Introduction

Our laboratory formulates, examines, and develops algorithmic solutions to a wide spectrum of problems of fundamental interest involving the manipulation of signals and information in diverse settings. Our work is strongly motivated by and connected with emerging applications and technologies.

In pursuing the design of efficient algorithm structures, the scope of research within the lab extends from the analysis of fundamental limits and development of architectural principles, through to implementation issues and experimental investigations. Of particular interest are the tradeoffs between performance, complexity, and robustness.

In our work, we draw on diverse mathematical tools—from the theory of information, computation, and complexity; statistical inference and learning, signal processing and systems; coding and communication; and networks and queuing—in addressing important new problems that frequently transcend traditional boundaries between disciplines.

We have many joint projects and collaborate closely with faculty, staff, and students in a variety of other labs on campus, including the Laboratory for Information and Decision Systems, the Microsystems Technologies Laboratories, and Computer Science and Artificial Intelligence Laboratory.

Much of our activity over the last few years has centered around a variety of different types of problems arising naturally in the context of wireless, sensor, multimedia, and broadband networks.

---

1 Dept. Electrical Engineering and Computer Sciences, University of California, Berkeley
2 Department of Electrical Engineering, Tel-Aviv University, Israel
3 NEC Corporation, Intelligence Systems Department, Tokyo, Japan
4 Department Electrical Engineering, Swiss Federal Institute of Technology (ETH), Zurich, Switzerland
5 Mitsubishi Electric Research Laboratories, Cambridge, Mass.
Some topics of current interest include:

- cross-layer design techniques and architectural considerations for resource-efficient wireless networks
- coding for multiple-element antenna arrays in wireless networks, and interactions with other layers; advanced antenna designs
- new classes of source and channel codes, and decoding algorithms, particularly for new applications
- diversity techniques and interference suppression and management algorithms for wireless networks
- distributed algorithms and robust architectures for wireless networks, especially ad-hoc networks and sensor networks
- algorithms and fundamental limits for multimedia security problems, including digital watermarking, encryption, and authentication of multimedia content
- algorithms and architectures for multimedia and streaming media networks
- algorithmic and coding techniques for generating reliable advanced systems from aggressively scaled devices, circuits, and microsystems.
- information-theoretic and algorithmic aspects of learning, inference, and perception; universal algorithms
- information-theoretic and signal processing aspects of neuroscience, and computational and systems biology

Projects

1. High Resolution Pipelined Analog-to-Digital Conversion Using Comparator-Based Switched-Capacitor Techniques

Sponsors
National Defense Science and Engineering Graduate (NSDEG) Fellowship
CICS (Center of Integrated Circuits and Systems)
Lincoln Laboratory ACC

Project Staff
Lane Brooks, Harry Lee and Professor Gregory W. Wornell

Recently, a new method of switched capacitor circuit design called comparator-based switched-capacitor circuit (CBSC) design methodology was introduced that replaces op-amps with comparators. This research seeks to realize the advantages of CBSC with the application to high-resolution pipelined analog-to-digital converters (ADC). The specific goal is to design and fabricate a 12 bit, 1 GHz, 10 mW ADC. This type of ADC has applications such as software radio, general test equipment, wide bandwidth modems, smart radios for wireless communications, advanced radar systems, multi-beam adaptive digital beam-forming array transceivers, and anti-jam GPS receivers. Theoretically CBSC offers more than an order of magnitude improvement in Figure of Merit (FOM) over traditional op-amp based pipelined ADCs. This means, for example, that for the same speed and resolution, a CBSC ADC can operate with more than an order of magnitude lower power consumption. The FOM advantages of CBSC come from reduced bandwidth requirements, reduced device count, reduced complexity, increased voltage range, and increased power efficient biasing.

This project seeks to develop new circuit techniques and optimize timing and architecture to achieve an aggressive design goal. The work has been divided into two prototype chips. First, a single-ended prototype is being fabricated that seeks to realize a 10 bit CBSC pipelined ADC at 500 MHz. This design embodies innovative techniques such that no static current is required in the entire ADC and only dynamic power is consumed. The goal was to focus on speed at a lower resolution. A second prototype will be developed that will be fully differential and improve the
resolution to 12 bits. In addition, channels will be time-interleaved to achieve the desired speed goal of 1 GHz.

2. Iterative Algorithms for Lossy Source Coding

Sponsors
NSF Grant No. CCF-0515109
Hewlett Packard through MIT/HP Alliance

Project Staff
Venkat Chandar, Emin Martinian, Pascal Vontobel and Professor Gregory W. Wornell

This research explores the problems of lossy source coding and information embedding. Lossy source coding is used in many widely-used algorithms such as JPEG or MPEG. Our goal is to design efficient lossy source codes. Because real-world sources such as audio or video are so complex, we consider a simple theoretical model called the binary symmetric source under a Hamming distortion. By drawing on tools from channel coding, including low density parity check codes and belief propagation techniques, we want to develop low-complexity source codes that can achieve the optimal tradeoff between compression rate and distortion.

Another related problem we are looking at is information embedding. This problem combines aspects of lossy source coding and channel coding. We have already found a capacity-achieving code construction for a simple information embedding model we call the double-erasure information embedding model. In future work, we plan to generalize this work to other channel models.

3. Calibration of Time-Interleaved Analog-to-Digital Converters

Sponsors
National Defense Science and Engineering Graduate (NSDEG) Fellowship
Lincoln Laboratory ACC

Project Staff
Vijay Divi and Professor Gregory W. Wornell

The performance of high-resolution time-interleaved analog-to-digital converters is often significantly degraded by timing mismatch errors. We examine low-complexity methods for performing blind calibration of such converters. In particular, we develop a least squares formulation for estimating the unknown time-skew parameters and for performing signal reconstruction from these estimates. The complexity of the proposed algorithm scales linearly with the number of converters, making it an attractive solution for calibration. We also examine signal recovery in the cases of low bit-depth and large numbers of converters.


Sponsors
MARCO/DARPA C2S2 Contract No. 2003-CT-888
Lincoln Laboratory

Project Staff
Everest Huang and Professor Gregory W. Wornell

When designing wireless communication systems, most hardware details are hidden from the
algorithm designer, especially with analog hardware. While it is difficult for a designer to understand all aspects of a complex system, some knowledge of circuit constraints can improve system performance by relaxing design constraints. The specifications of a circuit design are generally not equally difficult to meet, thus excess margin in one area can be used to relax the more difficult design constraint.

In the context of a wireless gigabit network (WiGLAN), we first propose an uplink/downlink architecture for a network with a multiple antenna central server. This design takes advantage of the central server to allow the nodes to achieve multiplexing gain by forming virtual arrays without coordination, or diversity gain to decrease SNR requirements. Computation and memory are offloaded from the nodes to the server, allowing less complex, inexpensive nodes to be used.

We can further use this SNR margin to reduce circuit area and power consumption, sacrificing system capacity for circuit optimization. Besides the more common transmit power reduction, large passive analog components can be removed to reduce chip area, and bias currents lowered to save power at the expense of noise figure. Given the inevitable crosstalk coupling between circuits, we determine the minimum required crosstalk isolation in terms of circuit gain and signal range. Viewing the crosstalk as a static fading channel, we derive a formula for the asymptotic SNR loss, and propose phase randomization to reduce the strong phase dependence of the crosstalk SNR loss.

The high peak to average power ratios (PAPR) that results from multicarrier systems pose difficult linearity and dynamic range requirements for analog circuits, resulting in low power efficiencies. We propose two algorithms, both of which can decrease the PAPR by 4~dB or more, resulting in an overall power reduction by a factor of three or more in the high and low SNR regimes, when combined with an outphasing linear amplifier.

5. Side-Information and Constraints in Media Coding Performance

Sponsors
NSF Graduate Research Fellowship
Hewlett Packard through MIT/HP Alliance

Project Staff
Ying-zong Huang, Emin Martinian, and Professor Gregory W. Wornell

The problem of coding of media data for delivery over unreliable networks has additional features compared to generic source- and channel- coding. One, high rates of compression can be achieved with little apparent perceivable quality loss, if side-information about the distortion measure can be extracted and used by the encoder efficiently. Two, media delivery is often subject to stringent delay constraints, such as in the context of streaming or interactive applications. The purpose of this research is to explore the possible gains and fundamental limits in performance that come with systems endowed with these features.

In one manifestation of this research problem, we observed that partial coding of an i.i.d. binary source, with encoder side-information indicating which bits to code, performs as poorly as a trivial scheme, as soon as delay is prohibited in the encoder. We further found that if causality is relaxed, the source is amenable to universal coding by a Lempel-Ziv type scheme.

In another manifestation of the research problem, we investigated competitive performance of joint source-channel coding strategies in delay-constrained transmission of sources with memory. In particular, we investigated end-to-end distortion performance when data is sent over a packet erasure channel. We found that at high rate, distortion due to erasure losses of a predictively coded Gauss-Markov packet source is linearly additive.
6. Variable Partition Codes for Wyner-Ziv Coding and Information Embedding.

**Sponsors**
NSF Grant No. CCF-0515109
Hewlett Packard under the HP/MIT Alliance

**Project Staff**
Ashish Khisti, Emin Martinian, Professor Gregory W. Wornell

The problem of source coding with decoder side information has found numerous applications in areas ranging from low complexity video coding to sensor networks. Traditionally, the side information at the decoder is modeled as a noisy version of the source signal with a given correlation model. However, the reliability across all the samples is the same. In this work we relax this latter assumption and consider a situation, where the decoder has access to a noisy side information and "knows" how noisy each sample is. Both information theoretic limits and practical code constructions based on variable partition codes are studied.

A related problem is information embedding when the encoder exploits sensitivity of the source samples. The natural intuition is that the encoder can embed more information in less sensitive samples. We again demonstrate the use of variable partition codes for this setting and identify regimes in which they are information theoretically optimal. An information theoretic study for the case of intentional attacks is also being investigated and near optimal coding schemes which are robust to such attacks have been developed.

7. Information Theoretic Limits for Key Distribution in Wireless Networks with Multiple Antenna Transmitter

**Sponsors**
NSF Grant No. CCF-0515109
Hewlett Packard under the HP/MIT Alliance

**Project Staff**
Ashish Khisti, Aslan Tchamkerten, and Professor Gregory Wornell

Traditional cryptographic solutions implicitly assume an offline key distribution mechanism and focus on encryption when the sender and receiver have a common key not available to an eavesdropper. Many emerging applications challenge this assumption. One application is pay TV broadcast, where it is desirable to encrypt each program with a separate key so that only users who pay for a certain program can view it. The key must be useless once the broadcast of a particular program terminates. Another application is sensor networks. It is desirable to periodically update the key so that key cannot be stolen from the nodes.

In this work, we study efficient mechanism to distribute keys in a wireless medium. We model the problem as a transmitter with multiple antennas intending to broadcast a key to a receiver or a group of receivers under the constraint that an eavesdropper cannot decode the key. Our approaches investigate the importance of artificial noise, opportunistic communication and smart array processing for this application.

8. Rateless Codes for Gaussian Multiple Access Channel

**Sponsors**
NSF Rateless Grant No. CCF-0515122
Draper Laboratory
Chapter 4. Signals, Information, and Algorithms

Project Staff
Urs Niesen, Uri Erez, Devavrat Shah, and Professor Gregory Wornell

We consider communication over the Gaussian multiple access channel with unknown set of active users. The proposed multiple access strategy is distributed and achieves a maximum sum rate point on the boundary of the capacity region for this channel for any set of active users $S$ simultaneously, as if $S$ were known at the transmitters. The proposed coding scheme splits each user into a set of virtual users, each of which can be decoded using a single-user decoder at the receiver instead of having to decode all users jointly. We also present a generalization of this scheme to the case where the channel gains differ between users and each user only knows its own channel gain.

9. Universal Codes for Parallel Gaussian Channels

Sponsors
Hewlett Packard under the HP/MIT Alliance
NSF Grant No. CCF-0515122

Project Staff
Maryam Modir Shanechi, Professor Gregory Wornell and Uri Erez

We study the design of universal codes for parallel Gaussian channels with 2 sub-channels present. We study the universality both in terms of the uncertainty in the relative quality of the two sub-channels for a fixed maximum rate and in terms of the uncertainty of the achievable maximum rate. In our architecture, we will convert the parallel Gaussian channel into a set of scalar Gaussian channels and use good base codes designed for the corresponding scalar channel in the coding schemes.

One scheme developed is a universal layered code with deterministic dithers. A minimum mean squared error (MMSE) receiver combined with successive cancellation is used for decoding. An alternative universal code developed, which is also extended to be rateless, is a sub-block structured code symmetric with respect to all layers. The decoder uses a maximal ratio-combining (MRC) receiver combined with successive cancellation. We examine the efficiency performance of these two schemes and the effect of different design parameters on this performance.

10. Efficient Scheduling and Quantization for MIMO Broadcasting Systems with Limited Feedback

Sponsors
NSF under Grant No. CNS-0434974
Mitre Corporation

Project Staff
Charles Swannack, Elif Uysal-Biyikoglu and Professor Gregory Wornell

There is growing interest in the development of efficient wireless broadcast systems for distributing independent data streams to different users over some geographical area. It is now widely appreciated that the use of a multiple-element antenna array at the transmitter can, in principle, greatly increase the capacity of such systems. When the number of users is no larger than the array size, the system design issues are rather well understood. Moreover, when it is desirable for complexity or other reasons to restrict one’s attention to case of linear multiplexing, the literature characterizing the associated performance tradeoffs is particularly extensive.

By contrast, comparatively little is known about how to design efficient systems when the number
of users becomes large relative to the array size, and in particular the nature of the fundamental tradeoffs between throughput, complexity, and feedback in such settings. Ultimately, the underlying scheduling problem is rather different and in many ways richer than that of more traditional networks.

We develop and analyze a simple, low-complexity system architecture for scheduling over a Gaussian multiple-input multiple-output (MIMO) broadcast channel with infinite message backlogs. In the system of interest, there is a transmitter with \( m \) antennas, and \( n \) receiving users, where \( n \gg m \). We show that the proposed architecture is strongly asymptotically optimal with respect to average throughput. We further characterize the feedback requirements of the architecture, and highlight various tradeoffs available to the system designer.

### 11. Information Theoretic Perspectives on Synchronization

**Sponsors**
NSF Grant CCF-0515122  
University IR&D Grant from Draper Laboratory

**Project Staff**
Alsan Tchamkerten, Ashish Khisti, and Professor Gregory Wornell

In Information Theory, a common assumption is that "whenever the transmitter speaks the receiver listens". In other words, in general, there is the assumption of perfect synchronization between the transmitter and the receiver, and, basic quantities, such as the channel capacity and the coding delay, are defined under this hypothesis. In practice, this assumption is rarely fulfilled; due to the spasmodic nature of the information source, the transmitter may start emitting at random moments, and the receiver needs a certain period of time to realize that the transmitter has started to emit information. The goal of the present project is to model the notion of synchronization, incorporate it as a basic notion into Information Theory, and propose high rate and reliable coding schemes that minimize the penalty due to a lack of synchronization.

The motivation for this project is twofold. First, in practice synchronization requires a non-negligible amount of energy to be spent in addition to the energy used for transmitting information. Hence, short and efficient synchronization procedures are needed. Second, formulating basic quantities, such as the capacity and the reliability function of a channel, taking into account the notion of synchronization may lead to new performance criteria as well as new channel coding designs.

### 12. Tracking Stopping Times

**Sponsors**
NSF Grant CCF-0515122  
University of IR&D Grant from Draper Laboratory

**Project Staff**
Alsan Tchamkerten, and Urs Niesen

Consider a sensor that monitors the seismic activity of a volcano, and sequentially sends the data to a remote analyzer. The analyzer, by observing only a noisy version of the collected data, has to raise an alarm as soon as an eruption is imminent. What is the loss in "forecast precision" incurred because of the noise? If the noise is strong enough so that the analyzer receives data that are almost independent from the ones obtained by the sensors, most of the time the analyzer will raise false-alarms, or alarms that come too late. At the opposite, if the analyzer gets
the same data as the sensor, “optimal forecasting” might be possible.

The above situation provides a motivation for the project defined by the following generic problem. Consider two sequences of random variables \( X = X_1, X_2, \ldots \) and \( Y = Y_1, Y_2, \ldots \). We assume that \( X \) and \( Y \) are correlated in the sense that, for all \( i \geq 1 \), given that \( X_i = x \) the symbol \( Y_i \) is distributed according to a conditional distribution \( Q(.|x) \). Suppose that Alice observes \( X \) and that she chooses a stopping time \( T \) with respect to \( X \). Observing only \( Y \), what is the best stopping time \( S \) Bob can find so that to minimize the delay \((S - T)^+\) while keeping the probability of false-alarm (given by the event \( T < S \)) below a certain threshold? In the language of the above example, Alice and Bob represent the sensor and the analyzer respectively, \( Q \) models the noise, \( T \) the optimal time to raise an alarm given perfect observations, and \( S \) the optimal time to raise an alarm given corrupted observations.

13. New Upper and Lower bounds on the Information Rate of Finite-State Channels

**Sponsors**
Hewlett Packard through the MIT/HP Alliance

**Project Staff**
Pascal O. Vontobel

Arnold, Loeliger, and Vontobel (Allerton Conference 2002) presented some auxiliary-channel-based upper and lower bounds on the information rate of finite-state channels. These bounds can be estimated efficiently to a precision that is sufficient for any engineering-type application. Moreover, the better the auxiliary channel models the finite-state channel, the tighter are the bounds. We have now derived new upper and lower bounds on the information rate of finite-state channels.

14. Enumeration of Pseudo-Codewords

**Sponsors**
NSF Grant CCF-0515109
HP through MIT/HP Alliance

**Project Staff**
Pascal O. Vontobel, Charles Swannack

In order to understand the performance of a code under maximum-likelihood (ML) decoding, one studies the codewords, in particular the minimal codewords, and their Hamming weights. In the context of linear programming (LP) decoding, one's attention needs to be shifted to the pseudo-codewords, in particular to the minimal pseudo-codewords, and their pseudo-weights. In this project we study techniques to obtain average pseudo-weight enumerators of certain pseudo-codewords where the average is taken over a specified class of low-density parity-check (LDPC) codes where the block length goes to infinity.

15. Dense Wireless Transmit and Receive Antenna Array

**Sponsors**
DARPA Contract No. HR0011-06-1-0004
MARCO/DARPA C2S2 Contract No. 2003-CT-888
A dense wireless antenna array consists of a regularly aligned set of antennas distributed in a spatial region (length, area, or volume). From antenna principles and sampling theorem, the number of degrees of freedom for any array occupying this region is determined solely by the size of the region (normalized by wavelength) and the aimed overall angular coverage of the communication system. The dense array has the number of antennas considerably larger than the number of degrees of freedom associated with the array’s spatial region. Thus the dense antenna array can be seen as an “over sampling” array.

When used in wireless transmitters, the antennas of the dense array are connected to an RF stage that consists of a signal splitter followed by a set of discrete-level phase shifters and fixed-level power amplifiers. (The outputs from the power amplifiers are fed to the antennas.) The fixed-level power amplifiers generate high-power RF waves with constant amplitude, and the discrete-level phase shifters take four phase values. These phase values, which correspond to the phase-shift values at distinct antennas, are determined from a set of antenna weights (including amplitudes and phases) through a process of direct spatial sigma-delta quantization. With this architecture, the discrete over sampling array guarantees to generate any radiation pattern that can be generated by a non-over sampling array whose antenna weights are continuous in both amplitude and phase.

When used in wireless receivers, the antennas of the dense array are connected to an RF stage that includes a set of low-noise amplifiers, phase shifters, and amplitude adjusters, followed by a coherent signal adder. (The antennas are connected to the inputs of the amplifiers.) The size of each antenna is made small so that the received interference at the antenna is not strong enough to overload the RF low-noise amplifier. The weak received signals owing to the reduced antenna size are compensated by the numerous coherent signal paths (i.e., the numerous antennas) so that the overall signal-to-noise ratio at the output of the coherent signal adder remains high.

The dense antenna array improves over existing antenna arrays by releasing the technical requirements on RF circuits while maintaining the same system performances. At the transmitter side, the dense array needs the phase shifters operating at only four phase values and the power amplifiers whose outputs have constant amplitude. That means neither the power amplifiers nor the phase shifters have to be analog, linear devices, as those in the majority of array transmitters’ RF stage. This is an important advantage for RF design engineers, since maintaining the linearity of power amplifiers and high-power phase shifters have been major design challenges, and its solution often involves complex circuit designs with high manufacturing cost. At the receiver side, the dense array and its associated RF stage can provide an RF output with sufficiently high overall signal-to-noise ratio, but impose lower requirements on individual low-noise “amplifiers” noise figures and linearity. The smaller antennas take a lesser chance for the environmental interference to saturate the low-noise amplifiers, so the amplifiers do not have to maintain a large dynamic range. Meanwhile, the numerous coherent signal paths not only compensate for weaker individual antenna signals, but also raise the overall signal-to-noise ratio. Therefore, the “amplifiers” noise-figure requirement can be reduced with the dense antenna array. Low noise level and large dynamic range have been two major challenges for the designs of low-noise amplifiers, another type of RF analog, linear circuits. The design solutions often require semiconductor materials other than silicon and special processing and manufacturing technologies. With the dense antenna, however, we can release the demands on the RF low-noise “amplifiers” noise figure and dynamic range, and probably implement the amplifiers on silicon chips using less elaborate processing technologies. This can considerably cut down the manufacturing cost of the amplifiers.
Chapter 4. Signals, Information, and Algorithms

Publications

Journal Articles


Conference Proceedings, Published


Chapter 4. Signals, Information, and Algorithms


Book Chapters


Theses & Dissertations

Chapter 4. Signals, Information, and Algorithms

