messages to be transmitted. The cooperation protocol used here is Willems conferencing. We show how this models base station cooperation in modern wireless cellular networks used for interference coordination and capacity enhancement. In particular, the coding theorem for the cooperative case shows how much cooperation is necessary in order to achieve maximal capacity in the network considered. In the second part of the talk we derive the capacity region of arbitrarily varying multiple-access channels with conferencing encoders for both deterministic and random coding. We obtain a dichotomy: either the channels deterministic capacity region is zero or it equals the two-dimensional random coding region. We determine exactly when either case holds. We also discuss the benefits of conferencing. For both the compound and the arbitrarily varying cases, we give the example of a channel which does not achieve any non-zero rate pair without encoder cooperation, but the two-dimensional random coding capacity region if conferencing is possible. Unlike compound multiple-access channels, arbitrarily varying multipleaccess channels may exhibit a discontinuous increase of the capacity region when conferencing is enabled. We use the arbitrarily varying multiple-access channel with conferencing encoders for an information-theoretic analysis of the performance of wireless networks with cooperating base stations disturbed by exterior interference.

Speaker: **Mark Braverman** (University of Toronto)
Title: *Tutorial on information complexity in interactive computing*
Abstract: We will discuss several new extensions of information-theoretic notions to the two-way communication setting. We use them to prove a direct sum theorem for randomized communication complexity, showing that implementing k copies of a functionality requires substantially more communication than just one copy.

More generally, we will show that information cost I(f) can be defined as a natural fundamental property of a functionality f, measuring the amount of information that the parties need to exchange in order to compute f. We will describe several new tight connections between I(f), direct sum theorems, interactive compression schemes, and amortized communication complexity.

Relevant papers:

1) ”How to Compress Interactive Communication”, B. Barak, M. Braverman, X. Chen, A. Rao, http://www.cs.washington.edu/homes/anuprao/pubs/directsum.pdf

2) ”Information equals amortized communication”, M. Braverman, A. Rao http://eccc.hpi-web.de/report/2010/083/

3) ”Interactive information complexity” M. Braverman http://eccc.hpi-web.de/report/2011/123/download

Speaker: **Jean-Francois Chamberland** (Texas A &M University)
Title: *Challenges and Potential Approaches in Combining Channels with Memory, Block Codes and Queues*
Abstract:

Speaker: **Stark Draper** (University of Wisconsin - Madison)
Title: *Reliability in streaming data systems with feedback*
Abstract:

Speaker: **Andrew Eckford** (York University)
Title: *Models and Capacities of Molecular Communication*
Abstract: What are the fundamental limits of diffusion-mediated molecular communication? This question, which has only recently attracted attention from information theorists, turns out to be surprisingly difficult. Not only is the communication medium unfamiliar to communication engineers; but the mathematical details of the communication environment are complicated. In this talk, we discuss mathematical models for molecular communication, which are both information-theoretically useful and physically meaningful; we discuss the difficulties of dealing exactly with these models; and we present some simplified scenarios in which capacity can be evaluated. Finally, we discuss the engineering and biological significance of these results.

Speaker: **Hesham El Gamal** (Ohio State University)
Title: *Proactive Wireless Networking*
Abstract:

Speaker: **Ersen Erkem** (University of Maryland)
Title: *The Vector Gaussian CEO Problem*
Abstract: We study the vector Gaussian CEO problem, where there are an arbitrary number of agents; each having a noisy observation of a vector Gaussian source. The goal of agents is to describe the source to a central unit, which wants to reconstruct the source within a given distortion. The rate-distortion region of the vector Gaussian CEO problem is unknown in general. Here, we provide an outer bound for the rate-distortion region of the vector Gaussian CEO problem. We obtain our outer bound by evaluating an outer bound for the multi-terminal source coding by means of a technique relying on the de Bruijn identity and the properties of the Fisher information. Next, we show that our outer bound strictly improves the other existing outer bounds. We show this strict improvement by providing a specific example, where there is a gap between our outer bound and the other existing outer bounds. Although our outer bound brings an improvement, we show that still our outer bound does not provide the rate-distortion region in general. In particular, we provide an example where the rate-distortion region is strictly contained in our outer bound.

Speaker: **Pulkit Grover** (Stanford University)
Title: *Interactive communication in circuits: understanding Shannon's ”magic trick”*
Abstract: Teaching an information theory class, a terribly soft-spoken instructor says “I am not going to speak louder or slower. Instead, I am going to ”mix” my information in such a way that you understand all of it as the lecture goes on.” This fascinating and counterintuitive proposition is inspired directly from one of the central concepts in information theory: Shannon's channel capacity. The capacity-concept proposes a doctrine widely followed in wireless communications: using bounded transmit power (”whispering”) even as the target error probability is lowered. What is the ”trick” to this magic? To understand this, for

VLSI-inspired models for encoding and decoding, I derive fundamental limits on the required interactive communication within the encoding/decoding circuits. I contend that these limits reveal the trick: they show that keeping the transmit power bounded even as the target error-probability is lowered fundamentally requires an unbounded increase in the encoding/decoding communication-complexity and power.

What if the goal is to minimize total (transmit + encoding + decoding) power? These limits show that the total-power-minimizing approach is neither Shannon-"whispering", nor uncoded transmission, but coding with unboundedly increasing transmit power. These limits also explain the empirical observations of practitioners: at short-distances, encoding/decoding power can dominate transmit power by orders of magnitude. I will argue that this is because the transmit-power-optimal codes fail spectacularly at minimizing total power. Then, I will describe our experimental work combining circuits and information theory that provides power-efficient code/decoder constructions that strongly depend on the communication distance and error probability.

Joint work with (theory) Andrea Goldsmith, Anant Sahai and (experimental) Karthik Ganesan, Yang Wen and Jan Rabaey.

Speaker: **Te Sun Han** (National Institute of Information and Communications Technology)
Title: *Trade-off of data compression and hypothesis testing*
Abstract:

Speaker: **Babak Hassibi** (Caltech)
Title: *Efficiently-Decodable Tree Codes for Erasure Channels*
Abstract:

Speaker: **Prakash Ishwar** (Boston University)
Title: *The Infinite-Message Limit of Interactive Source Coding*
Abstract: In distributed block source coding problems, multiround interaction can improve the communication efficiency of distributed computation. What is the ultimate limit of this efficiency when the number of messages is unbounded? Unlike asymptotics involving blocklength, rate, quantizer step-size and network size that have been explored in the literature, asymptotics involving an infinite number of messages, each with potentially infinitesimal rate, has not received much attention. This talk will sketch recent efforts to tackle this question for distributed computation in two-terminal and collocated networks.

Speaker: **Ashish Khisti** (University of Toronto)
Title: *Secret-Key Generation over Fading Channels*
Abstract: This talk will survey of known results on secret-key generation over wireless fading channels. Both coherent and non-coherent fading channels will be considered and both time-division and frequency division duplex systems will be surveyed. For some of these models, the results are a natural extension of the "channel wiretapper" (CW) model first proposed by Maurer and Ahlswede & Csiszar and the source emulation technique achieves capacity. In other cases the source emulation technique appears sub-optimal and new techniques are necessary. Some open problems will also be discussed.

Speaker: **Young-Han Kim** (UCSD)
Title: *On the role of interaction in network information theory*
Abstract:

Speaker: **Lifeng Lai** (University of Arkansas, Little Rock)
Title: *Information Theoretic Security with an Active Attacker*
Abstract:

Speaker: **Nan Ma** (University of California - Berkeley, USA)
Title: *The benefit of interaction in lossy source coding*
Abstract: In 1985 Kaspi provided a single-letter characterization of the sum-rate-distortion function for

a two-way lossy source coding problem in which two terminals send multiple messages back and forth with the goal of reproducing each other's sources. Yet, the question remained whether more messages can strictly improve the sum-rate-distortion function. Viewing the sum-rate as a functional of the distortions and the joint source distribution and leveraging its convex-geometric properties, we construct an example which shows that two messages can strictly improve the one-message (Wyner-Ziv) rate-distortion function. The example also shows that the multiplicative gain in terms of the ratio of the one-message rate to the two message sum-rate can be arbitrarily large, and simultaneously the ratio of the backward rate to the forward rate in the two message sum-rate can be arbitrarily small. Moreover, we construct a second example, where in addition to the above two properties, a third property also holds simultaneously: the additive gain in terms of the difference between the one-message rate and the two message sum-rate can be arbitrarily large.

Speaker: **Aditya Mahajan** (McGill University)
Title: *The stochastic control approach to real-time communication: an overview*
Abstract:

Speaker: **Matt Malloy** (University of Wisconsin - Madison)
Title: *Sequential testing in high dimensions*
Abstract: Sequential methods make use of information as it becomes available, creating an interactive connection between a sampling procedure and information gathered by that procedure. In this talk we explore sequential methods applied to sparse recovery problems, motivated by applications in both communications and biology. Surprisingly, sequential methods can result in a large reduction in the sample size needed to recover a sparse signal.

More specifically, we consider an n-dimensional vector $\mathbf{x}$ whose elements are drawn from one of two distributions, p_0 and p_1. Most of the elements are drawn from p_0, but a small number, s, are drawn from p_1. The goal is to identify the (unknown) locations of this sparse subset. Non-sequential testing schemes require at least $\log(n)/D(p_1||p_0)$ samples per dimension, where $D(p_0||p_1)$ is the KL-divergence from p_1 to p_0. In the high-dimensional and sparse regimes (n large, $s << n$) sequential methods can greatly reduce sample requirements. We begin by discussing a lower bound for any high dimensional sequential test. If the number of samples per dimension is less than $\log(s)/D(p_0||p_1)$ then no method can reliably determine the locations. Coordinate-wise sequential probability ratio tests (SPRT) can reliably identify the locations using $\log(s)/D(p_0||p_1)$ samples in expectation, achieving the lower bound.

Implementing an SPRT is often impractical, as it requires complete knowledge of p_0, p_1, and the level of sparsity. We consider and discuss a simple, robust alternative termed Sequential Thresholding (ST) that automatically adapts to unknown distribution parameters and sparsity levels. With some constraints on the sparsity, ST achieves the lower bound discussed above.

Speaker: **Jin Meng** (University of Waterloo, Canada)
Title: *Interactive Encoding and Decoding: Concept, Coding Theorems and Algorithm Design*
Abstract:

Speaker: **Prakash Narayan** (University of Maryland)
Title: *Multiple-access channels, feedback and secrecy generation*
Abstract: This talk, based on joint work with Imre Csiszar, deals with secrecy generation for multiaccess channel models. Connections are drawn to multiaccess transmission problems without secrecy constraints, and feedback. Open problems (especially those that flummoxed us) will be described.

Speaker: **Bobak Nazer** (Boston University)
Title: *Computation over Feedback Channels*
Abstract:

Speaker: **Robert Nowak** (University of Wisconsin - Madison)
Title: *Interactive Information Gathering and Statistical Learning*
Abstract: This talk will deal with the notions of adaptive and non-adaptive information, in the context of statistical learning and inference. Suppose that we have a collection of models (e.g., signals, systems, representations, etc.) denoted by X and a collection of measurement actions (e.g., samples, probes, queries, experiments, etc.) denoted by Y. A particular model x in X best describes the problem at hand and is measured as follows. Each measurement action, y in Y, generates an observation y(x) that is a function of the unknown model. This function may be deterministic or stochastic. The goal is to identify x from a set of measurements $y_1(x), ..., y_n(x)$, where y_i in Y, $i = 1, ..., n$. If the measurement actions $y_1, ..., y_n$ are chosen deterministically or randomly without knowledge of x, then the measurement process is non-adaptive. However, If y_i is selected in a way that depends on the previous measurements $y_1(x), ..., y_{i-1}(x)$, then the process is adaptive. Adaptive information is clearly more flexible, since the process can always disregard previously collected data. The advantage of adaptive information is that it can sequentially focus measurements or sensing actions to distinguish the elements of X that are most consistent with previously collected data, and this can lead to significantly more reliable decisions. The idea of adaptive information gathering is commonplace (e.g., humans and animals excel at this), but outside of simple parametric settings little is known about the fundamental limits and capabilities of such systems. The key question of interest here is identifying situations in which adaptive information is significantly more effective than non-adaptive information. The answer depends on the interrelationship between the model and measurement spaces X and Y. The talk will cover the general problem, connections to channel coding and compressed sensing, and more deeply consider two illustrative examples from machine learning.

Speaker: **Tobias Oechtering** (KTH, Sweden)
Title: *Transmit strategies for the bidirectional broadcast channel & latest results*
Abstract:

Speaker: **Petar Popovski** (Aalborg University)
Title: *Protocol Coding for Two-Way Relay Communication*
Abstract:

Speaker: **Anup Rao** (University of Washington)
Title: *Towards Coding for Maximum Errors in Interactive Communication*
Abstract:

Speaker: **Besma Smida** (Purdue University, USA)
Title: *On the utility of Feedback in Two-way Networks*
Abstract: The goal of this research is to provide a fundamental and practical understanding of the value of feedback in two-way networks. Feedback may improve data rates in several ways: in networks with perfect channel state information at the transmitter and receiver (CSITR), feedback may serve to increase rates by enabling the collaborative encoding or decoding of messages; in practical networks without CSITR, feedback has traditionally been used to either learn the channel state, or to request the re-transmission of a failed reception. In general, feedback has been studied from a one-way perspective, meaning data travels in one direction, and feedback often assumed to be perfect in the other. We propose a new unified framework which captures the key tradeoffs particular to two-way networks and presence of different types of feedback including quantized channel state information (Q-CSI), Automatic Repeat reQuest (ARQ) or extensions and combinations thereof.

Speaker: **Yossi Steinberg** (Technion)
Title: *The broadcast channel with action dependent states*
Abstract:

Speaker: **Daniela Tuninetti** (University of Illinois at Chicago)
Title: *Cooperation in interference channels*
Abstract:

Speaker: **Kaya Tutuncuoglu** (Penn State)
Title: *Interactive Transmission Policies for Energy Harvesting Wireless Systems*
Abstract:

Speaker: **Himashu Tyagi** (University of Maryland)
Title: Secrecy generation and secure computation
Abstract:

Speaker: **Sennur Ulukus** (University of Maryland)
Title: *Interacting with Nature: Information Theory of Energy Harvesting Communications*
Abstract:

Speaker: **Ramji Venkataramanan** (Yale University)
Title: *Interactive Codes for Synchronization from Insertions and Deletions*
Abstract: In this talk, we discuss efficient codes for synchronization from insertions and deletions. As an example, consider remotely located users who independently edit copies of a large file (e.g. video or text), where the editing may involve deleting certain parts of the file, and inserting new data in other parts. The users then want to synchronize their versions with minimal exchange of information, in terms of both the communication rate and the number of interactive rounds of communication. This problem has applications in online editing, file sharing, and data storage in the cloud. We focus on the case where the number of edits is small compared to the file-size, and describe an interactive synchronization algorithm which is computationally efficient and has near-optimal communication rate. The algorithm is based on a class of single-deletion correcting channel codes due to Varshamov and Tenengolts. Time permitting, we will also discuss the case where the number of edits is large (a constant fraction of the file-size), and obtain fundamental limits on the optimal communication rate.

Speaker: **Frans Willems** (TU Eindhoven)
Title: *Authentication based on secret generation*
Abstract: We consider authentication protocols in which, during enrollment, a secret and helper data are extracted by an encoder from the enrollment sequence of an individual. The helper data is stored in a public database and the secret is sent to an authenticator via a protected link. During authentication the (legitimate) individual again presents a sequence to the decoder that forms an estimate of the enrollment secret making use of the helper data. This estimated secret is handed over to the authenticator. The authenticator decides that the individual is legitimate if the estimated secret equals the enrollment secret. On the other hand an impostor could generate a sequence based on the public helper data and try to get authenticated in this way. We investigate the fundamental limit for this scenario. We show that there exist encoders and decoders that achieve an arbitrarily small false-reject rate, while on the other hand the so-called false-accept exponent can be as large as the mutual information between the enrollment and observation samples in the i.i.d. case, for any impostor. We also consider the trade-off between false-accept exponent and privacy-leakage rate. Also for this setting we found the fundamental limits. The scenarios described here can be regarded as extensions of the results of Ahlswede and Csiszar [1993] on secret sharing and of the results of Ignatenko and Willems [2009], and Lai, Ho, and Poor [2011] on the secret-key versus privacy-leakage trade-offs. Joint work with Tanya Ignatenko (Philips Research, Eindhoven)

Speaker: **Aylin Yener** (Penn State University)
Title: *The Gaussian two-way wiretap channel: Then and Now*
Abstract: