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]

Postdoctoral Scholars
Dr. Aslan Tchamkerten, Dr. Chen-Pang Yeang

Graduate Students
Anthony Accardi, Kevin Boyle, Lane Brooks, Venkat Chandar, Vijay Divi, Ying-Zong Huang, Ashish Khisti, Maryam Shanechi, Urs Niesen, Charles Swannack

Administrative Staff
Tricia Mulcahy

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] Department of Electrical Engineering, Tel-Aviv University, Israel
[2] NEC Corporation, Intelligence Systems Department, Tokyo, Japan
[3] 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. A 77 GHz System for Millimeter-Wave Active Imaging

Sponsors
FCRP Center for Circuits, Systems and Solutions, Contract No. 2003-CT-888
MIT Lincoln Laboratory

Project Staff
Anthony Accardi, J. Chu, K. Nguyen, J. Powell, H. Kim*, Professor Gregory Wornell, Professor Harry Lee, and Professor Charles Sodini
* MIT Lincoln Laboratory

Due to advances in silicon and digital processing technology, low-cost millimeter-wave (MMW) imaging solutions with high antenna array density are now viable. While millimeter resolution or better is desirable for many applications, this wavelength is large enough to avoid scattering by tiny interfering particles. Furthermore, a large bandwidth can be supported at this high carrier frequency. MMW technology is therefore well suited for applications such as automotive collision avoidance and concealed weapons detection.

By superimposing the signals recorded at antennas configured in an array, the imaging receiver can be focused on a portion of the scene corresponding to a particular pixel. This process, called beamforming, makes use of constructive interference at the carrier frequency, and allows the receiver to be “electronically steered” without any moving parts. However, very low phase noise is required for fine resolution at long range.

Traditionally, beamformers at such high frequencies are fabricated using custom analog technology to ensure precise phase control. Our system performs digital beamforming, allowing for low-cost, large-scale production and low power consumption. We address the phase noise by oversampling, averaging, and employing feedback. That is, we correct for phase noise introduced in the analog and data conversion circuitry in the digital domain, thereby driving research with high data rate, low phase noise, and low power consumption requirements.

Figure 1 illustrates the system, and indicates the components we plan to fabricate. Our goal is to justify the system architecture and establish a proof of concept by implementing the most challenging components.

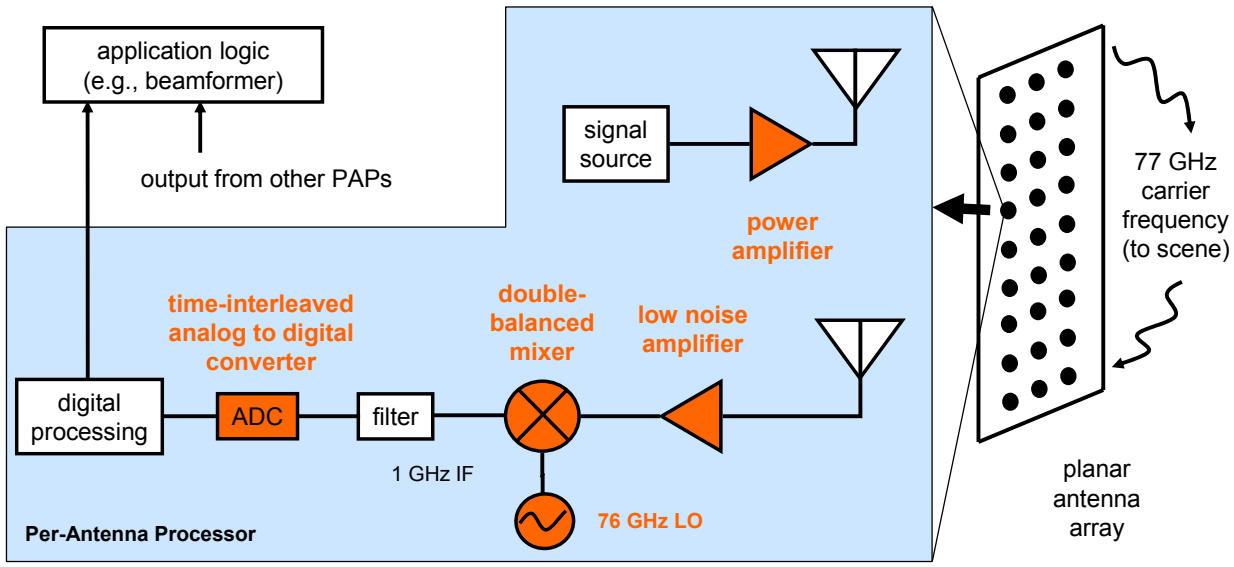

Figure 1: A functional block diagram indicating the key components in the active imaging system. These components are part of the Per-Antenna Processor (PAP), which is replicated for each node in the array.

2. Rateless Codes for the Additive White Gaussian Noise Channel

Sponsors
Draper Laboratory

Project Staff
Kevin Boyle, Professor Gregory Wornell, Dr. Chris Yu*, and Dr. Phil Lin*
*Draper Laboratory

Rateless codes are codes where the rate is not fixed *a priori* at the transmitter. Rather, the rate of the code automatically adapts to the quality of the channel, providing a robust and efficient method of transmitting information. Recently, several rateless codes have been developed that are capacity-approaching on the additive white Gaussian noise (AWGN) channel. The capacity-approaching behavior was shown from an information theoretic perspective.

Much of this work is focused on further analyzing those codes under practical constraints. Specifically, the rateless codes that were recently developed depend on the use of a good low-rate AWGN channel code as a building block. In the information theoretic analysis, it was assumed that a perfectly capacity-achieving AWGN code is used as a building block. In contrast, we analyze the performance of the rateless codes when an imperfect low-rate AWGN code is used as the building block. In addition to incorporating this practical constraint into our analysis, we simulate the rateless codes. Throughout our work, we compare these rateless codes to other forms of rateless codes, including hybrid automatic repeat request (HARQ).

Finally, we examine several extensions of these rateless codes including the creation of a code with both rateless and unequal error protection properties.

3. Zero-Crossing Based Circuits for Analog Circuit Design in Scaled CMOS Technologies

Sponsors
NDSEG Fellowship
CICS (Center of Integrated Circuits and Systems)

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

A new method of switched capacitor circuit design called comparator-based switched-capacitor circuit (CBSC) design methodology was recently introduced that replaces op-amps with comparators. 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.

The comparator input in a CBSC implementation is a constant slope voltage ramp, and so the comparator performs a zero-crossing detection. This work generalizes CBSC by replacing the general purpose comparator of CBSC circuits with a zero-crossing detector to realize new architecture called Zero-Crossing Based Circuits (ZCBC). Power efficiency savings can be realized by not using a general purpose comparator. The zero crossing detector used in our implementation of a 1.5bit/stage, 8 bit, 200MS/s ZCBC pipelined ADC draws no static current and is fast, simple, and amenable to scaling. Further innovations of this implementation include current source splitting for improved linearity and bit decision flip-flops for improved speed. The corresponding FOM for this implementation is 510 fJ/step at 200MS/s. This demonstrates best-in-class performance in terms of power-efficiency amongst other published ADCs in its class. A second chip is in fabrication that seeks further improvements in resolution and power efficiency.

4. Iterative Algorithms For Lossy Source Coding

Sponsors
NSF Graduate Fellowship
NSF Grant No. CCF-0515109

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

For many types of data encountered in the real world, including audio and video signals, it is known that if the signal is distorted the perceived quality may still be good. For example, if the high frequency components of an image are distorted, the image looks almost the same to the human eye. Lossy source coding attempts to answer the question of how much compression is possible when the compression algorithm is allowed to introduce a certain amount of distortion. In this framework, the decompressed signal must be close to the original signal with respect to some distortion measure. Our research focuses on developing efficient algorithms that come close to the information-theoretic limits on lossy source coding for some simple source and distortion models. Our goal is to use the insights gained from designing algorithms for simple models to develop algorithms for more general models that capture the behavior of real-world data.

5. Time-Skew Estimation and Signal Recovery in Time-Interleaved Analog-to-Digital Converters

Sponsors
MIT Lincoln Laboratory

Project Staff
Vijay Divi and Professor Gregory W. Wornell

The performance of 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 methods for estimating the unknown time-skew parameters and for performing signal reconstruction from these estimates. Calibration methods are presented for both a deterministic input model and a random input model. The performance and complexity of the proposed algorithms makes them attractive solutions for calibration.

6. Reliable and Secure Delivery of Streaming Media

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

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

The central problems of this research is motivated by some of the most pressing problems faced by the designers of streaming media systems in today's applications. Two issues that arise are reliable delivery in the face of unpredictable losses in the network and securing content during distribution.

In the first problem, systems that are compatible with existing clients are preferred. Thus, we developed a scheme that maximizes the expected received media quality by jointly selecting the data to retain and the amount of error protection to use, without resorting to re-packetization. This architecture ensures a straightforward implementation leveraging existing media delivery system components. Significant gains are shown in experiments on real video content coded with the H.264/MPEG-4 AVC standard.

In the second problem, which is the subject of ongoing research, we apply source-coding methods to develop a novel scheme where the media content remains secured through a larger part of the processing pipeline than is possible in existing systems.

7. Adaptive Alternating Minimization Algorithms

Sponsors
NSF Grant No. CCF-0635191

Project Staff
Urs Niesen, Professor Devavrat Shah, and Professor Gregory W. Wornell

The classical alternating minimization (or projection) algorithm has been successful in the context of solving optimization problems over two variables or equivalently of finding a point in the intersection of two sets. The iterative nature and simplicity of the algorithm has led to its application to many areas such as signal processing, information theory, control, and finance.

A general set of sufficient conditions for the convergence and correctness of the algorithm are quite well known when the underlying problem parameters are fixed. In many practical situations, however, the underlying problem parameters are changing over time, and the use of an adaptive algorithm is more appropriate. In this paper, we study such an adaptive version of the alternating minimization algorithm. As a main result of this paper, we provide a general set of sufficient conditions for the convergence and correctness of the adaptive algorithm. Perhaps surprisingly, these conditions seem to be the minimal ones one would expect in such an adaptive setting. Our result is a generalization of the work by Csiszar and Tusnady on alternating minimization procedures. We present applications of our results to adaptive decomposition of mixtures, adaptive log-optimal portfolio selection, and adaptive filter design.

8. Universal and Rateless Codes for Parallel Gaussian Channels

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

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

Many communication channels, such as time-invariant frequency-selective channels or time-varying fading channels, can be modeled and analyzed as parallel Gaussian channels. Design of practical universal codes for parallel Gaussian channels with unknown channel state at the transmitter and with channel state information at the receiver is of great interest because of their great modeling power in many practical communication systems. In this work, we design low complexity universal and rateless codes for parallel Gaussian channels. We study the universality both in terms of the uncertainty in the relative quality of the sub-channels for a fixed maximum rate and in terms of the uncertainty of the overall maximum achievable rate. In our architectures, we will convert the parallel Gaussian channel into a set of scalar Gaussian channels and use low complexity “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 receiver combined with successive interference cancellation (MMSE-SIC) 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. Two decoder structures are considered for this coding scheme, the MMSE-SIC, and a maximal ratio combining (MRC) receiver along with successive cancellation and the performance of each decoder is analyzed. Moreover, a scheme that involves an application of the faster than Nyquist signaling is also developed and analyzed. The efficiency performances of all these schemes and the effects of different design parameters on this performance and the tradeoffs involved are studied in detail.

9. Tracking Stopping Times

Sponsors
NSF Grant No. CCF-0515122
University R&D Grant from Draper Laboratory

Project Staff
Urs Niesen, Aslan Tchamkerten, and Professor Gregory W. Wornell

We consider a generalization of the change-point problem, a well-known quickest detection problem in quality control. This generalization leads to interesting applications in prediction,

monitoring, and communication.

Let $\{(X_i,Y_i)\}_{i\geq 1}$ be a sequence of pairs of random variables, and let S be a stopping time with respect to $\{(X_i,Y_i)\}_{i\geq 1}$. We consider the problem of finding a stopping time T with respect to $\{Y_i\}_{i\geq 1}$that optimally tracks S, in the sense that T minimizes the average reaction time $E(T-S)^+$, while keeps the false-alarm probability $P(T<S)$ below a given threshold $\alpha \in [0,1]$.

Here the (X_i,Y_i)'s take values in the same finite alphabet and S in bounded. By using elementary methods based on the analysis of the tree structure of stopping times, we first exhibit an algorithm that computes the optimal expected reaction times for all $\alpha \in [0,1]$ and constructs the associated optimal stopping times T. Second, we provide a sufficient condition on $\{(X_i,Y_i)\}_{i\geq 1}$and S under which the algorithm running time is polynomial in the bound of S. Finally we illustrate this condition with two examples: a Bayesian change-point problem and a pure tracking stopping time problem.

10. Broadcasting Secret Keys Over Fading Channels

Sponsors
NSF Grant No. CCF-0515109

Project Staff
Ashish Khisti, Dr. Aslan Tchamkerten, and Professor Gregory W. Wornell

Most cryptographic protocols assume that the intended terminals share a common key which is either distributed offline or updated via a secure channel. In certain applications (e.g., Pay TV systems) there is a natural need for an online key distribution mechanism over public channels. For such systems one has to naturally consider protecting signals at the physical layer.

In this project we consider taking advantage of time variations due to fading in wireless channels to deliver secure content to intended recipients while keeping it secure from potential eavesdroppers.

Both fundamental limits and practical architectures for distributing a common message to a set of intended users are investigated. Our systems require that the intended users feed-back the channel quality to the sender over authenticated public channels. The sender uses this knowledge to adapt the power and transmission rate to match the channel conditions of these intended users. Our protocols are provably secure against potential eavesdroppers, subject to modeling assumptions.

11. Secure Transmission with Multiple Antennas

Sponsors
NSF Grant No. CCF-NSF 0515109

Staff
Ahish Khisti, and Professor Gregory W. Wornell

Multiple antennas are known to provide significant gains in system throughput for wireless communications. In this project we explore the role of multiple antennas for covert communications. Our current focus is on developing information theoretic limits on the secrecy rate when all the terminals have multiple antennas and conclusive results have been obtained in

certain special cases.

Our initial results are quite promising. Secret communication is possible even when the eavesdropper has a significantly better channel than that sender. For the Rayleigh fading environment, even when the intended receiver has only a single antenna, the eavesdropper must have at least twice the number of antennas compared to the sender for the secrecy capacity to be zero. Thus in applications where the sender can have sufficiently many antennas, the eavesdropper has to pay a significant penalty in terms of hardware complexity to correctly receive the message.

At a higher level, we note that in recent times many "channel aware" architectures have been developed to increase the throughput of wireless systems. Many of these have side benefit of secrecy at the physical layer. Our goal is to quantify such gains and understand the potential applications.

12. Asynchronous Communication

Sponsors
NSF Grant No. CCF-0515122
University IR&D Grant from Draper Laboratory

Project Staff
Venkat Chandar, Ashish Khisti, Professor Gregory W. Wornell and Aslan Tchamkerten

It seems fair to say that in information theory the assumption of perfect synchronized communicating parties is ubiquitous and that the theory gives little insight on how to handle issues related to time uncertainty.

The basic question we address here is `how does a lack of synchronization between the transmitter and the receiver affect the range of achievable communication rates?'. To that aim we introduce a discrete time asynchronous channel model for point-to-point communication that can be seen as an extension of the detection and isolation problem setting in sequential analysis: the transmitter may start emitting information at any time within a certain interval that represents the level of asynchronism. The receiver must decode without knowing when transmission starts but being cognizant of the asynchronism level. Our main result is the characterization of the largest asynchronism level for which reliable communication can be achieved. Specifically we show that, among all coding schemes that operate at a strictly positive rate, the maximum achievable asynchronism level is (asymptotically) $e^{\alpha N}$ where N denotes the codeword length and where α represents the `synchronization threshold' and admits a simple expression depending on the channel. The scheme we propose to reliably communicate under extreme asynchronism, perhaps somewhat surprisingly, performs detection of the codeword and isolation of the message jointly rather than separately as often in practice.

13. Efficient Scheduling and Feedback in MIMO Networks

Sponsors
NSF Grant No. CCF-0635191

Project Staff
Charles Swannack and Professor Gregory W. 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. Recent approaches to this scheduling problem have examined the scaling behavior of the multiple-antenna broadcast channel in the large user limit with perfect channel channel state information using various interference canceling multiplexers and complexity constraints We provide a simple architecture for scheduling over the Gaussian MIMO broadcast channel with quantized feedback.

Publications

Journal Articles

L. Brooks and H.S. Lee, “A zero-crossing based 8b, 200ms/s pipelined ADC,” ISSCC Digest of Tech. Papers, pp. 460–461, Feb. 2007.

V. Divi and G.W. Wornell, “Blind Calibration of Timing Skew in Time-Interleaved Analog-to-Digital Converters” submitted to EURASIP Journal on Advances in Signal Processing

Y.Z. Huang, J. G. Apostopoulos, “Joint Packet Selection/Omission and FEC System for Streaming Video.” IEEE ICASSP, Apr. 2007.

A. Khisti, A. Tchamkerten, and G. W. Wornell, “Secure Broadcasting”, submitted for publication to *IEEE Trans. Inform. Theory* (Special Issue on Information Theoretic Security), Feb 2007.

U. Niesen, A. Tchamkerten, G. W. Wornell, “Tracking Stopping Times,” *submitted to journal Mathematics of Operations Research.*

P.O. Vontobel and A. Ganesan, “On universally decodable matrices for space-time coding,” Designs, Codes, and Cryptography, vol. 41, nr. 3, Dec. 2006, pp. 325-342.

U. Niesen, D. Shah, G. W. Wornell, “Adaptive Alternating Minimization Algorithms,” submitted to *IEEE Transactions on Information Theory.*

A. Khisti, U. Erez, A. Lapidoth, and G. W. Wornell, “Carbon Copying Onto Dirty Paper,” *IEEE Trans. Inform. Theory*, vol. 53, no. 5, pp. 1814--1827, May 2007.

A. Khisti, U. Erez, and G. W. Wornell, “Fundamental Limits and Scaling Behavior of Cooperative Multicasting in Wireless Networks,” *IEEE Trans. Inform. Theory*, vol. 52, no. 6, pp. 2762--2770, June 2006.

Conference Proceedings, Published

V. Chandar, E. Martinian, and G. W. Wornell, “Information Embedding Codes on Graphs with Iterative Encoding and Decoding*,”* in *Proc. IEEE International Symposium on Information Theory (ISIT*), July 2006.

C. Swannack, G. W. Wornell, and E. Uysal-Biyikoglu, “MIMO broadcast scheduling with quantized channel state information,” in *Proc. IEEE International Symposium on Information Theory (ISIT)*, July 2006.

A. Tchamkerten, A. Khisti, G. W. Wornell, “Information Theoretic Perspectives on Synchronization,” in *Proc. IEEE International Symposium on Information Theory (ISIT*), July 2006

A. Khisti, E. Martinian, G. W. Wornell, “Information Embedding with Distortion Side Information,”

in *Proc. Int. Symp. Inform. Theory* (ISIT-2006), July 2006.

U. Erez, M. D. Trott, G. W. Wornell, "Rateless Coding and Perfect Rate-Compatible Codes for Gaussian Channels," in *Proc. Int. Symp. Inform. Theory (ISIT-2006)*, July 2006.

A. Khisti, A. Tchamkerten, G. W. Wornell, "Secure broadcasting with Multiuser Diversity," in *Proc. Allerton Conf. Commun., Contr., and Computing,* (Illinois), October 2006.

U. Niesen, D. Shah, and G. W. Wornell, "Sampling Distortion Measures," in *Proc. Allerton Conf. Commun., Contr., Computing*, (Illinois), Sep. 2006.

C. Swannack, E. Uysal-Biyikoglu, and G. W. Wornell, "Efficient quantization for feedback in MIMO broadcasting systems," in *Proc. The Asilomar Conference on Signals, Systems, and Computers,* Asilomar, California, October 2006.

U. Niesen, U. Erez, D. Shah, and G. W. Wornell, "Rateless Coding for Gaussian Multiple-Access Channels," in *Proc. IEEE GLOBECOM*, (San Francisco, CA), Nov. 2006.

U. Niesen, D. Shah, G. Wornell, "Adaptive Alternating Minimization Algorithms," to appear in *Proc. IEEE International Symposium on Information Theory (ISIT),* June 2007.

U. Niesen, A. Tchamkerten, and G. W. Wornell, "The Complexity of Tracking a Stopping Time," to appear in *Proc. Int. Symp. Inform. Theory (ISIT).* June 2007.

A. Khisti, G. W. Wornell, A. Wiesel, and Y. Eldar, "On the Gaussian MIMO Wiretap Channel," to appear in *Proc. Int. Symp. Inform. Theory (ISIT*), June 2007.

U. Niesen, A. Tchamkerten, G. Wornell, "Tracking Stopping Times," *in Proc. Allerton Conf. Commun., Contr., and Computing,* (Illinois), October 2006.

J. M. Shapiro, R. J. Barron, and G. W. Wornell, "Practical Layered Rateless Codes for the Gaussian Channel: Power Allocation and Implementation," in *Proc. Workshop Signal Processing Advances in Wireless Commun. (SPAWC)* (Helsinki, Finland), June 2007.

E. W. Huang and G. W. Wornell, "Peak-to-Average Power Reduction for Low-Power OFDM Systems," in *Proc. Int. Conf. Commun. (ICC-2007),* (Glasgow, Scotland), June 2007.