Signals, Information, and Algorithms

RLE Group
Signals, Information and Algorithms Laboratory

Faculty
Professor Gregory W. Wornell

Visiting Scientists and Research Affiliates
Dr. Uri Erez[1], Hiroyuki Ishii[2], Dr. Emin Martinian[3], Prof. Venugopal Veeravalli[4], Dr. Aslan Tchamkerten[5], Dr. Chen-Pang Yeang[6], Prof. Ram Zamir[7]

Postdoctoral Scholars
Dr. Yuval Kochman[8]

Graduate Students
Anthony Accardi, Lane Brooks, Venkat Chandar, Vijay Divi, Ying-Zong Huang, James Krieger, Ashish Khisti, Maryam Shanechi, Urs Niesen, Charles Swannack, Da Wang

Visiting Students
V. Sreekanth Annapureddy[4]

Technical and Support Staff
Tricia O'Donnell

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.

---

[1] Department of Electrical Engineering, Tel-Aviv University, Israel
[2] NEC Corporation, Intelligence Systems Department, Tokyo, Japan
[3] Mitsubishi Electric Research Laboratories, Cambridge, Mass.
[4] University of Illinois at Urbana-Champaign, Chicago, Illinois
[5] Telecom ParisTech, Communications and Electronics Department, Paris, France
[6] University of Toronto, Toronto, Canada
[7] Department of Electrical Engineering, Systems Division, Faculty of Engineering, Tel-Aviv University, Israel
[8] Department of Electrical Engineering, Systems Division, Tel-Aviv University, Israel

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.

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
- sensing and imaging technologies
- information-theoretic and signal processing aspects of neuroscience, and computational and systems biology

Projects

1. Quasi Light Fields for Coherent Imaging

Sponsors
Microsoft Research
MIT Lincoln Laboratory
Semiconductor Research Corporation through the FCRP Center for Circuit & System Solutions No. 2003-CT-888 (C2S2)

Project Staff
Anthony Accardi, J. Chu, K. Nguyen, Professor Gregory Wornell, Professor Hae-Seung Lee and Professor Charles Sodini

The light field represents radiance as a function of position and direction, thereby decomposing optical power flow along rays. The light field is an important tool used in many imaging applications in different disciplines, but is traditionally limited to incoherent light. Our goal is to provide a model of coherent image formation that combines the utility of the light field with the comprehensive predictive power of Maxwell's equations.

Our contribution is to describe and characterize all the ways to extend the light field to coherent radiation, and to interpret coherent image formation using the resulting extended light fields. We call our extended light fields "quasi light fields", which are analogous to the generalized radiance functions of optics, the quasi-probability and phase-space distributions of quantum physics, and the quadratic class of time-frequency distributions of signal processing. We explain how to formulate, capture, and form images from quasi light fields. Our results generalize the classic beam forming algorithm used in sensor array processing.

Quasi light fields are attractive to researchers who desire more versatility than traditional energy-based methods, yet a more specialized model of image formation than Maxwell's equations.

2. The Capacity Region of Asynchronous Channels

Sponsors
NSF Grant No. CCF-0635191
DoD MURI Grant No. N00014-07-1-0738

Project Staff
Venkat Chandar, Aslan Tchamkerten, Professor Gregory Wornell

A formulation of the problem of asynchronous point-to-point communication is developed. In the system model of interest, the message codeword is transmitted over a channel starting at a randomly chosen time within a prescribed window. The length of the window scales exponentially with the codeword length, where the scaling parameter is referred to as the asynchronism exponent. The receiver knows the transmission window, but not the transmission time.

Communication rate is defined as the ratio between the message size and the elapsed time between when transmission commences and when the decoder makes a decision. Under this model, several aspects of the achievable tradeoff between the rate of reliable communication and the asynchronism exponent are quantified. First, the use of generalized constant-composition codebooks and sequential decoding is shown to be sufficient for achieving reliable communication under strictly positive asynchronism exponents at all rates less than the capacity of the synchronized channel. Second, the largest asynchronism exponent under which reliable communication is possible, regardless of rate, is characterized. In contrast to traditional communication architectures, there is no separate synchronization phase in the coding scheme. Rather, synchronization and communication are implemented jointly. Finally, inner and outer bounds are given on the capacity region of a general asynchronous DMC.

The results are relevant to a variety of sensor network and other applications in which intermittent communication is involved.

3. Locally Encodable and Decodable Source Codes

Sponsors
Microsoft Research
NSF Grant No. CCF-0515109

Project Staff
Venkat Chandar, Professor Gregory Wornell, Assistant Professor Devavrat Shah

In a variety of applications, ranging from high-speed networks to massive databases, there is a need to maintain histograms and other statistics in a streaming manner. Motivated by such applications, we establish the existence of efficient source codes that are both locally encodable and locally decodable. In the formulation of interest, N integers are to be stored in a data structure such that:
(a) they are represented in an efficiently compressed format; and (b) each of the integers can be both written/updated (encoded) and read (decoded) in essentially constant time. By contrast, existing data structures that have been proposed in the context of streaming algorithms and compressed sensing in recent years (e.g., various sketches) support local encodability, but not local decodability---to read even a single integer requires decoding the entire data structure.

Our solution is an explicit construction in the form of a (randomized) data structure that: (a) utilizes minimal possible space, and (b) takes near constant time (on average and with high probability) to read (decode) or write/update (encode) any of the N integers. Our construction uses multi-layered sparse graph codes based on a combination of Ramanujan graphs and the zigzag product.

4. Faster than Nyquist Signaling for Underwater Communication Channels

Sponsors
DoD MURI Grant No. N00014-07-1-0738

Project Staff
Dr. Vijay Divi, Dr. Uri Erez, Dr. James Preisig, Professor Gregory Wornell

We research methods for transmitting information in the underwater channel. While a variety of methods have been developed for wireless communication in the traditional air medium, the water channel introduces a new set of complications that require novel approaches. In particular, the ocean environment presents a large amount of inter-symbol interference (ISI) and a rapidly time-varying channel.

Our communication approach uses faster-than-Nyquist (FTN) signaling, where symbols are transmitted faster than the Nyquist rate of the transmit band. The method exploits the fact that the added ISI due to FTN is minimal in comparison to the ISI of the channel. The project focuses on the development of receiver architectures for such systems. By increasing the signaling rate, while decreasing the bits per symbol, FTN signaling can provide an increase in overall rate and allow for low-complexity implementations of acknowledgment messages and multi-rate coding.

Experimental data for the FTN transmit method has been attained during the SPACE08 experiment conducted by the Woods Hole Oceanographic Institute. Using a single transmit hydrophone and multiple receive hydrophone arrays, data was collected underwater over a month long period at distances of 60m, 200m, and 1000m. The current multiple hydrophone receivers we have developed show promise for providing an advancement in underwater communication rate by using FTN methods.

5. Low Latency Delivery of Lossless and Degradable Streams

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

Project Staff
Ying-zong Huang, Dr. Yuval Kochman, Dr. Emin Martinian, Professor Greg Wornell

Interactive Internet Applications that rely on sequential streams for lossless data exchange often use retransmission protocols (e.g. TCP) for reliability and the guarantee of sequential data ordering. More so than for bulk file transfer or media delivery, lossless sequential streaming poses an even greater challenge for the common problem cases of retransmission protocols, such as lossy links or long network paths, manifesting as significant latency in the interactive user experience. We developed a hybrid FEC-ARQ protocol that reduces to a simple strategy over sending or resending original data packets or check packets combining undecoded packets. Experimental results show that our proposed protocol can significantly improve the delay performance over retransmission and other schemes that use FEC, under a range of bandwidth and loss scenarios.

6. Secret-key Generation with Correlated Sources and Noisy Channels

Sponsors
NSF Grant No. CCF 0515109
University R&D Grant from Draper Laboratory

Project Staff
Ashish Khisti and Professor Gregory Wornell

A joint-source-channel setup for secret-key generation between remote terminals is considered. The sender communicates to the receiver over a discrete memoryless wiretap channel and the sender and receiver observe a pair of correlated discrete memoryless sources. Lower and upper bounds for the secret-key rate are presented and shown to coincide for the case when the underlying channel is a reversely degraded parallel channel. Our setup also provides an operational significance to the rate-equivocation tradeoff of the wiretap channel, and this is illustrated in detail for the Gaussian case.

7. Dense Transmit and Receive Antennas for Wireless Communications

Sponsors
MIT Lincoln Laboratory
Semiconductor Research Corporation through the FCRP Center for Circuit & System Solutions No. 2003-CT-888 (C2S2)

Project Staff
James Krieger, Dr. Chen-Pang Yeang, Professor Gregory Wornell, Professor Lizhong Zheng

In antenna array theory and design, the primary motivation for use of multiple antennas has historically been to increase channel capacity or to improve the controllability of radiation patterns. This work investigates the ability of multiple antennas to alleviate the complexity of RF circuitry. The proposed scheme involves a dense, over-sampled array in which the number of radiating elements exceeds the array's number of degrees of freedom. A Delta-Sigma quantization method allows the use of simple inexpensive phase quantizers in lieu of high-end costly linear power amplifiers and phase shifters.

This work includes a description of the feasibility of the Delta-Sigma quantization scheme as a viable method of reproducing intended radiation patterns with simple 2-bit phase quantizers. Further, it is shown that this may be easily adapted from a linear array to a two-dimensional planar array. Continued work will study the deleterious effects of the strong mutual impedance inherent in closely spaced array elements. Finally, a Mutual Coupling Compensation Network (MCCN) to mitigate these effects will be investigated, providing both accurate beam-shaping and adequate power transfer efficiency.

8. Caching in Wireless Networks

Sponsors
HP/MIT Alliance
NSF under Grant No. CCF-0635191

Project Staff
Urs Niesen, Professor Devavrat Shah, Professor Gregory Wornell

We consider the problem of delivering content cached in a wireless network of n nodes randomly located on a square of area n. In the most general form, this can be analyzed by considering the

2^n*n-dimensional caching capacity region of the wireless network. We propose a communication scheme for transmission of messages cached in the network. This provides an inner bound to the caching capacity region.

9. Decoding Algorithms for Neural Prosthetic Devices

Sponsors
NSERC

Project Staff
Maryam Modir Shanechi, Professor Gregory Wornell, Emery Brown and Ziv Williams

Brain Machine Interfaces (BMIs) aim to restore lost motor function in patients with various neurological disorders by creating a new communication link from the functioning brain to outside devices. BMIs work in part by mapping the noisy observations of the neural signal to the intended movement. This process is also known as 'decoding'. There are various parameters of a movement that could potentially be decoded and used in reconstructing the intended trajectory. These include high-level cognitive signals such as intended target and low-level kinematics of the movement such as speed or direction. In this work we are interested in jointly decoding both high-level and low-level movement related parameters.

10. Efficient Universal Coding for Parallel Gaussian Channel

Sponsors
NSF Grant No. CCF-0515122
DoD MURI N00014-07-1-0738
NSERC

Project Staff
Maryam Modir Shanechi, Dr. Yuval Kochman, Dr. Uri Erez and Professor Gregory Wornell

The design of practical universal codes for parallel Gaussian channels, when the capacity is known at the transmitter but the channel parameters themselves are not, is of significant interest in a variety of emerging wireless applications and standards.

In this work, we investigate various universal coding approaches for the parallel Gaussian channel. While repetition coding and a previously suggested concatenated Gaussian/erasure coding are efficient in the limits of low and high channel capacity, respectively, both these approaches have low efficiency at intermediate channel conditions. A previously suggested strategy of MMSE combination and successive decoding improves the efficiency at the intermediate regime, but it involves numerical optimization that becomes difficult to solve for a large number of sub-channels. We seek a practical method that performs well for all channel conditions, as well as being optimal in the low- and high- capacity limits.

An additional direction in this work, is to find methods for exploiting a very low-rate feedback for improving the efficiency of coding.

11. On the Role of Feedback in Multiuser MIMO Downlink System Design

Sponsors
MITRE Corporation
NSF Grant No. CCF-0635191

Project Staff
Charles Swannack and Professor Gregory Wornell

In multiple antenna systems with many users it is impractical to consider transmission to every user due to multiplexing and power constraints. In such a setting user selection algorithms may be employed to a select subset of users for transmission. We consider a scenario in which a large number of distributed non-cooperating users independently measure the channel between themselves and the transmitter. In order for the transmitter to select an appropriate subset of users for transmission these users send a quantized version of their channel vector to the transmitter. For such a system, it may be impractical to collect every quantized channel vector or intractable computationally to use all available data to form the signal for transmission.

In this work, we use a simple architecture for user subset selection. We show that in such a system, the design of the quantization codebook used in the quantization of the random channel vectors is a key component in the design of subset selection algorithms. We show that the quantization codebook is a key to developing efficient algorithms to find near-optimal sets for transmission. Further, we provide a structured class of quantization codebooks that, while being efficient, are also highly immune to unmodeled (or unknown) correlation in the channel.

12. Practical Coding Schemes for Asynchronous Communication

Sponsors
NSF Grant No. CCF-0635191
DoD MURI Grant No. N00014-07-1-0738
University R&D Grant from Draper Laboratory

Project Staff
Da Wang and Professor Gregory Wornell

In modern communication systems, most (initial) frame synchronization schemes use fixed-length sync words with certain lengths at the beginning of the data stream, and choose a proper design to achieve certain synchronization error probability for a given SNR. In these schemes, the synchronization word is used for synchronization only and thus is a pure overhead in terms of data transmission. This overhead may become significant in many emerging applications that involve intermittent communication, such as sensor networks, where sensors only occasionally transmits a short message to a remote base station, or inter-vehicle networks, where different vehicles need to communicate from time to time on some time-critical information, such as collision avoidance. Therefore, it is desirable to develop efficient synchronization schemes, that is reliable (in terms of error probability), efficient (in terms of communication rate) and fast (in terms of detection/decoding delay).

Specifically, we investigate the joint synchronization-coding schemes, which uses codewords for both synchronization and coding purposes. Information theoretical analysis has shown that under certain conditions, this scheme is able to achieve channel capacity, and we are investigate the design of efficient coding schemes to achieve joint synchronization and coding reliably and efficiently.

Publications

Journal Articles, Published

V. Chandar, A. Tchamkerten, and G. W. Wornell, “Optimal Sequential Frame Synchronization”, *IEEE Trans. Inform. Theory*, vol. 54, no. 8, pp. 3725 – 3728, Aug. 2008.

V. Divi and G. W. Wornell, “Blind Calibration of Timing Skew in Time-Interleaved Analog-to-Digital

Converters,” *IEEE Journal of Selected Topics in Signal Processing*, Special Issue on DSP Techniques for RF/Analog Circuit Impairments, vol 3, no 3, pp. 509 – 522, June 2009.

A. Khisti, A. Tchamkerten, and G. W. Wornell, “Secure Broadcasting over Fading Channels,” *IEEE Transactions on Information Theory,* vol 6, pp. 2453-69, June 2008.

E. Martinian, G. W. Wornell, and R. Zamir, “Source Coding with Distortion Side Information”, *IEEE Trans. Inform. Theory*, vol. 54, no. 10, pp. 4638-65, October 2008.

U. Niesen, D. Shah and G. W. Wornell, “Adaptive Alternating Minimization Algorithms”, *IEEE Trans. Inform. Theory*, vol. 55, no. 3, pp. 1423-29, March 2009.

U. Niesen and A. Tchamkerten, “Tracking Stopping Times Through Noisy Observations”, *IEEE Trans. Inform. Theory*, vol. 55, no. 1, pp. 422-32, January 2009.

E. Martinian, G. W. Wornell, and R. Zamir, “Source Coding with Distortion Side Information”, *IEEE Trans. Inform. Theory*, vol. 54, no. 10, pp. 4638-4665, Oct. 2008.

Journal Articles, Accepted for Publication

A. Khisti and G. W. Wornell, "Secure Transmission with Multiple Antennas II: The MIMOME Wiretap Channel”, to appear in *IEEE Trans. Inform. Theory*, 2009.

A. Khisti and G. W. Wornell, "Secure Transmission with Multiple Antennas I: The MISOME Wiretap Channel”, to appeaer in *IEEE Trans. Inform. Theory*, 2009.

A. Tchamkerten, V. Chandar, and G. W. Wornell, "Communication under Strong Asynchronism", to appear in *IEEE Trans. Inform. Theory*, 2009.

Journal Articles, Submitted for Publication

A. Accardi and G. W. Wornell, "Quasi Light Fields: Extending the Light Field to Coherent Radiation", submitted *to J. Op. Soc. Am.*, May 2009.

A. Khisti, S. Diggavi, and G. W. Wornell, "Secret-Key Generation using Correlated Sources and Channels”, submitted to *IEEE Trans. Inform. Theory*, 2009.

M. Shanechi, R. Porat, and U. Erez, "Comparison of Practical Feedback Algorithms for Multiuse MIMO", submitted to *IEEE Trans. Commun*., March 2009.

Meeting Papers, Published

G. Avoine, A. Tchamkerten, “An Asymptotically Optimal Authentication Protocol Against Relay Attacks,” submitted to Asiacrypt, International Conference on the Theory and Application Cryptology & Information Security, (Melbourne, Australia), December 2008.

A. Tchamkerten, V. Chandar, and G. W. Wornell, “On the Capacity Region of Asynchronous Channels,” in *Proc. Int. Symp. Inform. Theory* (Toronto, Canada), July 2008.

Huang, Y., Mehrotra, S., Li, J., "A Hybrid FEC-ARQ Protocol for Low-Delay Lossless Sequential Streaming", in *Proc. IEEE Int. Conf. Multimedia, Expo*, May 2009.

A. Khisti, S. Diggavi, and G. W. Wornell, "Secret-Key Generation with Correlated Sources and Noisy Channels”, in *Proc. Int. Symp. Inform. Theory* (ISIT), (Toronto, Canada), July 2008.

M. Shanechi, U. Erez, and G. W. Wornell, "Time-Invariant Rateless Codes for MIMO Channels", in *Proc. IEEE International Symposium on Information Theory* (ISIT), Toronto, Canada, July 2008.

M. Shanechi, U. Erez, and G. W. Wornell, "Rateless Codes for MIMO Channels", in *Proc. IEEE Int. Global Commun. Conf.* (GLOBECOM), (New Orleans, LA), Nov. 2008.

M. Shanechi, R. Porat, and U. Erez, "Comparison of Practical Feedback Algorithms for Multiuse MIMO", in *Proc. IEEE Vehic. Technol. Conf.* (VTC), (Barcelona, Spain), April 2009.

S. K. Shin, Y. S. You, S. H. Lee, K. H. Moon, J. W. Kim, L. Brooks, and H. S. Lee, "A Fully Differential Zero-Crossing-Based 1.2V 10b 26MS/s Pipelined ADC in 65nm CMOS", *Digest of Technical Papers, Symposium on VLSI Circuits*, June 2008.

Meeting Papers, To Appear

V. Chandar, A. Tchamkerten, and G. W. Wornell, "A Novel Asynchronous Communication Paradigm: Detection, Isolation, and Coding", *in Proc. Int. Workshop Sequential Methodologies (Troyes, France)*, June 2009.

A. Khisti, S. Diggavi, and G. W. Wornell, "Secret Key Agreement Using Asymmetry in Channel State Knowledge", in *Proc. Int. Symp. Inform. Theory* (Seoul, Korea), June 2009.

U. Niesen, D. Shah, G. W. Wornell: "Caching in Wireless Networks", *Proc. IEEE Int. Symp. Inform. Theory* (ISIT), (Seoul, Korea), June 2009.

Theses

A. Khisti, *Algorithms and Architectures for Multiuser, Multiterminal, and Multilayer Information – Theoretic Security*, Ph.D. diss., Department of Electrical Engineering and Computer Science, MIT, 2008.

V. Divi, *Estimation and Calibration Algorithms for Distributed Sampling Systems*, Ph.D. diss., Department of Electrical Engineering and Computer Science, MIT, 2008.

L. Brooks, *Circuits and Algorithms for Pipelined ADCs in Scaled CMOS Technologies*, Ph.D. diss., Department of Electrical Engineering and Computer Science, MIT, 2008.