

President's Column

Alon Orlitsky

One should never start with a cliché. So let me end with one: where did 2016 go? It seems like yesterday that I wrote my first column, and it's already time to reflect on a year gone by?

And a remarkable year it was! Each of earth's corners and all of life's walks were abuzz with activity and change, and information theory followed suit. Adding to our society's regularly hectic conference meeting/publication calendar, we also celebrated Shannon's 100th anniversary with fifty worldwide centennials, numerous write-ups in major journals and magazines, and a coveted Google Doodle on Shannon's birthday. For the last time let me thank Christina Fragouli and Rudi Urbanke for co-chairing the hyperactive Centennials Committee.

Our major centennial project, the Shannon documentary, has also shaped up well. Proceeding past the family-, student-, and colleague-videos, we are gearing up for the main "Shannon interview" at the family's Winchester house, now anticipated at the end of January. We hired a production designer to re-assemble Shannon's mechanical widgets, and are concluding the Shannon-actor search with hopefully-final auditions planned for the coming weeks. Not long from now, I look forward to all of us enjoying the first major documentary about the genesis of our field.

At the beginning of the year we also set out to increase communication from, to, and within our community. We followed up with four initiatives:

- Matthieu Bloch, Michelle Effros, and other society members, have been working with producer Brit Cruise to create short videos explaining information theoretic concepts and contributions, and the first two videos, about MIMO and Network Coding, are expected early next year.
- Suhas Diggavi and Salim El Rouayheb are leading the effort to create an online lecture series similar to TCS+



that would bring and curate information theoretic lectures for large audiences.

- Jeff Andrews and Elza Erkip are heading a BoG ad-hoc committee exploring the creation of a new publication connecting information theory to other topics and communities, with two main formats considered: a special topics journal, and a popular magazine.
- Christina Fragouli and Anna Scaglione are co-authoring a children's book on information theory, the first chapter is completed and the rest are expected next year.

As the holidays ushered in, twelve-shy-one society members received jolly good tidings. Raviraj Adve, Alexei Ashikhmin, Huaiyu Dai, Xinzhou Dong, Michael Gastpar, Stephen Hanly, Masahito Hayashi, Amir Khandani, Witold Krzymien, Teng-joon Lim, and Xiaojun Lin were elevated to IEEE Fellow grade. Only one tenth of one percent of IEEE members can become Fellows annually, which for our society amounts to roughly three. Thrice exceeding our quota attests to the high regard at which the whole institute holds our society. Please join me in congratulating our fellow fellows on this deeply deserved and warmly welcome recognition of their accomplishments.

2016 was notable in another respect as well. Over the past half century, numerous information-theoretic innovations, from compression to coding and from modulation to MIMO have enabled and propelled the communication revolution. And this year, two more information-theoretic inventions are poised to make worldwide communication even faster and more efficient and reliable.

Last month, the international mobile telecommunications organization, 3GPP, decided on the standards for the 5G

(continued on page 33)

From the Editor

Michael Langberg



Dear colleagues,

Our winter issue of 2016 opens with Alon Orlitsky's final column as President of the IT Society. Please join me in thanking Alon for his dedication and inspiring leadership over the past year, and in warmly welcoming our incoming President Rüdiger Urbanke. We then proceed to present two excellent technical contributions. "The classical capacity of quantum Gaussian gauge-covariant channels: beyond i.i.d." by Alexander S. Holevo, this year's Shannon award winner. The article extends the Shannon lecture given at ISIT 2016 and studies a challenging family of quantum Gaussian channels. "Sparse Regression Codes", by Ramji Venkataraman, Sekhar Tatikonda, and Andrew Barron, based on their tutorial at ISIT 2016. The article surveys the topic of sparse regression codes at both an intuitive and formal level, and includes a list of intriguing open problems. Many thanks to the contributors for their significant efforts!

The issue continues with a number of regular columns and reports including Tony Ephremides's Historian's column; our "Students' Corner" column presenting "A Perspective on Implicit Gender Bias" by Mine Alsan; the column "From the field" by the IEEE Information Theory Society German Chapter, Volker Kühn, Gerhard Bauch, and Dirk Wübben; a new regular column that presents a list of recent articles published in the IEEE Transactions on Information Theory and in Foundations and Trends® in Communications and Information Theory; and reports from recent Shannon Centenary events: Ninoslav Marina describes the journey that led to a commemorative stamp presenting Claude E. Shannon issued by the Macedonian Post, Alfred Hero reports on the University of Michigan Shannon Centennial Symposium, and Natasha Devroye reports on the "IEEE ITSoc Chicago Chapter Shannon Centennial Event". In addition you will find a report on the "2016 IEEE International Symposium on Information Theory" that took place in Barcelona, Spain by Albert Guillén i Fàbregas, Alfonso Martínez and Sergio Verdú; a report by Bobak Nazer on the IHP program "Nexus of Information and Computation Theories" that took place during the early spring in Paris; a report on the "2016 IEEE IT Society Summer School" that took place in the Indian Institute of Science at Bangalore; a report by Han Vinck on the celebration of Piet Schalkwijk's 80th birthday; and minutes from the IEEE Information Theory Society Board of Governors meeting this summer at ISIT.

With sadness, we conclude this issue with a tribute to Robert Fano, a pillar and leader of our community, who passed away on July 13th; and a tribute to Titsa Panayota Papantoni-Kazakos,

continued on page 33

IEEE Information Theory Society Newsletter

IEEE Information Theory Society Newsletter (USPS 360-350) is published quarterly by the Information Theory Society of the Institute of Electrical and Electronics Engineers, Inc.

Headquarters: 3 Park Avenue, 17th Floor, New York, NY 10016-5997.

Cost is \$1.00 per member per year (included in Society fee) for each member of the Information Theory Society. Printed in the U.S.A. Periodicals postage paid at New York, NY and at additional mailing offices.

Postmaster: Send address changes to IEEE Information Theory Society Newsletter, IEEE, 445 Hoes Lane, Piscataway, NJ 08854.

© 2016 IEEE. Information contained in this newsletter may be copied without permission provided that the copies are not made or distributed for direct commercial advantage, and the title of the publication and its date appear.

IEEE prohibits discrimination, harassment, and bullying. For more information, visit <http://www.ieee.org/web/aboutus/whatis/policies/p9-26.html>.



Table of Contents

President's Column	1
From the Editor	2
The Classical Capacity of Quantum Gaussian Gauge-Covariant Channels: Beyond i.i.d.	3
Sparse Regression Codes	7
The Historian's Column	16
Students' Corner	17
From the Field: IEEE Information Theory Society German Chapter	18
Shannon Centenary	19
IEEE ITSOC Chicago Chapter Shannon Centennial Event	21
2016 IEEE International Symposium on Information Theory	22
IHP Program on the "Nexus of Information and Computation Theories"	23
2016 IEEE IT Society Summer School. Indian Institute of Science	24
Seminar on Information—and Communication Theory on the Occasion of the 80th Birthday of Piet Schalkwijk	25
IEEE Information Theory Society Board of Governors Meeting	26
In Memoriam: Robert Fano	29
In Memoriam: Dr. Titsa Panayota Papantoni-Kazakos	32
Golomb's Puzzle Column™: Collection, Part 2	34
Call for Nominations	46
Recent Publications	48
Call for Papers	52
Conference Calendar	56

The Classical Capacity of Quantum Gaussian Gauge-Covariant Channels: Beyond i.i.d.

A. S. Holevo, *Steklov Mathematical Institute, Russian Academy of Sciences*

Abstract

Following ISIT2016, the workshop “Beyond i.i.d. in Information Theory” was held in Barcelona. This note sketches the author’s contribution which can be considered as an extension of the Shannon lecture delivered at ISIT2016. A coding theorem for the classical capacity of a broadband gauge-covariant Gaussian channel with stationary quantum Gaussian noise is formulated and discussed.

1. Introduction

Recently, the Gaussian optimizer conjecture in quantum information theory was confirmed for bosonic Gaussian gauge-covariant or contravariant channels including phase-insensitive channels such as attenuators, amplifiers and additive classical noise channels [3]. It was shown that the classical capacity of these channels under the input energy constraint is additive and achieved by Gaussian encodings. These results use the *i.i.d.* model of the quantum noise.

In this paper we consider a quantum Gaussian signal+noise model with *time-continuous stationary coloured noise*. The main result is the coding theorem for the classical capacity of quantum broadband gauge-covariant Gaussian channels. There were several previous works in which similar problems were considered for different special cases, with different degree of justification. In this paper we rely upon the proof of coding theorem for a model of classical signal+quantum Gaussian noise involving the Planck spectrum given in [8]. In the paper of V. Giovannetti, S. Lloyd, L. Maccone, P.W. Shor [4] the authors considered a broadband pure-loss channel by formal passage from discrete to continuous spectrum and demonstrated numerical solutions for the capacities C , C_{cl} , Q . The paper of G. De Palma, A. Mari, V. Giovannetti [14] was devoted to a rigorous treatment of discrete time, Markov memory model, with flat noise spectrum. Recently B. R. Bardhan, J. H. Shapiro [1] studied a narrowband approximation for phase-insensitive time-invariant channels, basing on the result of [3].

The classical AGWN model is given by the equation

$$Y_k = X_k + Z_k; \quad k = 1, \dots, n \quad (1)$$

where $Z_k \sim N(0, N)$ are real Gaussian *i.i.d.* random variables representing the noise and the signal sequence X_k is subject to the energy constraint

$$n^{-1}(X_1^2 + \dots + X_n^2) \leq E.$$

The asymptotic ($n \rightarrow \infty$) capacity of this model is given by the famous Shannon formula¹

$$C = \frac{1}{2} \log(E + N) - \frac{1}{2} \log N = \frac{1}{2} \log\left(1 + \frac{E}{N}\right). \quad (2)$$

In the quantum analog of the signal+noise equation

$$Y = X + Z$$

¹Throughout this paper we use natural logarithms. In the context of quantum channels “capacity” will always mean the *classical capacity*.



one replaces any of the classical variables X, Y, Z by a (multiple of) pair of selfadjoint operators q, p , satisfying the Heisenberg canonical commutation relation (CCR) $[q, p] = i\hbar I$, or, equivalently, by a single operator $a = (1/\sqrt{2\hbar\omega})(\omega q + ip)$, (with Hermitean conjugate $a^\dagger = (1/\sqrt{2\hbar\omega})(\omega q - ip)$), satisfying the canonical commutation relation (CCR)

$$[a, a^\dagger] = I. \quad (3)$$

In applications p and q describe quantized quadratures of the harmonic mode of frequency ω ,

$$q \cos \omega t + \frac{p}{\omega} \sin \omega t \quad (4)$$

while a, a^\dagger , are quantizations of the complex amplitude and its adjoint.

As distinct from the classical case, the quantum models should respect the CCR i.e. arise as a part of a linear canonical transformation. Below we give a list of such models most important for applications. In these models a presents the quantum input signal, b – the quantum Gaussian noise variable and a' – the quantum output signal, all of them satisfying the CCR (3).

0. Classical-quantum channel (state preparation)

$$a' = x + b,$$

where x is the complex random variable representing classical signal at the background quantum noise.

1. Attenuator

$$a' = ka + \sqrt{1 - k^2} b, \quad 0 \leq k \leq 1.$$

2. Amplifier

$$a' = ka + \sqrt{k^2 - 1} b^\dagger, \quad k \geq 1.$$

3. Quantum channel with additive classical Gaussian noise

$$a' = a + \eta,$$

where η is the classical complex random variable having circular Gaussian distribution.

All these equations have the form $Y = X + Z$, where the noise Z is described by quantum or classical variable in Gaussian state² with the first two moments

$$\langle Z \rangle = 0, \quad \langle Z^\dagger Z \rangle = N, \quad \langle ZZ \rangle = 0. \quad (5)$$

Thus in all the cases the quantum AGWN model has the form (1) where Z_k are quantum or classical Gaussian *i.i.d.* noise variables obeying (5) and the signal sequence X_k is subject to the energy constraint

$$n^{-1} \langle X_1^\dagger X_1 + \dots + X_n^\dagger X_n \rangle \leq E.$$

A basic difference of the quantum signal variables is that one cannot simply impose on them zero or other deterministic values; one should instead define the *state* describing these variables. In the classical case the deterministic values are obtained from degenerate probability distributions, while in the quantum case existence of such “dispersion-free” states is forbidden by the uncertainty principle.

This circumstance underlies the two basic difficulties in finding the quantum analog of the Shannon formula (2): one is the proof of additivity $C_n = nC_1$, and the other is finding the minimum of the output entropy in the formula

$$C_1 = \max_{\langle X^\dagger X \rangle \leq E} H(Y) - \min_X H(Y).$$

When the signal X is classical (case 0), the minimum $\min_X H(Y) = H(Z)$ is attained for $X \equiv 0$. The resulting solution for the asymptotic capacity obtained in [8] is

$$C = g(E + N) - g(N), \quad (6)$$

where

$$g(N) = (N + 1) \log(N + 1) - N \log N \quad (7)$$

is the function representing the entropy of quantum Gaussian state with the moments (5).

In the cases 1–3 a similar “Gaussian optimizers conjecture” [9] was open for a dozen of years and finally solved in [3]. The resulting capacity formula in the cases 1–3 has the same form as (6), i.e.

$$C = g(E + N) - g(N), \quad E = \langle X^\dagger X \rangle, \quad N = \langle Z^\dagger Z \rangle. \quad (8)$$

All these solvable models possess symmetry under the gauge transformation $a \rightarrow ae^{i\varphi}$, $\varphi \in \mathbb{R}$. The quantum channels 1–3, as well as classical-quantum channel 0, are gauge-covariant i.e. their output changes similarly to the input: $a' \rightarrow a'e^{i\varphi}$. A complete classification of normal forms of single-mode quantum Gaussian channels was given in [10]. In this classification the cases 1–3 represent those normal forms which possess the gauge symmetry.

In the classical prototype of the gauge-covariant models X, Y, Z are complex Gaussian random variable having circular distribution and the capacity is twice the Shannon expression (2) i.e.

$$C = \log(E + N) - \log N.$$

2. The Coding Theorem

In classical information theory the broadband channel can be treated by reduction to parallel channels, i.e. by decomposing the Gaussian stochastic process into independent one-dimensional harmonic modes (4). In quantum theory such a decomposition plays an important additional role as a tool for *quantization* of the classical process. As a starting point for the time-domain model of quantum noise we take the expression for quantized electric field in a square box of size L (see, e.g. [6])

$$E(x, t) = \frac{i}{L^{3/2}} \sum_k \sqrt{\frac{\hbar \omega_k}{2}} a_k e^{ikx} e^{-i\omega_k t} + \text{h.c.}$$

where a_k^\dagger, a_k are the creation-annihilation operators of independent bosonic modes satisfying the standard canonical commutation relations³

$$[a_j, a_k^\dagger] = \delta_{jk} I, \quad [a_j, a_k] = 0. \quad (9)$$

Basing on this expression and redefining a_k , we consider the following periodic operator-valued function as a model for observations on the time interval $[0, T]$ at the spatial point $x = 0$:

$$\hat{Z}(t) = \sum_k \sqrt{\frac{\hbar \omega_k}{2T}} (a_k e^{-i\omega_k t} + a_k^\dagger e^{i\omega_k t}), \quad t \in [0, T], \quad (10)$$

$$\omega_k = \frac{2\pi k}{T}, \quad k = 1, 2, \dots; \quad \Delta\omega = \frac{2\pi}{T},$$

see [8]. To avoid ultraviolet divergence, we introduce the cutoff function $\tilde{\omega}(T), T > 0$, with the properties: $\tilde{\omega}(T)$ is positive and monotonously increasing with $\lim_{T \rightarrow \infty} \tilde{\omega}(T) = \infty$, and for each T include in all summations over k only the frequencies $\omega_k \in [0, \tilde{\omega}(T)]$. Then the energy operator has the expression (as distinct from the narrowband approximation):

$$\int_0^T \hat{Z}(t)^2 dt = \sum_k \hbar \omega_k (a_k^\dagger a_k + \frac{1}{2})$$

We modify the argument of [8] related to classical-quantum channel and generalize it to include the Gaussian gauge-covariant channels (cases 1–3). For a fixed T the equations of the channel Φ_T for the collection of frequency modes are

$$a_{k,Y} = K(\omega_k) a_{k,X} + \hat{n}_{k,Z}, \quad 0 \leq \omega_k \leq \tilde{\omega}(T), \quad (11)$$

with the noise operators

$$\hat{n}_{k,Z} = \begin{cases} \sqrt{1 - |K(\omega_k)|^2} a_{k,Z}, & |K(\omega_k)| < 1 \text{ attenuator} \\ \eta_{k,Z}, & |K(\omega_k)| = 1 \text{ class.noise} \\ \sqrt{|K(\omega_k)|^2 - 1} a_{k,Z}^\dagger(\omega) & |K(\omega_k)| > 1 \text{ amplifier} \end{cases}$$

satisfying the commutation relations

$$[\hat{n}_{k,Z}, \hat{n}_{l,Z}^\dagger] = \delta_{kl} (1 - |K(\omega_k)|^2),$$

and described by a centered Gaussian state with the second moments

$$\langle \hat{n}_{l,Z}^\dagger \hat{n}_{k,Z} \rangle = \delta_{kl} N(\omega_k), \quad \langle \hat{n}_{l,Z} \hat{n}_{k,Z} \rangle = 0.$$

²For detailed account of quantum Gaussian states see [1].

³For simplicity we do not consider the polarization degree of freedom.

Here $K(\omega), N(\omega)$ are continuous functions, $N(\omega) > 0$ in the domain $\omega \geq 0$.

Then Φ_T is Gaussian gauge-covariant channel in the Hilbert space \mathcal{H}_T of the modes with frequencies $0 \leq \omega_k \leq \bar{\omega}(T)$. We consider the family of channels $\{\Phi_T; T \rightarrow \infty\}$ as our model for the broadband channel.

Definition. For each $T > 0$ a code (Σ, M) is a collection $\{\rho^j, M_j; j = 1 \dots N\}$ where ρ^j are quantum states (density operators) in \mathcal{H}_T satisfying the energy constraint⁴

$$\text{Tr} \rho^j \left(\sum_k \hbar \omega_k a_{k,X}^\dagger a_{k,X} \right) \leq ET, \quad (12)$$

and M is a POVM in \mathcal{H}_T .

We define the *capacity* of the family $\{\Phi_T; T \rightarrow \infty\}$ as the supremum of rates R for which the infimum of the average error probability

$$\bar{\lambda}_T(\Sigma, M) = \frac{1}{N} \sum_{j=1}^N (1 - \text{Tr} \Phi_T[\rho^j] M_j).$$

with respect to all codes of the size $N = e^{TR}$ tends to zero as $T \rightarrow \infty$.

Theorem. Let $N(\omega), K(\omega)$ be continuous functions, $0 < |K(\omega)| \leq \kappa$, and $\bar{\omega}(T)/T \rightarrow 0$ as $T \rightarrow \infty$. The capacity of the family of channels $\{\Phi_T; T \rightarrow \infty\}$ is equal to

$$C = \int_0^\infty (g(\tilde{N}_\theta(\omega)) - g(N(\omega)))_+ \frac{d\omega}{2\pi}, \quad (13)$$

where

$$\tilde{N}_\theta(\omega) = \frac{1}{e^{\theta \hbar \omega / |K(\omega)|^2} - 1},$$

and θ is chosen such that

$$\int_0^\infty (\hbar \omega / |K(\omega)|^2) (\tilde{N}_\theta(\omega) - N(\omega))_+ \frac{d\omega}{2\pi} = E.$$

The capacity is upperbounded as

$$C \leq \frac{\pi \kappa^2}{6 \hbar \theta}.$$

The proof given in [11] combines the solution of the quantum Gaussian optimizer conjecture [3] with the estimates from the proof of the coding theorem for constrained infinite dimensional channel [8]. The underlying mechanism is emergence of increasing number of parallel channels in arbitrarily small neighbourhood of each frequency.

For completeness we briefly recall here the case of classical-quantum channel which was essentially considered in [8]. The channel equation in the frequency domain is:

$$\Phi_T: a_{k,Y} = x_k + a_{k,Z}.$$

In this case it can be rewritten in the time domain as “classical signal + quantum noise” equation

$$\hat{Y}(t) = X(t) + \hat{Z}(t), \quad t \in [0, T],$$

⁴Notice that the vacuum energy $(1/2) \sum_k \hbar \omega_k$ is explicitly excluded from the constraint to avoid the divergence when $T \rightarrow \infty$.

where the classical signal

$$X(t) = \sum_k \sqrt{\frac{\hbar \omega_k}{2T}} (x_k e^{-i\omega_k t} + \bar{x}_k e^{i\omega_k t}), \quad x_k \in \mathbb{C}.$$

The mean power constraint on the signal

$$\sum_k \hbar \omega_k |x_k|^2 = \int_0^T X(t)^2 dt \leq ET.$$

Then with appropriate modification of Definition of the code, one obtains the expression for the classical capacity

$$C = \int_0^\infty (g(N_\theta(\omega)) - g(N(\omega)))_+ \frac{d\omega}{2\pi}, \quad (14)$$

$$N_\theta(\omega) = \frac{1}{e^{\theta \hbar \omega} - 1},$$

and θ is chosen such that

$$\int_0^\infty \hbar \omega (N_\theta(\omega) - N(\omega))_+ \frac{d\omega}{2\pi} = E.$$

which coincides with the expression (13) for $K(\omega) \equiv 1$.

A test example is the case of equilibrium quantum noise $N(\omega) = N_{\theta_P}(\omega) \equiv (e^{\theta_P \hbar \omega} - 1)^{-1}$ with $\theta_P = \sqrt{\pi/12\hbar P}$ determined from

$$\int_0^\infty \frac{\hbar \omega}{e^{\theta_P \hbar \omega} - 1} \frac{d\omega}{2\pi} = P.$$

Then

$$\int_0^\infty g((e^{\theta_P \hbar \omega} - 1)^{-1}) = \frac{\pi}{6\hbar\theta_P} = \sqrt{\frac{\pi P}{3\hbar}}$$

(see e.g. [8] for detail of computation) and

$$C = \sqrt{\frac{\pi(P+E)}{3\hbar}} - \sqrt{\frac{\pi P}{3\hbar}},$$

which coincides with the capacity of the semiclassical model of broadband photonic channel [12], [2].

3. Discussion

3.1 The Limiting Broadband Process Model

In the limit $T \rightarrow \infty$, the periodic process (10) converges in distribution to the quantum stationary Gaussian noise described in detail in [8], [7]:

$$\hat{Z}(t) = \int_0^\infty \sqrt{\frac{\hbar \omega}{2}} (d\hat{A}(\omega) e^{-i\omega t} + d\hat{A}(\omega)^\dagger e^{i\omega t}).$$

Here $\hat{A}(\omega)$ is the quantum Gaussian independent increment process with the commutator

$$[d\hat{A}(\omega), d\hat{A}(\omega')^\dagger] = \frac{1}{2\pi} \delta(\omega - \omega') d\omega d\omega',$$

zero mean, and the normally-ordered correlation

$$\langle d\hat{A}(\omega)^\dagger d\hat{A}(\omega') \rangle = \frac{1}{2\pi} \delta(\omega - \omega') N(\omega) d\omega d\omega'$$

with the spectral density $N(\omega) \geq 0; \omega \geq 0$. The noise commutator is causal

$$[\hat{Z}(t), \hat{Z}(s)] = i\hbar/2 \int_0^\infty \omega \sin \omega(s-t) d\omega = i\hbar/2\delta'(t-s),$$

and the noise symmetrized correlation function is

$$\alpha(t-s) \equiv \langle \hat{Z}(t) \circ \hat{Z}(s) \rangle = \beta(t-s) + \frac{1}{2}j(t-s),$$

where

$$\begin{aligned} \beta(t) &= \hbar \int_0^\infty \omega N(\omega) \cos \omega t \frac{d\omega}{2\pi}, \\ j(t) &= \hbar \int_0^\infty \omega \cos \omega t \frac{d\omega}{2\pi} = -\frac{\hbar}{2\pi} t^{-2}. \end{aligned}$$

so that the vacuum symmetrized correlation function is $(1/2)j(t-s)$.

This noise is *generalized* quantum (operator-valued) Gaussian process, $R(f) = \int_{-\infty}^\infty \hat{Z}(t)f(t)dt$, where f runs an appropriate space of test functions. The mathematical construction which gives to it a rigorous meaning is based on quasi-free representations of the C^* -algebra $\mathfrak{A}(\mathcal{H}, \Delta)$ of CCR [13] over the symplectic space $\mathcal{H} = \mathcal{K}(\mathbb{R})$ of real-valued infinite differentiable functions with compact support, ($\hbar = 2$), with the skew-symmetric form Δ and the vacuum inner product j , given by

$$\begin{aligned} \Delta(f, g) &= \int_{-\infty}^\infty f(t) \frac{d}{dt} g(t) dt = \pi^{-1} \text{Im} \int_0^\infty \overline{\omega f(\omega)} \tilde{g}(\omega) d\omega, \\ j(f, g) &= \pi^{-1} \text{Re} \int_0^\infty \overline{\omega f(\omega)} \tilde{g}(\omega) d\omega \\ &= \pi^{-1} \int_{-\infty}^\infty g(t) \int_{-\infty}^\infty \frac{2f(t) - f(t-s) - f(t+s)}{s^2} ds dt, \end{aligned}$$

see n.7.1 of [7]. The operator of complex structure J is multiplication by $i \text{sgn}(\omega)$ in the frequency domain or the Hilbert transform in the time domain

$$(Jz)(t) = \frac{1}{\pi} \text{V.P.} \int_{-\infty}^\infty \frac{z(s)}{t-s} ds$$

One can then introduce the gauge-covariant channels in the frequency domain by the equation

$$d\hat{A}_Y(\omega) = K(\omega) d\hat{A}_X(\omega) + d\hat{A}_Z(\omega)$$

where the appropriately modified Gaussian noise $\hat{Z}(t)$ satisfies (cf. [1])

$$\begin{aligned} [d\hat{A}_Z(\omega), d\hat{A}_Z^\dagger(\omega')] &= \frac{1}{2\pi} \delta(\omega - \omega') (1 - |K(\omega)|^2) d\omega d\omega', \\ \langle d\hat{A}_Z^\dagger(\omega) d\hat{A}_Z(\omega') \rangle &= \frac{1}{2\pi} \delta(\omega - \omega') N(\omega) d\omega d\omega' \end{aligned}$$

In the time domain, asymptotically (as $T \rightarrow \infty$)

$$\hat{Y}(t) \approx (KX)(t) + \hat{Z}(t), \quad (15)$$

with nonanticipating real-valued filter

$$(K\hat{X})(t) = \int^t \hat{X}(s)k(t-s)ds, \quad K(\omega) = \int_0^\infty k(t)e^{i\omega t} dt = \overline{K(-\omega)}.$$

If K is instantaneous or has finite memory, then (15) becomes equality.

A natural conjecture would be that the asymptotic (as $T \rightarrow \infty$) capacity of the channel (15) over observations in the subspace

$\mathcal{H}_T = \mathcal{K}([0, T])$ of test functions with support in $[0, T]$ is given by the expression (13) from the coding theorem above. Such a proof would be free from a simplification inherent in our model due to the assumed independence of the modes a_k for each T .

However an attempt to adapt the classical proof [5] meets the obstacles arising from the additional symplectic structure and the fact that the observation subspace \mathcal{H}_T is *not invariant* under the complex structure J . Such kind of problems do not arise in the “narrowband” approximations of the type considered in [1] where the Planck vacuum spectrum is replaced by the flat one. It is anticipated that the coding theorem for this model can be obtained by a complexification of the classical proof. For a comparative discussion of the two models see [11].

References

- [1] B. R. Bardhan, J. H. Shapiro, Ultimate capacity of linear time-invariant Bosonic channel, arXiv:1602.03182.
- [2] C. M. Caves, P. B. Drummond, Quantum limits of bosonic communication rates, *Rev. Mod. Phys.* **66:2** (1994) 481-538.
- [3] V. Giovannetti, A. S. Holevo, R. Garcia-Patrón, A solution of Gaussian optimizer conjecture for quantum channels, *Commun. Math. Phys.*, **334:3** (2015), 1553-1571.
- [4] V. Giovannetti, S. Lloyd, L. Maccone, P.W. Shor, Broadband channel capacities, *Phys. Rev. A* **68**, (2003) 062323.
- [5] R. G. Gallager, *Information Theory and Reliable Communications*. New York: J. Wiley 1968.
- [6] C. W. Helstrom, Quantum Detection Theory, *Progress in Optics*, **10** (1972) 291-369.
- [7] A. S. Holevo, *Investigations in the General Theory of Statistical Decisions*, Proc. of the Steklov Institute of Mathematics, vol. **124**, 1976 (AMS Translation 1978, Issue 3).
- [8] A. S. Holevo, Quantum coding theorems. *Russian Math. Surveys*, **53:6** 1998, 1295-1331. Arxiv:quant-ph/9809023.
- [9] A. S. Holevo, R. F. Werner, Evaluating capacities of Bosonic Gaussian channels. *Phys. Rev. A* **63**, (2001) 032312.
- [10] A. S. Holevo, Single-mode quantum Gaussian channels: structure and quantum capacity, *Probl. Inform. Transmission*, **43:1** (2007) 1-11.
- [11] A. S. Holevo, Quantum signal+noise models: beyond *i.i.d.* arXiv:1607.06905.
- [12] D. S. Lebedev, L. B. Levitin, The maximal amount of information transmissible by an electromagnetic field, *Information and Control*, **9** (1966) 1-22.
- [13] F. Manuceau, A. Verbeure, Quasi-free states of the CCR algebra and Bogoliubov transformations, *Commun. Math. Phys.* **9** (1968), 293-302.
- [14] G. De Palma, A. Mari, V. Giovannetti, Classical capacity of Gaussian thermal memory channels, *Phys. Rev. A* **90**, (2014) 042312.

Sparse Regression Codes

Ramji Venkataramanan, University of Cambridge, ramji.v@eng.cam.ac.uk
 Sekhar Tatikonda, Yale University, sekhar.tatikonda@yale.edu
 Andrew Barron, Yale University, andrew.barron@yale.edu

1. Introduction

Developing computationally-efficient codes that approach the Shannon-theoretic limits for communication and compression has long been one of the major goals of information and coding theory. There have been significant advances towards this goal in the last couple of decades, with the emergence of turbo and sparse-graph codes in the '90s [1, 2], and more recently polar codes and spatially-coupled LDPC codes [3–5]. These codes are all primarily for discrete-alphabet sources and channels.

There are many channels and sources of practical interest where the alphabet is inherently continuous, e.g., additive white Gaussian noise (AWGN) channels, and Gaussian sources. A promising class of codes for Gaussian models is the recently proposed *Sparse Superposition Codes* or *Sparse Regression Codes* (SPARCs). This article provides a broad overview of SPARCs, covering theory, algorithms, and some practical implementation aspects. At the end, we discuss some open problems and future directions for research.

This survey is based on the tutorial on sparse regression codes presented at ISIT '16¹. The discussion will be relatively informal. We paraphrase some of the technical results with the aim of providing intuition, and point the reader to references for an in-depth discussion.

To motivate the construction of SPARCs, let us begin with the standard AWGN channel with signal-to-noise ratio denoted by snr . The goal is to construct codes with computationally efficient encoding and decoding that *provably* achieve the channel capacity $C = (1/2)\log(1 + \text{snr})$ bits/transmission. In particular, we are interested in codes whose encoding and decoding complexity grows no faster than a low-order polynomial in the block length n .

Though it is well known that rates approaching C can be achieved with Gaussian codebooks, this has been largely avoided in practice due to the high decoding complexity of unstructured Gaussian codes. Instead, the popular approach has been to separate the design of the coding scheme into two steps: *coding* and *modulation*. State-of-the-art coding schemes for the AWGN channel such as coded modulation [6–8] use this two-step design, and combine binary error-correcting codes such as LDPC and turbo codes with standard modulation schemes such as Quadrature Amplitude Modulation (QAM). Though such schemes have good empirical performance, they have not been proven to be capacity-achieving for the AWGN channel.

With sparse regression codes, we step back from the coding/modulation divide and instead use a structured codebook to construct low-complexity, capacity-achieving schemes tailored to the AWGN channel. In a SPARC, codewords are sparse linear combinations of columns of a design matrix (see Fig. 1). The codewords are indexed by the locations of non-zeros in each section.

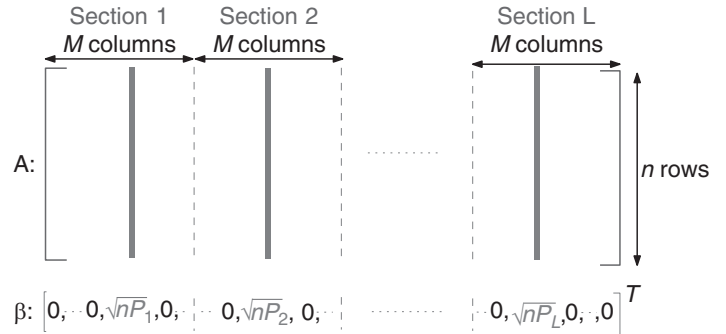


Figure 1: A Gaussian sparse regression codebook of block length n : A is a design matrix with independent Gaussian entries, and β is a sparse vector with one non-zero in each of L sections, where $L \sim (n/\log n)$. Codewords are of the form $A\beta$, i.e., linear combinations of the columns corresponding to the non-zeros in β . The message is indexed by the *locations* of the non-zeros, and the values P_1, \dots, P_L are fixed a priori.

We explain in Sec. 2 how the parameters of the design matrix determine the rate of the code, average power etc. In Sec. 3, we will see how the structure of the design matrix enables fast iterative decoding algorithms whose probability of decoding error decays rapidly with block length for rates $R < C$. Further, these codes also achieve the Shannon limit for lossy compression (Sec. 4), and can be easily combined to implement superposition and binning (Sec. 5). Thus sparse regression codes offer a way to construct low-complexity, rate-optimal codes for a variety of canonical models in network information theory.

We should mention that lattice codes are another class of structured codes for Gaussian channel and source models [9]. Several elegant coding schemes based on lattices have been proposed in the literature, e.g. [10–12], but we will not discuss these further in this article.

2. The Sparse Regression Codebook

As shown in Fig. 1, a SPARC is defined in terms of a ‘dictionary’ or design matrix A of dimension $n \times ML$, whose entries are *i.i.d.* $\mathcal{N}(0, \frac{1}{n})$. Here n is the block length, and M, L are integers whose values are specified below in terms of n and the rate R . We think of the matrix A as being composed of L sections with M columns each. Each codeword is a linear combination of L columns, with one column coming from each section. Formally, a codeword can be expressed as $A\beta$, where β is an $ML \times 1$ vector $(\beta_1, \dots, \beta_{ML})$ with the following property: there is exactly one non-zero β_j for $1 \leq j \leq M$, one non-zero β_j for $M + 1 \leq j \leq 2M$, and so forth. The non-zero value of β in section $\ell \in [L]$ is set to $\sqrt{nP_\ell}$, where the positive constants P_ℓ satisfy $\sum_{\ell=1}^L P_\ell = P$. (We use the notation $[L]$ to denote the set $\{1, \dots, L\}$.)

P is the average power per input symbol in the case of channel coding; in lossy compression it will be the variance of each codeword symbol.

¹The slides from the tutorial are available at <https://goo.gl/8H8wrk>

Since each of the L sections contains M columns, the total number of codewords is M^L . To obtain a rate R code, we need

$$M^L = 2^{nR} \quad \text{or} \quad L \log M = nR. \quad (1)$$

(Throughout, we use \log for logarithm with base 2, and \ln for base e .) There are several choices for the pair (M, L) which satisfy (1). For example, $L = 1$ and $M = 2^{nR}$ recovers the Shannon-style random codebook in which the number of columns in A is 2^{nR} . For our constructions, we will choose M equal to L^a , for some constant $a > 0$. In this case, (1) becomes

$$aL \log L = nR. \quad (2)$$

Thus $L = \Theta(n/\log n)$, and the size of the design matrix A (given by $n \times ML = n \times L^{a+1}$) grows polynomially in n . In our numerical simulations, typical values for L are 512 or 1024.

We note that the SPARC is a non-linear code with pairwise dependent codewords. Two codewords $A\beta$ and $A\beta'$ are dependent whenever the underlying message vectors β, β' share one or more common non-zero entries.

Power Allocation: The coefficients $\{P_\ell\}_{\ell=1}^L$, plays an important role in determining the performance of the code, both for channel coding and for lossy compression. We will consider allocations where $P_\ell = \Theta(1/L)$. Two examples are:

- Flat power allocation across sections: $P_\ell = \frac{P}{L}, \ell \in [L]$.
- Exponentially decaying power allocation: Fix parameter $\kappa > 0$. Then $P_\ell \propto 2^{-\kappa\ell/L}, \ell \in [L]$.

In Section 3, we discuss computationally efficient decoders which asymptotically achieve capacity with the exponentially decaying allocation (with $\kappa = 2C$). To improve decoding performance at practical block lengths, we explore different power allocation strategies in Section 3.3, and demonstrate that judicious power allocation can lead to dramatic improvements in decoding performance at finite block lengths. We also describe how decoding complexity can be reduced by replacing the Gaussian design matrix with a Hadamard-based design.

3. AWGN Channel Coding with SPARCs

The channel is described by the model

$$y_i = x_i + w_i, \quad i = 1, \dots, n. \quad (3)$$

The noise variables w_i are *i.i.d.* $\sim \mathcal{N}(0, \sigma^2)$. There is an average power constraint P on the input: the codeword $x := (x_1, \dots, x_n)$ should satisfy $\frac{1}{n} \sum_{i=1}^n x_i^2 \leq P$. The signal-to-noise ratio P/σ^2 is denoted by snr .

Encoding: The encoder splits its stream of input bits into segments of $\log M$ bits each. A length ML message vector β_0 is indexed by L such segments – the decimal equivalent of segment ℓ determines the position of the non-zero coefficient in section ℓ of β_0 . The input codeword is then computed as $x = A\beta_0$. Note that computing x simply involves adding L columns of A , weighted by the appropriate coefficients.

Optimal Decoding: Assuming that the codewords are equally likely, the optimal decoder produces

$$\hat{\beta}_{\text{opt}} = \underset{\beta}{\text{argmin}} \|y - A\beta\|^2,$$

where $y := (y_1, \dots, y_n)$, and the minimum is over all the message vectors in the codebook.

Probability of Error: The performance of a SPARC decoder is measured by the *section error rate*, which is the fraction of sections decoded wrongly. The section error rate is denoted by $\mathcal{E}_{\text{sec}} := \frac{1}{L} \sum_{\ell=1}^L 1\{\hat{\beta}_\ell \neq \beta_{0\ell}\}$. For a given decoder, we will aim to bound the probability of the event $\{\mathcal{E}_{\text{sec}} > \epsilon\}$ for $\epsilon > 0$. Assuming that the mapping determining the non-zero location for each segment of $\log M$ input bits is generated uniformly at random, a section error will, on average, lead to half the bits corresponding to the section being decoded wrongly. Therefore, when a large number of segments are transmitted, the *bit error rate* of a SPARC decoder will be close to half its section error rate.

If we want the decoding error probability of the message β_0 to be small, we can use a concatenated code with the SPARC as the inner code and an outer Reed-Solomon (RS) code. (An RS code of rate $(1 - 2\epsilon)$ can correct upto a fraction ϵ of section errors in the SPARC; see [13] for details.)

We will not consider the outer RS code in the remainder of this article, and focus mostly on the section error rate (or bit error rate) of the SPARC.

Performance with Optimal Decoding: For rates $R < C$, the least-squares decoder was shown in [13] to have error probability decaying exponentially in the block length.

Theorem 1. [13] *Consider a SPARC with rate $R < C$, block length n , and equal power allocation, i.e. $P_\ell = (P/L), \ell \in [L]$. For any $\epsilon > 0$, the section error rate of the least-squares decoder satisfies*

$$\mathbb{P}(\mathcal{E}_{\text{sec}} > \epsilon) \leq Ke^{-\kappa n \min\{\epsilon, (C-R)^2\}},$$

where κ, K are universal positive constants.

This result was extended to SPARCs with *i.i.d.* binary (± 1) design matrices in [14, 15]. The exponent κ in Theorem 1 is smaller than the Shannon-Gallager random coding exponent, but the result shows that SPARCs are essentially as good as Shannon-style random codes for the AWGN channel with maximum-likelihood decoding.

3.1. Feasible SPARC Decoders

In contrast to the least-squares decoder, the feasible decoders we discuss all use a decaying power allocation across sections. Thinking of the L sections of a SPARC as analogous to L users sharing a Gaussian multiple-access channel (MAC), leads to an exponentially decaying power allocation of the form $P_\ell \propto 2^{-2C\ell/L}, \ell \in [L]$. Indeed, consider the equal-rate point on the capacity region of a L -user Gaussian MAC where each user gets rate C/L . It is well-known [16, 17] that this rate point can be achieved with the above power allocation via successive cancellation decoding, where user 1 is first decoded, then user 2 is decoded after subtracting the codeword of user 1, and so on.

However, successive cancellation performs poorly for SPARC decoding. This is because L , the number of sections (“users”) in the codebook, grows as $n/\log n$, while M , the number of codewords per user, only grows polynomially in n . An error in decoding one section affects the decoding of future sections, leading to a large number of section errors after L steps.

The first feasible SPARC decoder, proposed in [18], controls the accumulation of section errors using *adaptive* successive decoding. The idea is to not pre-specify the order in which sections are decoded, but to look across all the undecoded sections in each step, and adaptively decode columns which have a large inner product with the residual. The main ingredients of the algorithm are as follows. In the first step, the decoder computes the inner product of each column of the design matrix with the normalized channel output sequence $y/\|y\|$, and picks those columns for which this test statistic exceeds a pre-specified threshold; this gives the first estimate $\hat{\beta}_1$. In the second step, the test statistic is generated based on the *residual* $r^1 = y - A\hat{\beta}_1$: the decoder picks the columns (from the as yet undecoded sections) whose inner product with $r^1/\|r^1\|$ crosses the threshold; this gives $\hat{\beta}^2$. The algorithm continues in this fashion, decoding columns using the residual-based statistics in each step. The algorithm is run for a pre-specified number of steps, arranged to be of the order of $\log M$; it terminates earlier if at least one column has been selected from each section, or the test-statistics in any step are all below the threshold.

The performance of this decoder was analyzed in [18]. With power allocation $P_\ell \propto 2^{-2c\ell/L}$, it was shown that the probability of message decoding error decays as $\exp(-kL(C_M R)^2)$, where $C_M = C(1 - \frac{c}{\log M})$ for a constant $c > 0$, and R is the total rate (SPARC combined with an outer Reed-Solomon code).

Therefore the adaptive successive threshold decoder is capacity-achieving, and the gap to capacity is of order $1/\log M$. However, in practice, the section error rates at practically feasible block lengths are observed to be rather high for rates near capacity. The following two decoders improve the decoding performance by avoiding hard decisions about which columns to decode in each step.

3.2. Iterative Soft-decision Decoding

The key idea in the next two decoders is to iteratively update the posterior probabilities of each entry of β being the true non-zero in its section. The goal in both decoders is to iteratively generate test statistics that (in step t) have the form $\text{stat}_t \approx \beta + \tau_t Z_t$, where Z_t is standard normal and independent of β . In words, stat_t is essentially the message vector observed in independent additive Gaussian noise with known variance τ_t^2 . Assuming this is true, the Bayes-optimal estimate for β in the next step is

$$\beta^{t+1}(\text{stat}_t) = \mathbb{E}[\beta | \beta + \tau_t Z_t = \text{stat}_t] = \eta_t(\text{stat}_t),$$

where the conditional expectation $\eta_t(\cdot)$ can be computed using the known prior on β (locations of non-zeros uniformly distributed within each section). For indices j in section ℓ of β , we have

$$\eta_{i,j}(s) := \sqrt{nP_\ell} \frac{\exp(\sqrt{nP_\ell} s_j / \tau_t^2)}{\sum_{k \in \text{sec}_\ell} \exp(\sqrt{nP_\ell} s_k / \tau_t^2)}, \quad j \in \text{section } \ell, \ell \in [L]. \quad (4)$$

Note that $\eta_{i,j}(s)/\sqrt{nP_\ell}$ is the posterior probability (given stat_t) that term j is the non-zero coefficient in section ℓ of β .

In addition to stat_t having the desired distributional representation, we also want τ_t^2 , the variance of the noise in the test statistic, to be computable iteratively from τ_{t-1}^2 as follows. Starting with $\tau_0^2 = \sigma^2 + P$, we define

$$\begin{aligned} \tau_t^2 &= \sigma^2 + \frac{1}{n} \mathbb{E} \|\beta - \mathbb{E}[\beta | \beta + \tau_{t-1} Z_{t-1}]\|^2 \\ &= \sigma^2 + \frac{1}{n} \mathbb{E} \|\beta - \eta_t(\beta + \tau_{t-1} Z_{t-1})\|^2, \end{aligned} \quad (5)$$

where the expectation on the right is over β and the independent standard normal vector Z_t . In other words, we want the noise in the test statistic to have two independent Gaussian components: one component with variance σ^2 arising from the channel noise, and the other component arising from the error in the current estimate β^t . The recursion to generate τ_t^2 from τ_{t-1}^2 can be written as

$$\tau_t^2 = \sigma^2 + P(1 - x_t(\tau_{t-1})) \quad (6)$$

where $x_t := x(\tau_{t-1})$ is an expectation of a function of ML standard normal random variables. The exact formula for $x(\tau_{t-1})$ can be found in [19, Sec. 3]. Compact asymptotic formulas for x_t , τ_t^2 are given in Lemma 1 below.

Therefore, under the assumed distribution for stat_t , we have $\frac{1}{n} \mathbb{E} \|\beta - \beta^t\|^2 = P(1 - x_t)$; it can also be shown that $\frac{1}{n} \mathbb{E}[\beta^T \beta^t] = \frac{1}{n} \mathbb{E} \|\beta^t\|^2 = P x_t$ [19, Prop. 3.1]. Thus the scalar x_t can be interpreted as the expected (power-weighted) success rate, and $P(1 - x_t)$ as the expected interference contribution to the noise variance τ_t^2 due to the undecoded sections. With this interpretation, for successful decoding we want x_t to be very close to 1 when the algorithm terminates. Indeed, it can be verified that for all rates less than C and $P_\ell \propto 2^{-2c\ell/L}$, the iteration (6) has a fixed point with τ_t^2 close to σ^2 , i.e., x_t is close to one. A more precise version of this statement in the large system limit is given in Lemma 1 below.

Finally, the key question is: how do we iteratively generate statistics stat_t that *in each step* are well-approximated as $\beta + \tau_t Z_t$, with τ_t^2 having the representation described above? The two decoders described below achieve this via seemingly very different approaches.

Adaptive Successive Soft-Decision Decoder [20–22]

The statistics for this decoder are defined using the fits $\text{Fit}_0 := Y, \text{Fit}_1 := A\beta^1, \dots, \text{Fit}_t := A\beta^t$. With $G_0 := Y$, recursively define G_t to be the part of Fit_t that is orthogonal to G_0, G_1, \dots, G_{t-1} . The ingredients of stat_t are the vectors $\mathcal{Z}_0, \dots, \mathcal{Z}_t$, defined as

$$\mathcal{Z}_k = \sqrt{n} \frac{A^T G_k}{\|G_k\|}, \quad k \geq 0.$$

The test statistic is then defined as $\text{stat}_t = \tau_t \sum_{k=0}^t \lambda_k \mathcal{Z}_k + \beta^t$. The weights λ_k have to be carefully chosen in order for stat_t to be close enough in distribution to the desired form $\beta + \tau_t \mathcal{Z}_t$. The estimate β^{t+1} is generated as $\eta_t(\text{stat}_t)$, where $\eta_t(\cdot)$ is given by (4).

Two different ways to choose the weights $\lambda_k, 0 \leq k \leq t$, are proposed in [21, 22]. Each of these choices is based on a technical lemma [20, Lemma 1] characterizing the distribution of $\mathcal{Z}_k, \forall k$. The first choice of weights is deterministic, and given by

$$(\lambda_0, \lambda_1, \dots, \lambda_t) : \tau_t \left(\frac{1}{\tau_0}, -\sqrt{\frac{1}{\tau_1^2} - \frac{1}{\tau_0^2}}, \dots, -\sqrt{\frac{1}{\tau_t^2} - \frac{1}{\tau_{t-1}^2}} \right), \quad (7)$$

where τ_0, \dots, τ_t are given by (5). The analysis in [21] shows that this choice of weights makes stat_t close to the desired representation $\beta + \tau_t Z_t$, leading to the following concentration result.

Theorem 2. [21, Lemma 7] Consider a SPARC with rate $R < C$, parameters (n, L, M) chosen according to (1), and power allocation $P_\ell \propto 2^{-2c\ell/L}$. For $t \geq 1$, let

$$\mathcal{A}_t := \left\{ \left| \frac{1}{nP} \beta^T \beta^t - x_t \right| > \epsilon \right\} \cup \left\{ \left| \frac{1}{nP} \|\beta^t\|^2 - x_t \right| > \epsilon \right\}.$$

Then, we have

$$\mathbb{P}\{\cup_{k=1}^t \mathcal{A}_k\} \lesssim \sum_{k=1}^t a_k \exp\left(-k \frac{n}{(\log M)^{2k+1}} \epsilon^2\right),$$

where k, a_1, \dots, a_t are universal constants depending on R, C .

The probability bound on the event \mathcal{A}_t in Theorem 2 can be shown to imply a probability bound for the section-error rate exceeding $c\epsilon$, where $c > 0$ is a constant. Thus the probability of decoding failure decays exponentially in $n/(\log n)^{2T^*+1}$, where T^* is the number of steps for which the algorithm is run. This is in contrast to the optimal decoder in Theorem 1 whose probability of decoding failure decays exponentially in n .

As an alternative to the deterministic weights in (7), weights $\{\lambda_k\}$ depending on the channel output y were also proposed in [21]. This choice is based on the Cholesky decomposition of a matrix generated from the estimates $\{\beta^1, \dots, \beta^t\}$. A performance guarantee similar to Theorem 2 can be obtained for this set of weights as well; see [21, 22] for details.

Approximate Message Passing Decoder [19, 23]

Approximate message passing (AMP) refers to a class of algorithms [24–30] that are Gaussian or quadratic approximations of loopy belief propagation algorithms (e.g., min-sum, sum-product) on dense factor graphs. In its basic form [24, 27], AMP gives a fast iterative algorithm to solve the LASSO, i.e., to compute

$$\hat{\beta}_{\text{LASSO}} = \arg \min_{\hat{\beta}} \|y - A\hat{\beta}\|_2^2 + \lambda \|\hat{\beta}\|_1,$$

for any $\lambda > 0$. Recall that the decoding problem we wish to solve is

$$\hat{\beta}_{\text{SPARC}} = \arg \min_{\hat{\beta}} \|y - A\hat{\beta}\|_2^2 \text{ over } \hat{\beta} \text{ that are valid SPARC code-words.}$$

One cannot directly use the LASSO-AMP of [24, 27] for SPARC decoding as it does not use the prior knowledge about β , i.e., the knowledge that β has exactly one non-zero value in each section, with the values of the non-zeros also being known.

An AMP decoder for SPARCs can be derived by writing down min-sum like updates for the SPARC decoding problem, and then approximating them using the recipe in [26]. This leads to a decoder with the following update rules [19]. Define $r^0 = y$, and for $t \geq 1$ compute:

$$\begin{aligned} r^t &= y - A\beta^t + \frac{r^{t-1}}{\tau_{t-1}^2} \left(P - \frac{\|\beta^t\|^2}{n} \right), \\ \text{stat}_t &= A^T r^t + \beta^t, \\ \beta^{t+1} &= \eta_t(\text{stat}_t). \end{aligned}$$

The coefficients τ_t^2 are recursively defined by (6), starting with $\tau_0^2 = \sigma^2 + P$. Following the terminology in [24, 26], we refer to this recursion as state evolution (SE). Recall that the SE equations are derived under the assumption that stat_t is distributed as $\beta + \tau_t Z_t$. The presence of the ‘‘Onsager’’ term $r^{t-1}/\tau_{t-1}^2 (P - \frac{\|\beta^t\|^2}{n})$ in the definition of the modified residual r^t is crucial to ensure that the distributional assumption is valid, at least asymptotically. Intuition about role of the Onsager term in the standard AMP algorithm can be found in [26, Section I-C].

We can derive a compact asymptotic formula for the SE recursion by taking the limit as $L, M, n \rightarrow \infty$ while satisfying (1). (This limit is denoted below by ‘lim’.)

Lemma 1. [19] For $t \geq 1$, the asymptotic value of τ_t^2 , denoted by $\bar{\tau}_t^2$, is given by

$$\bar{\tau}_t^2 = \sigma^2 + P(1 - \bar{x}(\bar{\tau}_{t-1})),$$

where the function $\bar{x}(\cdot)$ is defined as follows. With $c_\ell := LP_\ell$, we have

$$\bar{x}(\tau) := \lim x(\tau) = \lim \sum_{\ell=1}^L \frac{P_\ell}{P} 1\{\lim c_\ell > 2(\ln 2)R\tau^2\}.$$

Recalling that x_{t+1} is the expected power-weighted fraction of correctly decoded sections after step $(t+1)$, for any power allocation $\{P_\ell\}$, Lemma 1 may be interpreted as follows: in the large system limit, for a section ℓ to be correctly decoded in step $(t+1)$, the limit of LP_ℓ must exceed a threshold equal to $2(\ln 2)R\bar{\tau}_t^2$. All sections which satisfy this condition will be decodable in step $(t+1)$ (i.e., will have most of the posterior probability mass on the correct term). Conversely, any section whose power falls below the threshold will not be decodable in this step.

Lemma 1 can be used to quickly check whether a given power allocation is good by checking whether $\bar{x}(\tau_t)$ monotonically increases with t from 0 to 1. When applied to the exponentially decaying power allocation $P_\ell \propto 2^{-2c\ell/L}$, Lemma 1 gives

$$\bar{\tau}_t^2 = \sigma^2(1 + \text{snr})^{1-\xi_{t-1}}, \quad \bar{x}_t = \frac{(1 + \text{snr}) - (1 + \text{snr})^{1-\xi_{t-1}}}{\text{snr}} \text{ for } t > 0, \quad (8)$$

where $\xi_{t-1} := 0$ and

$$\xi_t = \min\left\{\left(\frac{1}{2C}\right)\log\left(\frac{C}{R}\right) + \xi_{t-1}, 1\right\}.$$

The constants $\{\xi_t\}_{t \geq 0}$ have a nice interpretation in the large system limit: for $R < C$, at the end of step $t+1$, the first ξ_t fraction of sections in β^{t+1} will be correctly decodable with high probability. An additional $\frac{1}{2C}\log(\frac{C}{R})$ fraction of sections become correctly decodable in each step until step $T^* = \lceil 2C/\log(C/R) \rceil$, when all the sections are correctly decodable with high probability.

The following theorem shows that the AMP decoder achieves capacity by showing that the above interpretation based on the SE equations is true in the large system limit.

Theorem 3. For any rate $R < C$, consider a sequence of rate R SPARCs $\{S_n\}$ indexed by block length n and power allocation $P_\ell \propto 2^{-2c\ell/L}$. Then the section error rate of the AMP decoder (run for T^* steps, with the constants $\bar{\tau}_t^2$ given by (8)) converges to zero almost surely, i.e., for any $\epsilon > 0$,

$$\lim_{n_0 \rightarrow \infty} \mathbb{P}(\mathcal{E}_{\text{sec}}(S_n) < \epsilon, \forall n \geq n_0) = 1.$$

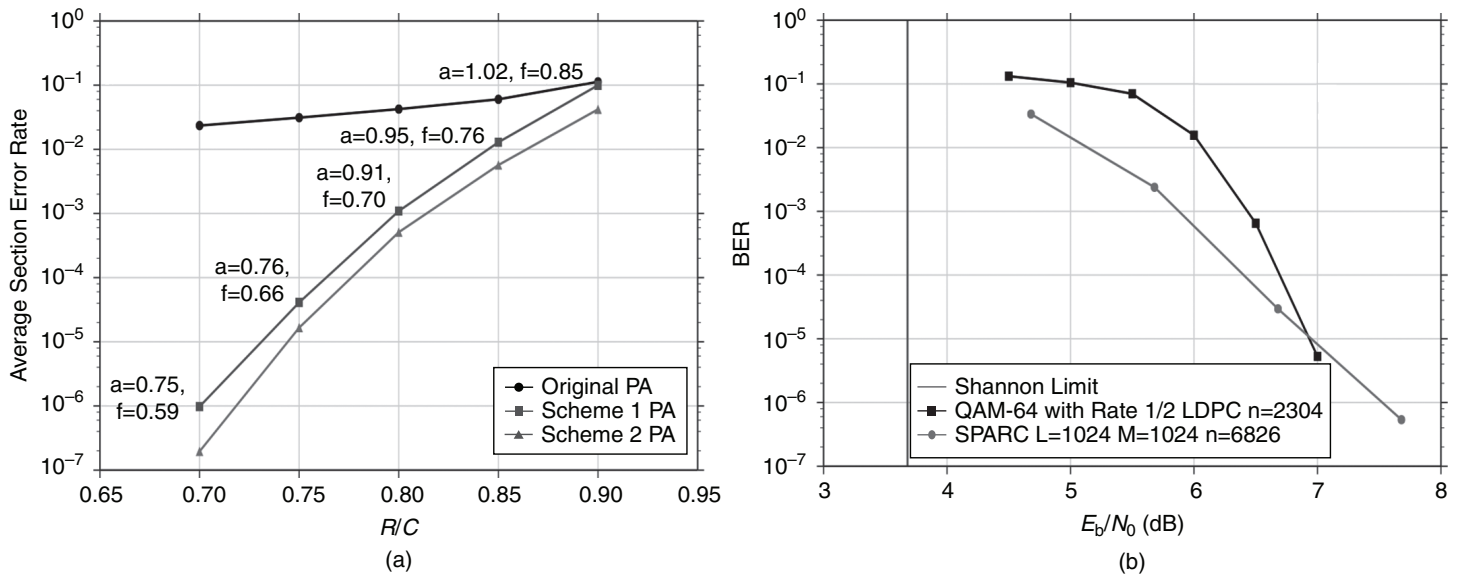


Figure 2: Performance with AMP decoding: a) Section error rate vs. R with $\text{snr} = 15$, $C = 2$ bits, SPARC parameters $M = 512$, $L = 1024$; b) Bit error rate of SPARC vs. E_b/N_0 at $R = 1.5$, compared with coded modulation at information rate = 1.5 bit/dimension.

In recent work, we have used the the finite-sample AMP analysis techniques of [31] to refine the asymptotic result of Theorem 3 and obtain a large-deviations bound similar to Theorem 2 for the probability of the section error rate exceeding ϵ .

Computational Complexity

With a Gaussian design matrix, the running time and memory requirement of both the adaptive successive soft-decision decoder and the AMP decoder are of the same order: $O(nML)$. However, in practice the AMP decoder is faster as no orthonormalization or Cholesky decomposition is required to compute its test statistic in each step. Further, as described in [19], choosing the design matrix by uniformly sampling n rows of the $ML \times ML$ Hadamard matrix reduces the AMP running time to $O(ML \log M)$. The Hadamard-based design matrix does not need to be stored, hence there is also a large saving in required memory. Finally, the partitioned structure of the SPARC could be exploited to design parallelized or pipelined implementations of the above decoders.

3.3. Empirical performance at practical blocklengths

Though all three decoders theoretically have section error-rate decaying to zero with increasing block length for any fixed $R < C$, the soft-decision decoders have much better empirical performance [19, 22]. In the following, we illustrate the performance of the AMP decoder for block lengths of the order of a few thousands. All the simulation results are obtained using Hadamard-based designs.

Fig. 2a illustrates the performance for a SPARC with $M = 512$, $L = 1024$, $\text{snr} = 15$ at various values of rate R . The block length n is determined by R according to (1). For example, we have $n = 7680$ for $R = 0.6C$, and $n = 5120$ for $R = 0.9C$. The top curve shows the average section error rate of the AMP (over 1000 runs) with the power

$P_\ell \propto 2^{-2C\ell/L}$ allocation. The bottom two curves are obtained with two alternative power allocation (PA) schemes, discussed below. Though $P_\ell \propto 2^{-2C\ell/L}$ is the optimal PA for rates very close to C , it is clear that as we back off from capacity, a carefully chosen PA can reduce the error rate by several orders of magnitude.

PA Scheme 1: The PA is determined by two parameters a, f . For $a > 0$ and $f \in [0, 1]$, let

$$P_\ell = \begin{cases} \kappa \cdot 2^{-a2C\ell/L}, & 1 \leq \ell \leq fL \\ \kappa \cdot 2^{-a2Cf}, & fL + 1 \leq \ell \leq L, \end{cases}$$

where κ is a normalizing constant chosen so that $\sum_\ell P_\ell = P$. The parameter a controls the decay of the exponential. Increasing a increases the power allocated to the initial sections which makes them more likely to decode correctly, which in turn helps by decreasing the effective noise variance in subsequent AMP iterations. However, if a is too large, the final sections may have too little power to decode correctly – this is why the standard PA with $a = 1$ performs poorly for rates that are not close to capacity. Thus we want the parameter a to be large enough to ensure that the AMP gets started on the right track, but not much larger.

The parameter f controls the *flattening* of the PA. The exponentially decaying PA may leave too little power for the final sections. To address this issue, the idea is to have an exponential PA only for a fraction f of the sections, and allocate the remaining power equally among the rest of the sections. The middle curve in Fig. 2a shows the performance of the AMP with numerically optimized (a, f) values for each rate. As expected, the optimal values of a, f decrease as we back off from capacity.

PA Scheme 2: Optimizing the parameters (a, f) is computationally intensive and has to be done separately for each rate and snr value of interest. To address this, we have recently developed a simple PA algorithm based on Lemma 1. If the AMP decoder is run for T^* steps, the goal (in the large system limit) is to have the first $1/T^*$ fraction of sections be decodable in the first step; the second $1/T^*$ fraction be decodable in the second step, and so on. Starting with $\bar{\tau}_0^2 = \sigma^2 + P$, Lemma 1 lets us calculate the minimum power required for a

section to be decodable in the first step. We allocate approximately this power to each of the first L/T^* sections. Then compute $\hat{\tau}_1^i$, and from Lemma 1, the minimum power required for a section to now be decodable; allocate approximately this amount of power to the next L/T^* sections. Repeat this process sequentially for each set of L/T^* sections, with the following caveat: at any stage if the minimum power prescribed by Lemma 1 is less than what could be obtained by allocating the available power equally among the remaining sections, then choose the latter and complete the power allocation.

The bottom curve at the bottom in Fig. 2a shows the decoding performance of the AMP with this PA scheme. Clearly, the performance is at least as good as the first scheme, without having to optimize over the parameters (a, f) . We used the second PA scheme to compare the performance of the SPARC with that of coded modulation schemes which combine QAM constellations with a powerful binary LDPC code. Fig 2b illustrates the bit-error performance of a SPARC vs. coded modulation at rate 1.5 bit/dim. at various values of E_b/N_0 . (For the SPARC, E_b/N_0 can be calculated as $E_b/N_0 = \text{snr}/(2R)$.) The coded modulation scheme consists of a 64-QAM constellation with a rate 1/2 LDPC code. The LDPC code is specified in the WiMAX standard 802.16e and was implemented using the Coded Modulation Library [32]. We see that the SPARC with AMP decoding achieves a BER of 10^{-4} at snr around 2.5 dB from the Shannon limit.

Another way to improve the empirical performance of SPARCs is via *spatially coupled* design matrices, as demonstrated in [23, 33, 34]. Here the idea is to have a band-diagonal structure for the design matrix, with overlapping Hadamard blocks near the diagonal and zeros elsewhere. The idea is to have some extra channel outputs to reliably determine the first few sections of β ; this kick-starts a decoding progression due to the overlapping structure of the design matrix.

4. Lossy Compression with SPARCs

In this section we show that SPARCs are useful for lossy compression of continuous alphabet sources with squared-error distortion criterion. For any ergodic source with variance v^2 , the goal is to develop computationally efficient codes that achieve a target distortion D with a rate R as close as possible to the Gaussian rate-distortion bound $R^*(D) = v^2 e^{-2R}$ nats. (For this section alone, it will be convenient to use natural logarithms and measure rate in nats.)

The sparse regression codebook is exactly as described in Section 2, with codewords of the form $A\beta$ where β has one non-zero entry in each section. The only difference is that the values of the non zeros, $\{\sqrt{nP_\ell}\}$, do not have to satisfy a power constraint; they can be chosen in any way to help the compression encoder.

Optimal Encoding: Given a source sequence $s := (s_1, \dots, s_n)$, the optimal (least-squares) encoder determines $\hat{\beta}_{opt} := \text{argmin} \|s - A\hat{\beta}\|^2$, where the minimization is over all $\hat{\beta}$ with the SPARC structure. The positions of the non-zeros in $\hat{\beta}_{opt}$ are conveyed using R nats/sample to the decoder, which produces the reconstruction $\hat{s} = A\hat{\beta}_{opt}$.

The following result characterizes the probability of excess distortion with optimal encoding.

Theorem 4. [35, 36] Let $s := (s_1, \dots, s_n)$ be drawn from an ergodic source with mean zero and variance σ^2 . Let $D \in (0, \sigma^2)$, $R > \frac{1}{2} \ln \frac{\sigma^2}{D}$, and $\gamma^2 \in (\sigma^2, De^{2R})$. Let $P_\ell = (P/L) \forall \ell$ and let the SPARC parameters

determined by (1) satisfy $M = L^a$ for $a > a^*$, where the constant a^* depends only on R and γ^2/D . Then for all sufficiently large n ,

$$\mathbb{P}\left(\frac{1}{n} \|s - A\hat{\beta}_{opt}\|^2 > D\right) \leq \mathbb{P}\left(\frac{\|s\|^2}{n} > \gamma^2\right) + \exp(-\kappa n^{1+c}), \quad (9)$$

where κ, c are strictly positive constants.

A few remarks about the two terms on the right-hand side of (9). The first term is the probability of the source sequence being atypical, i.e., the probability that its second moment is significantly greater than σ^2 . The second term is the probability that the SPARC does not contain a codeword within distortion D of a typical source sequence. Note that the second term decays super-exponentially in n . Thus, if the probability of observing an atypical source sequence decays exponentially in n (e.g., as for an i.i.d. Gaussian source), it is the first term that dominates the excess distortion probability. The phenomenon of source atypicality being the dominant error event can also be observed in the analysis of the optimal excess-distortion exponent for memoryless discrete and Gaussian sources [37, 38].

An immediate corollary of Theorem 4 is that SPARCs with least-squares encoding achieve the *optimal* excess-distortion exponent for memoryless Gaussian sources derived in [38]. This result should be contrasted with the AWGN channel coding result (Theorem 1), where SPARCs with optimal decoding have probability of error decreasing exponentially in n , but the error exponent is smaller than the Shannon-Gallager random coding exponent [13].

The proof of Theorem 4 uses some techniques recently developed to characterize thresholds for random graph coloring and random constraint satisfaction problems [39, 40]. Denote the number of codewords that are within distortion D of the source sequence by Z . We need to upper bound the probability of the event $Z = 0$. Due to the dependence structure of the codewords, the techniques we use boils the analysis down to showing that $\mathbb{E}Z^2$ is of the same order as $(\mathbb{E}Z)^2$. Curiously, for distortions $D \geq 0.2v^2$, the required condition is true only for rates greater than a threshold which is *strictly larger* than $R^*(D)$ [35]. To prove that Theorem 4 holds for all distortions, we use a refined second-moment analysis in [36] that excludes design matrix realizations that give rise to an atypically large number of solutions. This approach is inspired by a similar idea used to obtain improved thresholds for the problem of coloring random hypergraphs [39], and could potentially be useful in other probabilistic settings where one needs to count the number of (dependent) solutions.

Feasible Encoding: A simple SPARC compression encoder based on successive cancellation was proposed in [41]. The encoder starts with $\beta^0 = 0$, and sequentially encodes the position of the non-zero in each section of β . The non-zero location in section ℓ corresponds to the column in the ℓ th section of A that maximizes the inner product with the residual $S - A\beta^{\ell-1}$. The update β^ℓ is then generated by setting the non-zero value in section ℓ to $\sqrt{2(\ln M)v^2(1 - \frac{2R}{L})^{\ell-1}}$. After the non-zero location in the final section is chosen, the codeword is computed as $A\beta^L$.

Theorem 5. [41] For an ergodic source S with mean 0 and variance v^2 , the encoding algorithm produces a codeword $A\hat{\beta}$ that satisfies the following for sufficiently large M, L :

$$\mathbb{P}\left(\frac{1}{n} \|S - A\hat{\beta}\|^2 > v^2 e^{-2R} + \Delta\right) < e^{-\kappa n(\Delta - \frac{c \ln \ln M}{\ln M})}$$

where κ, c are universal positive constants.

We can view the encoder as successively refining the source over $L \sim (n/\log n)$ stages, with each stage being a rate-distortion code of rate R/L . The first stage is an optimal code of rate R/L for an *i.i.d.* $\mathcal{N}(0, \nu^2)$ source. This implies that the residual $r_1 = s - A\beta^1$ satisfies $\|r_1\|^2/n \approx \nu^2 e^{-2R/L} \approx \nu^2 (1 - \frac{2R}{L})$. The residual r_1 acts as the ‘source’ sequence for the second stage, which is an optimal rate-distortion code for source variance $\nu^2 e^{-2R/L}$. At the end of the second stage, we have the residual r_2 , which gets refined by the third stage, and so on. Each stage of refinement reduces the variance of the incoming residual by a factor of approximately $(1 - \frac{2R}{L})$. Therefore, we expect that the final distortion $\|r_L\|^2/n \approx \nu^2 (1 - \frac{2R}{L})^L \leq \nu^2 e^{-2R}$.

However, since the rate R/L is infinitesimal, the deviations from the expected distortion in each stage can be significant. The essence of the proof of Theorem 5 is in analyzing these deviations, and showing that the final distortion $\|r_L\|^2/n$ is close to the typical value $\nu^2 e^{-2R}$. We note that such a ‘‘hard-decision’’ successive cancellation approach does not work well for AWGN channel decoding, i.e., the section error rate would decay much slower than exponentially with block length n . One explanation for this is that in channel coding, there is a unique codeword that the decoder has to determine, whereas in lossy compression, the number of good codewords is exponential in n when the rate is larger than the rate-distortion function.

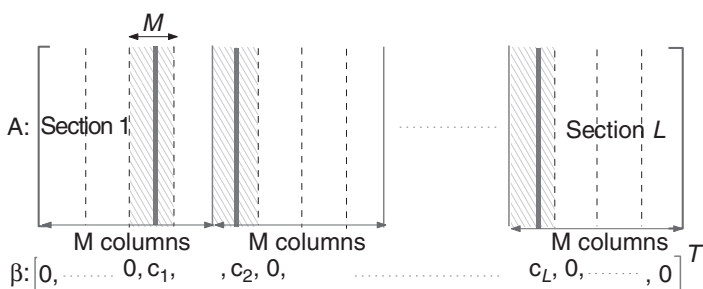
With a Gaussian design matrix, the running time and memory required for the successive cancellation encoder are $O(nML)$. As in channel coding, implementing the compressor with a Hadamard-based design matrix can lead to significant speedup and memory savings.

5. Multi-terminal Source and Channel Coding with SPARCs

Coding schemes that achieve the optimal rate-regions for several multi-terminal source and channel coding models often use the following ingredients: i) rate-optimal point-to-point source and channel codes, and ii) combining or splitting these point-to-point codes via superposition or binning [17].

Superposition with SPARCs: Superposition is easy to implement with SPARCs since the structure of the code itself is motivated by the idea of superposition! Indeed, to construct a superposition codebook with rates R_1 and R_2 , use two design matrices A_1, A_2 with rates R_1, R_2 , each with block length n . Then the concatenated SPARC defined by the matrix $A := [A_1, A_2]$ defines a superposition codebook with sum-rate $R_1 + R_2$. The message vector β is $[\beta_1, \beta_2]^T$, with β_1 and β_2 being the messages corresponding to the rate R_1 and rate R_2 SPARCs, respectively.

Binning with SPARCs [42]: We now describe how to bin a rate R_1 SPARC (with 2^{nR_1} codewords) into 2^{nR} bins, where $R < R_1$. Fix the parameters M, L, n of the design matrix A such that $L \log M = nR_1$.



As shown above, divide each section of A into sub-sections consisting of M' columns each. Then each *bin* is indexed by picking one sub-section from each section. For example, the collection of shaded sub-sections in the figure together forms one bin. The key observation is that each bin is a sub-matrix of A that defines a rate $(R_1 - R)$ SPARC with parameters (n, L, M') . Since we have (M/M') sub-section choices in each of the L sections, the total number of bins is $(M/M')^L$. Choosing M' such that $L \log M' = n(R_1 - R)$, we have 2^{nR} bins as required.

We have divided a higher rate SPARC of rate R_1 into 2^{nR} bins, each of which is a rate $(R_1 - R)$ SPARC. Note that the sub-matrices defining the bins have overlapping sub-sections, just like the SPARC codewords have overlapping columns. It was shown in [42], this superposition and binning constructions described above let us construct rate-optimal SPARCs for a variety of Gaussian multi-terminal models including broadcast channels, multiple-access channels, as well as source/channel coding with decoder/encoder side-information.

6. Open Questions

We conclude with a list of open questions in each of the topics discussed in this survey.

AWGN Channel Coding

- Theoretical guarantees for Hadamard designs: Current analysis techniques for both the AMP decoder and the adaptive successive decoder depend on the Gaussianity of A . Empirically, Hadamard-based SPARCs have very similar error performance to Gaussian ones (and much lower complexity), but there are no existing theoretical bounds.
- Getting closer to C at moderate block lengths: One idea in this direction is to combine power allocation techniques with spatially-coupled design matrices to boost empirical performance at rates close to C .
- Polynomial gap from C : A major open problem is to design a feasible SPARC decoder whose gap from capacity (for a fixed error probability) provably shrinks as $O(\frac{1}{n^a})$ for some $a \in (0, \frac{1}{2})$? With optimal decoding, the analysis in [13] shows that the gap from capacity for SPARCs is close to order $\frac{1}{\log n}$. The current analysis for the feasible decoders proposed so far suggests that the gap from capacity is of order $1/(\log n)^c$, where the constant $c \gtrsim 1$ varies according to the decoder.
- Generalizing the sparse regression construction: An interesting direction is to extend SPARCs to models such as fading channels and MIMO channels. A more general question is to construct efficient codes for other memoryless channels: There has been some recent work in this direction [43].

Lossy Compression

- Smaller gap from $D^*(R)$: Can we design feasible encoders with better compression performance, i.e., whose gap from $D^*(R)$ is smaller than $O(\log \log n / \log n)$? In particular, can we design soft-decision based encoders, e.g., an AMP encoder?

- Bernoulli dictionaries: Can one extend the results for optimal encoding and successive cancellation encoding (which are proved for Gaussian dictionaries) to dictionaries with *i.i.d.* ± 1 entries? For AWGN channels, SPARC ML decoding with *i.i.d.* ± 1 design matrices has been analyzed in [14].
- Finite-alphabet lossy compression: Can one use SPARC-like constructions to compress to finite alphabet sources, e.g., binary sources with Hamming distortion?

Multi-terminal models

- Approaching the Shannon limits with feasible encoding and decoding: The construction in Sec. 5 implements binning by nesting a lower-rate source/channel code inside a higher-rate channel/source code. Since the optimal power allocation for feasible encoding/decoding will depend on the rate, we may not be able to ensure that the SPARC power allocation is simultaneously optimal for both the high-rate and low-rate codes.

An open question is: how to do we design good PA schemes for problems that require binning so that both the high-rate and low-rate codes are close to their Shannon limits, thereby ensuring that the overall rate is also near-optimal? We note that PA is not an issue when we use optimal encoding and decoding, as flat power-allocation is sufficient at all rates.

- Implementing SPARCs at near-optimal rates for basic models with binning (such as Gaussian Wyner-Ziv and ‘writing on dirty paper’) will pave the way to construct low-complexity, rate-optimal codes for a variety of Gaussian multi-terminal models such as multiple descriptions, distributed lossy compression, and relay channels.

Acknowledgements

This survey is based on work done in collaboration with Sanghee Cho, Adam Greig, Antony Joseph, Cynthia Rush, and Tuhin Sarkar. The work was supported in part by the National Science Foundation under Grant CCF-1217023, and by a Marie Curie Career Integration Grant (GA No. 631489) from the European Commission.

References

- [1] C. Berrou and A. Glavieux, “Near optimum error correcting coding and decoding: turbo-codes,” *IEEE Transactions on Communications*, vol. 44, pp. 1261–1271, Oct 1996.
- [2] T. Richardson and R. Urbanke, *Modern Coding Theory*. Cambridge University Press, 2008.
- [3] E. Arıkan, “Channel polarization: A method for constructing capacity-achieving codes for symmetric binary-input memoryless channels,” *IEEE Trans. Inf. Theory*, vol. 55, pp. 3051–3073, July 2009.
- [4] S. Korada and R. Urbanke, “Polar codes are optimal for lossy source coding,” *IEEE Trans. Inf. Theory*, vol. 56, pp. 1751–1768, April 2010.
- [5] S. Kudekar, T. Richardson, and R. L. Urbanke, “Spatially coupled ensembles universally achieve capacity under belief propagation,” *IEEE Trans. Inf. Theory*, vol. 59, pp. 7761–7813, December 2013.
- [6] G. D. Forney and G. Ungerboeck, “Modulation and coding for linear gaussian channels,” *IEEE Transactions on Information Theory*, vol. 44, no. 6, pp. 2384–2415, 1998.
- [7] A. Guillén i Fàbregas, A. Martinez, and G. Caire, *Bit-interleaved coded modulation*. Now Publishers Inc, 2008.
- [8] G. Böcherer, F. Steiner, and P. Schulte, “Bandwidth efficient and rate-matched low-density parity-check coded modulation,” *IEEE Transactions on Communications*, vol. 63, no. 12, pp. 4651–4665, 2015.
- [9] R. Zamir, *Lattice Coding for Signals and Networks: A Structured Coding Approach to Quantization, Modulation, and Multiuser Information Theory*. Cambridge University Press, 2014.
- [10] U. Erez and R. Zamir, “Achieving $1/2 \log(1 + \text{snr})$ on the AWGN channel with lattice encoding and decoding,” *IEEE Trans. Inf. Theory*, vol. 50, no. 10, pp. 2293–2314, 2004.
- [11] N. Sommer, M. Feder, and O. Shalvi, “Low-density lattice codes,” *IEEE Trans. Inf. Theory*, vol. 54, no. 4, pp. 1561–1585, 2008.
- [12] Y. Yan, L. Liu, C. Ling, and X. Wu, “Construction of capacity-achieving lattice codes: Polar lattices,” *arXiv preprint arXiv:1411.0187*, 2014.
- [13] A. Barron and A. Joseph, “Least squares superposition codes of moderate dictionary size are reliable at rates up to capacity,” *IEEE Trans. on Inf. Theory*, vol. 58, pp. 2541–2557, Feb. 2012.
- [14] Y. Takeishi, M. Kawakita, and J. Takeuchi, “Least squares superposition codes with Bernoulli dictionary are still reliable at rates up to capacity,” *IEEE Trans. Inf. Theory*, vol. 60, pp. 2737–2750, May 2014.
- [15] Y. Takeishi and J. Takeuchi, “An improved upper bound on block error probability of least squares superposition codes with unbiased bernoulli dictionary,” in *Proc. IEEE Int. Symp. Inf. Theory*, pp. 1168–1172, 2016.
- [16] T. M. Cover and J. A. Thomas, *Elements of Information Theory*. John Wiley and Sons, 2012.
- [17] A. El Gamal and Y.-H. Kim, *Network Information Theory*. Cambridge University Press, 2011.
- [18] A. Joseph and A. R. Barron, “Fast sparse superposition codes have near exponential error probability for $R < C$,” *IEEE Trans. Inf. Theory*, vol. 60, pp. 919–942, Feb. 2014.
- [19] C. Rush, A. Greig, and R. Venkataramanan, “Capacity-achieving sparse superposition codes via approximate message passing decoding,” *arXiv:1501.05892*, 2015. (Shorter version appeared in ISIT ‘15).
- [20] A. R. Barron and S. Cho, “High-rate sparse superposition codes with iteratively optimal estimates,” in *Proc. IEEE Int. Symp. Inf. Theory*, 2012.

- [21] S. Cho and A. Barron, "Approximate iterative bayes optimal estimates for high-rate sparse superposition codes," in *Sixth Workshop on Information-Theoretic Methods in Science and Engineering*, 2013.
- [22] S. Cho, *High-dimensional regression with random design, including sparse superposition codes*. PhD thesis, Yale University, 2014.
- [23] J. Barbier and F. Krzakala, "Approximate message-passing decoder and capacity-achieving sparse superposition codes," *arXiv:1503.08040*, 2015.
- [24] D. L. Donoho, A. Maleki, and A. Montanari, "Message-passing algorithms for compressed sensing," *Proceedings of the National Academy of Sciences*, vol. 106, no. 45, pp. 18914–18919, 2009.
- [25] A. Montanari, "Graphical models concepts in compressed sensing," in *Compressed Sensing* (Y. C. Eldar and G. Kutyniok, eds.), pp. 394–438, Cambridge University Press, 2012.
- [26] M. Bayati and A. Montanari, "The dynamics of message passing on dense graphs, with applications to compressed sensing," *IEEE Trans. Inf. Theory*, pp. 764–785, 2011.
- [27] M. Bayati and A. Montanari, "The LASSO risk for Gaussian matrices," *IEEE Trans. Inf. Theory*, vol. 58, no. 4, pp. 1997–2017, 2012.
- [28] F. Krzakala, M. Mézard, F. Sausset, Y. Sun, and L. Zdeborová, "Probabilistic reconstruction in compressed sensing: algorithms, phase diagrams, and threshold achieving matrices," *Journal of Statistical Mechanics: Theory and Experiment*, no. 8, 2012.
- [29] S. Rangan, "Generalized approximate message passing for estimation with random linear mixing," in *Proc. IEEE Int. Symp. Inf. Theory*, pp. 2168–2172, 2011.
- [30] D. L. Donoho, A. Javanmard, and A. Montanari, "Information-theoretically optimal compressed sensing via spatial coupling and approximate message passing," *IEEE Trans. Inf. Theory*, pp. 7434–7464, Nov. 2013.
- [31] C. Rush and R. Venkataramanan, "Finite sample analysis of approximate message passing," in *Proc. IEEE Int. Symp. Inf. Theory*, 2016. Full version: <https://arxiv.org/abs/1606.01800>.
- [32] "Coded modulation library." Online: <http://www.iterativesolutions.com/Matlab.htm>.
- [33] J. Barbier, C. Schülke, and F. Krzakala, "Approximate message-passing with spatially coupled structured operators, with applications to compressed sensing and sparse superposition codes," *Journal of Statistical Mechanics: Theory and Experiment*, no. 5, 2015.
- [34] J. Barbier, M. Dia, and N. Macris, "Proof of threshold saturation for spatially coupled sparse superposition codes," in *Proc. IEEE Int. Symp. Inf. Theory*, 2016.
- [35] R. Venkataramanan, A. Joseph, and S. Tatikonda, "Lossy compression via sparse linear regression: Performance under minimum-distance encoding," *IEEE Trans. Inf. Thy*, vol. 60, pp. 3254–3264, June 2014.
- [36] R. Venkataramanan and S. Tatikonda, "The rate-distortion function and error exponent of sparse regression codes with optimal encoding," *arXiv:1401.5272*, 2014. (Shorter version appeared in ISIT '14).
- [37] K. Marton, "Error exponent for source coding with a fidelity criterion," *IEEE Trans. Inf. Theory*, vol. 20, pp. 197–199, Mar 1974.
- [38] S. Ihara and M. Kubo, "Error exponent for coding of memoryless Gaussian sources with a fidelity criterion," *IEICE Trans. Fundamentals*, vol. E83-A, pp. 1891–1897, Oct. 2000.
- [39] A. Coja-Oghlan and L. Zdeborová, "The condensation transition in random hypergraph 2-coloring," in *Proc. 23rd Annual ACM-SIAM Symp. on Discrete Algorithms (SODA)*, pp. 241–250, 2012.
- [40] A. Coja-Oghlan and D. Vilenchik, "Chasing the k-colorability threshold," in *Proc. IEEE 54th Annual Symposium on Foundations of Computer Science (FOCS)*, pp. 380–389, 2013.
- [41] R. Venkataramanan, T. Sarkar, and S. Tatikonda, "Lossy compression via sparse linear regression: Computationally efficient encoding and decoding," *IEEE Trans. Inf. Theory*, vol. 60, pp. 3265–3278, June 2014.
- [42] R. Venkataramanan and S. Tatikonda, "Sparse regression codes for multi-terminal source and channel coding," in *50th Allerton Conf. on Commun., Control, and Computing*, 2012.
- [43] J. Barbier, M. Dia, and N. Macris, "Threshold saturation of spatially coupled sparse superposition codes for all memoryless channels," in *Proc. Inf. Theory Workshop*, 2016.

The Historian's Column

You are a freshly graduated Ph.D. student who performed research under Professor X who is an expert and is interested in area Y and, now, as you are starting your career, you wonder what problems to study and what direction to take. You liked (or, more correctly, you ended up liking) the area Y and you had some fun working in it, but you are not sure that it is a good idea to continue working in it. What should you do?

Well, welcome to the ranks of all those who have agonized over the years about which direction to take their research in. With handfuls of exceptions of people who felt a natural spark that led them to what they ended up passionately loving, everybody else has gone through the purgatory of deciding what to do in their research (let alone more generally in their lives).

More often than not, the decision is made for you by your environment and forces that reside outside your inner mind. Your boss (department chairman or supervisor) tells you that area Z is important or that the emerging area W holds the promise for the Holy Grail or, more typically, major announcements from Funding Agencies declare that area Q will see rivers of money flowing to the research community. Some people are swayed rather easily. Others tend to be skeptical and tend to demure. Bottom line is that you need to decide, one way or another.

I was thinking of that, the other day, when a friend from the "old country" reminded me what was happening in the streets of Athens, Greece, during and immediately after the end of World War II. Supplies of Feta cheese (a staple in the Greek diet) would become available occasionally and then pop-up distribution stations would be set up at street corners where Feta rations would be distributed gratis. As expected, throngs of people would flock to these stations and form long queues to obtain their share. This phenomenon did not last too long but it did give rise to a metaphor used in everyday parlance in Greece. When people flock somewhere in large numbers (to buy "hot" tickets, or to access something new or valuable), the question is asked (often "tongue-in-cheek") whether Feta is being handed out there.

Today, when we go to conferences and meetings that hold sessions on what is perceived as "hot" (or, perhaps, to stay with the times, "cool") topics, we see overflow crowds who eagerly populate these sessions in the hope of obtaining their share of intellectual "Feta". Yes, it is an admission of uncertainty or curiosity or hope, but it is true. There is even another, more sarcastic, metaphor one can use based on the story of that prankster who was walking the streets of Manhattan and would occasionally turn his gaze to the sky, assume an expression of horror, and, sometimes, point his finger up or even let out a cry of bewilderment. Almost everyone around him would also turn their heads up with concern to see what ill omen of doom was causing that reaction, and, of course there was nothing.

Over the years there have been many "new" trends, or areas, that have captured the imagination and interest of our colleagues to the point where veritable waves of activity have followed. There are numerous examples. My favorite is the famous (or infamous) ATM (not the cash dispenser but the "Asynchronous Transfer Mode") from the Internet technology in the late '80's to early '90's. In those days, at

Anthony Ephremides



conferences like the IEEE Infocom, ATM featured prominently in multiple sessions. Funding for ATM research was plentiful. And ardent young researchers would swear that they had seen the future, and it was ATM! By the turn of the century, if one wrote in a job application that ATM was one of the areas of his/her interest, that application would be dead on arrival and quickly meet the trashcan. And, today, most people have forgotten even what ATM stood for.

The IEEE Transactions on Networking used to be a repository for lots of papers (ranging from innovative and influential to banal and incremental) that dealt with the use of queueing theory for modeling networking problems. Until an activist Editor-in-Chief declared that even mentioning of the word "queueing" would be reason enough to return a submitted paper to the authors without review. Such backlash is not uncommon after the pendulum swings too far in a certain direction.

There was also the subject of random access and conflict resolution algorithms. Boy, was it "hot" (or, "cool") in the '80's! Now only a few "cognoscenti" remember what the Capetanakis algorithm was.

Today we are confronted with many new areas that emerge and compete for our attention (and for funding). Some are the likes of cognitive systems, cooperative systems, compressive sensing, big data, cyber-physical systems, and many more. Will they face the fate of ATM? Are they like Feta distribution stations (or, perhaps, nowadays, like Foie Gras distribution centers)? Or are they here to stay, like error-correcting codes, distributed control, multi-user systems, and several others?

Well, let us not forget that the field of Information Theory itself was the object of eulogies multiple times over its history. And let us not forget that some areas go dormant only to reawaken with vigor. A good example is sampling theory. After Nyquist, Landau, and Masry (and scores of others around the middle part of last century) studied how to reconstruct analog signals from samples, there were many years of silence. Until recently, with the emergence of new applications of signal processing, like blind deconvolution, there has been a vigorous resurgence of the area. And, yes, there is a book going to appear soon on the subject of "Aloha"! So, what to do?

As was said in a memorable plenary lecture at the 1986 ISIT in Michigan, "there is nothing, no matter how complicated, which, when viewed the right way, doesn't become even more complicated". How should we sift through the intellectual "particles" that are bombarding us on a daily basis and sort out the golden nuggets from the rubble? There is no easy answer my dear graduate (or colleague). Which brings to mind a parallel pronouncement in the famous Dustin Hoffman movie "The Graduate" (remember the line about "plastics"?). Ideas flow like water in a river bed. And, just like water, they can sink into the gutter, or can yield spectacular waterfalls, or evaporate only to come back down as rain. What counts is to enjoy wading in them or to have an exciting trip by riding the rapids.

Students' Corner

A Perspective on Implicit Gender Bias

Mine Alsan
minealsan@gmail.com

I volunteered to write this column about implicit gender bias after Prof. Goldsmith announced to the Women in Information Theory (WITHITS) mailing list that the IEEE Awards Board accepted her and Prof. Mitesserschmidt's implicit bias write-up. This is great news and hopefully signals positive change in the IEEE's recognition of women's achievements.

After the Student Subcommittee endorsed my suggestion, I started thinking about what message I could convey in such a limited amount of space. I could write about absurd events during my PhD. I shared an office with someone from the department whose silence was interpreted as shyness by his (male) supervisor and as a refusal to talk to women for religious reasons by that supervisor's (female) secretary. You may know that implicit associations are formed by exposure to gender stereotypes but you would be quite surprised to learn to what extent implicit bias affects women's careers. I could also talk about various discussions I've had with female colleagues about affirmative action. You might think that they justifiably hold that women can use all the help they can, given the biases and glass ceilings working against them, but most of the women from my generation are opposed to it, since they believe it would diminish their achievements in the eyes of others.

To expand my horizon, I decided to do a quick Google search. First, I hit headlines about the recent national news on implicit racial bias that most of us must have heard about. Then, I came across an institute which releases yearly reports on implicit bias research. Here are some informative myth-busters from one of them:

- Implicit bias shouldn't be confused with explicit bias;
- it doesn't make us bad people—everyone has implicit biases;
- it goes beyond stereotyping to include un/favorable evaluations toward groups of people;
- it is robust and pervasive.

My search continued. I took a short test on implicit gender bias developed by Harvard researchers¹. I urge you to do it; it takes under 10 minutes. It will be revealing to discover that you might be taking slightly more time—even one second more—to categorize “children” into the “male or family” box and not the “women or career” one and it will bring you closer to understanding how implicit bias controls your brain's automatic responses. The upshot is that even if you believe explicitly that women and men should be equally associated with science, your automatic associations could show that you more readily associate it with men.

Frankly, it has been enlightening for me. Recently, I was “weeping” on the WITHITS mailing list, asking “Have I decided to build my career in a field where most people (which are males) are in fact not so open-minded after all, and have extremely biased mindsets? If many fields like medicine, law, architecture have managed to better adapt to the changing gender dynamics in society, doesn't this tell something about the males dominating the

STEM fields?” After taking the test, I think we might be lagging because of our talent for quickly learning associations, regardless of any scientific basis.

After my web survey, I decided to bring attention to four cases that illustrate how implicit gender bias manifests in the IT society².

- 1) Prof. Jane Osten, a prominent researcher with many career accomplishments, is invited to give a conference talk as a plenary speaker. One of the organizing chairs, Prof. Alfred Eggstein, is about to introduce her and her accomplishments to the audience, as is customary. He begins with the following story: “In the 90's, there was an open problem in Information Theory: How to find a wife?” The audience reacts with clamorous laughter.

I have no objections to humor. In fact, it took me a second to refrain from joining the crowd's reaction. Picture the stereotypical diligent, shy, lonely scientist without much social status and physical or economical attractiveness. His quest for a partner might have seemed as difficult as trying to solve an open problem in IT. But I held back, because once again implicit gender associations were collectively reinforced and I didn't want to contribute to something highly damaging to my own career.

Have you ever heard such details emphasized during a male researcher's introduction? Will we soon hear: after founding a start-up, which raised X-million bitcoins, Prof. Eggstein, a great husband, decided to take a short leave to care for his newborn?

- 2) In another venue, Prof. Osten is invited to address the room. Her introduction mentions her having X children. The audience reacts unanimously with a “wow!”

Why was the audience so surprised? How did we get to the conclusion that having many children and a promising career are mutually exclusive? Why not consider that having children might actually help women build more successful careers?

- 3) Alice is about to obtain her PhD and is looking for postdoc positions. She contacts Prof. Eggstein to discuss opportunities in his laboratory. His first reaction is to ask why Alice wants to do a postdoc. He encourages her to apply for faculty positions, not because she has already a good track record but because he claims that women have jobs ready for them. According to him, since the 90's, US universities decided to hire women but can't find enough to fill faculty positions, so they'll embrace any woman holding a PhD degree.

This might be well-intentioned but should Alice be happy to be told that a job might be waiting just because of her gender? Should she change her mentality and seek to lazily benefit from affirmative action? Should Alice be upset that Prof. Eggstein

¹Project Implicit – <https://implicit.harvard.edu/implicit/takeatest.html>.

²Note that all names in the four cases are made up.

implicitly sent the message that women only make it thanks to affirmative action?

- 4) Alice and Bob are chatting about the challenges of finding faculty positions after graduation. At some point, they start talking about the job search experiences of three of their senior colleagues, Jack, Jane, and James. Being quite competent researchers, all three had applied to the same top university, but only Jane was offered a position. In the ensuing conversation, Bob mentions that Jane had the advantage of being a woman, while Alice counters that Jane had the advantage of having a widely cited publication.

It's interesting that Alice's explanation was based on a comparable measure that clearly distinguished Jane from the other candidates, while Bob's wasn't. Bob was, in fact, implicitly biased because neither of them had information about the hiring process, and couldn't know whether Jane benefited from affirmative action.

The solution is simple: we have to collectively unlearn and replace associations our brains have made throughout our lives. Unfortunately, it seems there are no known effective strategies to quickly reduce implicit bias. On a brighter note, consider this comment from Dr. Nancy Hopkins:

"If you asked me to name the greatest discoveries of the past 50 years, alongside things like the internet and the Higgs particle, I would include the discovery of unconscious biases and the extent to which stereotypes about gender, race, sexual orientation, socioeconomic status, and age deprive people of equal opportunity in the workplace and equal justice in society."

My only advice to those interested in combating implicit gender bias and helping your female colleagues advance their careers is: expect as much from them as you do from their male colleagues—and expect nothing less. Their day will come.

From the Field: IEEE Information Theory Society German Chapter

Since 2003, the German chapter of the information theory society organizes workshops on applied information theory twice a year. The aim of the workshops is to bring together young PhD students presenting their work even in an early stage and to discuss new ideas with experienced scientists. Each workshop is dedicated to a specific topic and includes a tutorial. Prof. Rudolf Mathar and Prof. Anke Schmeink at the RWTH Aachen hosted the first workshop in 2016 on March 16–17. Approximately 50 scientists attended the workshop with the topic "Information Processing: Methods and Technologies". The tutorial "What is Data Science?" by Dr. Ulrich Kerzel (Blue Yonder GmbH) completed the program.

The second workshop in 2016 took place on 25–26. October at the Ruhr University Bochum and was hosted by Prof. Aydin Sezgin. The tutorial on "Robust Interference Management: An Information Theoretic Perspective" was given by Prof. Syed Jafar of the University of California, USA. The workshop's topic was "Emerging Trends in 5G" and covered 13 presentations. Further information

on the workshops are provided by the coordinator Dr. Dirk Wübben and can be found at <http://www.ant.uni-bremen.de/ait/>.

Besides the workshops on applied information theory, the German chapter organizes a biannual international conference. The 11th International ITG Conference on Systems, Communications and Coding (SCC) will take place on February 6–9, 2017 in Hamburg. We set up an interesting program including tutorials presented by Robert Heath and Gianluigi Livi. Moreover, we will have prestigious invited speakers like Fumiyuki Adachi, Christian Bettstetter, Joachim Hagenauer, Frank R. Kschischang, Gernot Kubin, Amos Lapidoth, Erik G. Larsson, Sergei K. Turitsyn, Moe Z. Win, Peter J. Winzer, Henk Wymeersch, and Raymond W. Yeung. Interested scientists are warmly invited to attend the conference and can find detailed information at www.scc2017.net.

*Volker Kühn
Gerhard Bauch
Dirk Wübben*

Shannon Centenary



U-M Shannon Centennial Symposium Celebrates the Father of Information Theory

*Alfred Hero
University of Michigan*

Researchers from around the world gathered at the University of Michigan in Ann Arbor to celebrate the 100th birthday of alumnus Claude E. Shannon (BSE EE/Eng Math '36, ScD hon.' 61) at the Shannon Centennial Symposium on September 16, 2016. The event was co-organized by Al Hero, Hye Won Chung, Dave Neuhoff, and Sandeep Pradhan.

The symposium welcomed more than 300 registered participants from around the nation, and included a poster session and plenary lectures by Abbas El Gamal (Stanford University), Emmanuel

Candes (Stanford University), Michelle Effros (CalTech), and Robert Calderbank (Duke University). The lectures, which can be accessed from the link below, were inspired by Shannon's foundational work in computing, communication and information theory.

On display was an exhibit showing Shannon's Michigan connections, including his hand-written college application from 1932, his diploma application, and the page from his 1936 Commencement program where his name appeared under both Mathematics and Electrical Engineering.



Top: Co-organizers and invited lecturers in the lobby of the Symposium venue, the Rackham building at the University of Michigan. **From left to right:** Sandeep Pradhan, Alfred Hero, Michelle Effros, Abbas El Gamal, Hye Won Chung, Emmanuel Candes, David Neuhoff, Robert Calderbank. **Left:** Attendees enjoying a sunny coffee break on the balcony of the Rackham building. **Right:** A poster presentation at the Symposium poster session.

Attendees could also view the video tribute to Claude Shannon prepared by the IEEE Information Theory Society, as well as ten posters showing the impact of Shannon's work, prepared by individual members of the IT Society.

The University of Michigan Shannon Centennial Symposium was sponsored by the University of Michigan College of Engineering, the University of Michigan Institute for Data Science, the University of Michigan Department of Electrical Engineering and Computer Science (Division of Electrical and Computer Engineering), and the IEEE Information Theory Society, The

celebration will continue at Michigan throughout the year with a biweekly Shannon Centennial Lecture Series, featuring invited speakers: Robert M. Gray, Rebecca Willett, Bruce Hajek, Frank Kschischang, Prakash Narayan, Yuejie Chi, Daniel Costello, and Elza Erkip.

More Information: Shannon Centennial Lecture Series: midas.umich.edu/shannon. Links to the talks, photos, and Information Theory Society posters of Shannon's impact can be found on the University of Michigan Shannon Centennial webpage : eecs.umich.edu/n/shannon

Shannon stamp in Macedonia

*Ninoslav Marina
University of Information Science and Technology
Ohrid, Republic of Macedonia*

In July 2016, Macedonian Post issued a commemorative stamp with Claude E. Shannon to mark the 100 years anniversary of his birth. The idea came in February 2015 when Sergio Verdú asked me if we could try to issue a Macedonian postal stamp of Shannon. During the following months I sent couple of letters and contacted several offices to finally schedule a meeting with the Macedonian Post Deputy Director General Goce Bobolinski. I met him in July 2015 and he immediately replied positively saying that the Macedonian Post has a line of stamps to mark historical persons or events and the Shannon stamp will be issued as a philatelist limited edition. He projected the whole process to be finished by mid 2016. In



January 2016, my colleague Yane Bakreski and myself had proposed a design that was sent to the responsible person at Macedonian Post. After completing the internal procedure, the stamp came out of print on July 12, 2016 during the ISIT in Barcelona. Initially, 7000 stamps were printed, however more may be printed if necessary. I promoted the stamp officially during the speech at the opening ceremony of the academic year 2016/17 at the University of Information Science and Technology "St. Paul the Apostle" in Ohrid, Republic of Macedonia, where I currently hold the position of a Rector. I like to use this opportunity to thank everyone who was involved, especially Mr. Bobolinski, for his support during the whole process.

Future Events:

IEEE Antennas and Propagation Chapter, IEEE Kerala Section, India

IEEE Antennas and Propagation Chapter, IEEE Kerala Section, India is going to host a technical symposium on "Revisiting Claude Shannon's Contribution" during December 13-14 '2016 in Thiruvananthapuram, Kerala, India. The program is technically and financially sponsored by Shannon Centennial Committee, IEEE

Information Theory Society and consists of various events which include mass awareness on Shannon's contribution through public lectures by renowned speakers, a poster competition amongst engineering students and technical lectures. Around 100 engineering students and faculty members from various parts of Kerala are expected to attend the event. Dr. Chinmoy Saha, Dr. CK Vineeth and Dr. B.S. Manoj, faculty members, Indian Institute of Space Science and Technology are the key organizers for this event.

IEEE ITSOC Chicago Chapter Shannon Centennial Event

by *Natasha Devroye*

The IEEE ITSOC Chicago Chapter Shannon Centennial Event was a one-day workshop held on September 23, 2016 at Motorola Mobility—a Lenovo company’s 18th floor conference venue and roof in downtown Chicago’s landmark Merchandise Mart. Open and free to all, about 25 academics, 25 industrial professionals (many but not all from Motorola Mobility—a Lenovo company), and 25 students attended to celebrate Shannon’s life and contributions.

After welcoming remarks by Natasha Devroye, the audience was treated to a keynote on Shannon’s Legacy: Coding Theory from 1948 to 2016 by Bettex Chair Professor Emeritus at the University of Notre dame, Daniel J. Costello. One of the few attendees to have met Shannon in person, he commented on his graciousness and interest in the stock market (or was it gambling?) and led us through the Seven Days of Creation of coding theory. Dan did some extra research for this talk and polled various US politicians on their favorite codes, with some very insightful responses <http://www.ece.iit.edu/~salim/Costello.pdf>

We are currently thriving in the Eighth exciting Day of coding theory—thanks for the excellent keynote Dan.

Robert Love, a Fellow of Technical Staff at Motorola Mobility who has worked in the wireless arena for over 25 years, offered a clear, thoughtful vision of 5G and beyond Next Generation Wireless Networks and the new challenges they pose. To understand 5G once and for all, have a look at his informative slides <http://www.ece.iit.edu/~salim/Love.pdf>

The remainder of the technical talks were given by Chicago-area academics in information theory.

Natasha Devroye talked about the Gaussian interference channel and the surprisingly good performance of the simple scheme of treating interference as noise when using properly chosen discrete inputs. Randall Berry talked about information and games, and the impact information theory can have on game theory and vice versa. Daniela Tuninetti presented a variation of the index coding

problem—pliable index coding and caching in which a user in an index coding setting is happy if they can decode at least one new message. Salim El Rouayheb talked about the tricky task of retrieving private information from coded data—i.e. ensuring that a user can retrieve records in a database or files in a distributed storage system while revealing no information on which record or file is being retrieved. Hulya Seferoglu spoke about having nodes in networks cooperate for energy, computational, and throughput efficiency. Slides of all talks are available at <http://www.ece.iit.edu/~salim/itsoc.html>

Lunch was enjoyed on the roof of the Merchandise Mart, with a beautiful view of the Chicago river and skyline. Right afterwards, Dongning Guo presented a review of some of the past successes of information theory and presented his observations of current research trends in the field. The day was concluded by a video and live demo of Motorola Mobility’s new Moto Z MotoMods Developer Kit, see <https://www.youtube.com/watch?v=HLSLRzmcXGM>

This event was the first of its kind in the Chicago-land area and appreciated by all—it brought together academia, industry and students in a beautiful and central venue to discuss information theory and its impact on other areas. It succeeded in connecting academia and industry in celebration of Shannon. A repeat of this event was welcomed by all, and we thank all involved for making it happen: the event was jointly organized by the IEEE ITSOC Chicago Chapter (currently chaired by Natasha Devroye) and Motorola’s Mohammed Abdul-Gaffoor and Katherine Coles. The event was co-sponsored by the University of Illinois at Chicago, Northwestern University, the Illinois Institute of Technology, and the Information Theory Society. Details may be found at <http://www.ece.iit.edu/~salim/itsoc.html> Thank you to all!

Image caption: a subset (taken at the end of the day) of the attendees at the IEEE ITSOC Chicago Chapter’s Shannon Centennial Workshop on September 23, 2016 at Motorola Mobility—a Lenovo company—’s downtown location.



2016 IEEE International Symposium on Information Theory

*Universitat Pompeu Fabra, Barcelona, Spain, 10–15 July 2016.
By Albert Guillén i Fàbregas, Alfonso Martínez and Sergio Verdú*

Held in Spain for the first time, the 2016 ISIT took place at the Ciutadella Campus of the Universitat Pompeu Fabra in Barcelona on July 10–15, 2016

There were 891 participants, including 290 students, 44 of which volunteered to help at the sessions. There were 1037 submissions and 618 technical papers were presented. 96 students received financial aid in the form of partial travel support to present their papers. For the first time in the history of ISIT, published papers were made available online prior to and during the conference, and were distributed on a USB stick. The conference app allowed to link with the papers as well as containing all the relevant program information.

Five conference tutorials held on Sunday drew a total of 351 delegates. The presenters were A. Ozgur, S. Ulukus and A. Yener, “Energy Harvesting and Remotely Powered Wireless Networks”; Jayadev Acharya, Alon Orlitsky and Ananda Theertha Suresh, “Theoretical Elements of Data Science”; A. Barron and R. Venkataramanan, “Sparse Regression Codes”; M. Wilde, “Quantum Information Theory”; A. Barg and I. Tamo, “Theory and Practice of Codes with Locality”.

On Sunday evening, a traditional welcome cocktail was held at the Marqués de Comillas Hall of the Museu Marítim. For five days, except on Wednesday afternoon, nine parallel tracks were scheduled with two morning sessions and two afternoon sessions, each consisting of four 20 minutes talks. Talks covered the whole spectrum of Information Theory. A recent results session took place on Wednesday morning where 26 posters were presented.

Each day commenced with a plenary lecture at the Roger de Llúria Central Courtyard:

- Monday: Prof. Elza Erkip from New York University (USA) lectured on “From 3T to 5G: Theory and Practice of Cooperation in Wireless Networks”;
- Tuesday: Prof. Daniel Spielman from Yale University (USA) lectured on “The Laplacian Matrices of Graphs”;
- Thursday: Prof. Giorgio Parisi from the University of Rome I, La Sapienza (Italy) lectured on “The SAT-UNSAT Transition for Random Satisfiability Problems in the Case of Continuous Variables”;
- Friday: Prof. Alexander Barg from the University of Maryland (USA), lectured on “Codes, Metrics and Applications”.

The 2016 Shannon Lecture was given by Prof. Alexander Holevo from the Steklov Mathematical Institute (Russia) on Wednesday morning, with the title “The Classical Capacity of a Quantum Channel”.

This year’s Awards of the Information Theory Society were presented on Tuesday during a lunch ceremony hosted by the Society president, Prof. Alon Orlitsky.



The banquet dinner was held at the Oval Hall of the majestic National Palace in Montjuïc which currently hosts the Museu Nacional d’Art de Catalunya. After dinner, the recipient of the 2017 Shannon Award was announced: Prof. David Tse, who will give his Shannon Lecture at the 2017 ISIT in Aachen. At the conclusion of the banquet, Profs. Rudolf Mathar and Gerhard Kramer welcomed everyone to participate in the next ISIT that will be held in Aachen, Germany, 25–30 June 2017.

During the conference, a number of events were held in parallel to the technical sessions. The WITHITS event “The Samoan Circle” was held on Monday at lunchtime. This year’s Outreach Committee event was entitled “All the mentoring you need in 60 minutes”, and was held on Monday evening. The event featured 9 round tables on “Industry or Academia” (E. Soljanin, C. Tian), “Effective Teaching Techniques” (E. Telatar, S. Verdú), “Funding your Research” (R. Brown from NSF, N. Sebastián Gallés from the ERC), “Achieving Work-Life Balance” (N. Kiyavash, A. Sarwate), “Time Management” (H. Böelcke, F. Kschischang), “Branching into Allied Fields” (A. Dimakis, O. Milenkovic), “Navigating the Academic Job Market” (G. Durisi and Y. Polyanskiy), “Navigating the Tenure-Track” (N. Devroye, A. Khisti), and “The Postdoc Experience” (Y. Altug, A. El Gamal). The “Meet the Shannon Awardee” event was held on Thursday lunchtime.

A number of innovations were introduced this year, ranging from free ice-cream to the use of an LED screen to display the support material of the plenary speakers and award ceremony as well as videos during the coffee breaks. The technical program also experienced some changes. No semiplenary sessions were held; instead, the Jack Keil Wolf Student Award nominees were scheduled in the same session and were assigned a substantially larger room. The technical program booklet underwent a significant format change, bringing it closer to its entropy. Last but not least, the registration fees were as low as those in 2006 in Seattle. This was achieved with intense negotiation efforts with all confernee providers, including the university itself, catering and audiovisual companies as well as the PCO. Even credit card fees were brought down from 2% to 0.4%. We hope that this cost reduction will inspire the organizers of upcoming ISITs and ITWs to make every effort to reduce costs without sacrificing in conference quality.

IHP Program on the “Nexus of Information and Computation Theories”

Bobak Nazer

The Institut Henri Poincaré (IHP) is a research institute dedicated to mathematics and theoretical physics. It was founded by Émile Borel and George Birkhoff, and is currently directed by Cédric Villani. Each quarter, IHP hosts a thematic program that brings together researchers from a particular discipline to foster the exchange of ideas. For the Winter 2016 quarter, IHP hosted a program on the “Nexus of Information and Computation Theories,” which sought to consider questions at the interface of information theory and theoretical computer science.

This program was coorganized by Aslan Tchamkerten (Télécom Paristech) and Bobak Nazer (Boston University) from the information theory community as well as Mark Braverman (Princeton University) and Anup Rao (University of Washington) from the theoretical computer science community. To the best of our understanding, this was the first time that IHP had ventured into the “engineering” disciplines for a thematic quarter (and just in time for the Shannon Centennial).

The program began with a tutorial week at the Centre International de Rencontres Mathématiques (CIRM) in Marseille, France. We were very fortunate to have four great speakers, who tailored their talks to provide background for the major themes of the program. The four tutorials were

- 1) Concentration of Measure, Sudeep Kamath (Princeton)
- 2) Algorithmic Aspects of Inference, Ankur Moitra (MIT)
- 3) Communication Complexity and Information Complexity, Anup Rao (University of Washington)
- 4) Privacy and Security via Randomized Methods, Guy Rothblum (Samsung Research America) and all talks are available through <http://csnexus.info>. The basic format was similar to that of an Information Theory School, with time allotted for student poster presentations and a group hike. One innovation is that we split each tutorial into four onehour slots across four days, in order to give students a chance to absorb the material.

After the tutorial week, the participants travelled north to Paris to IHP for the remainder of the program, which focused on four primary themes, each spanning two weeks. The themes were

- 1) Distributed Computation and Communication, organized by Péter Gács (Boston University), János Körner (Sapienza University of Rome), and Leonard Schulman (Caltech).
- 2) Fundamental Inequalities and Lower Bounds, organized by Kasper Green Larsen (Aarhus University), Babak Hassibi (Caltech), Iordanis Kerenidis (University Paris Diderot 7), and Raymond Yeung (Chinese University of Hong Kong).

- 3) Inference Problems, organized by Amit Chakrabarti (Dartmouth College), Andrew McGregor (University of Massachusetts, Amherst), Henry Pfister (Duke University), Devavrat Shah (MIT), and David Woodruff (IBM).
- 4) Secrecy and Privacy, organized by Prakash Narayan (University of Maryland), Aaron Roth (University of Pennsylvania), Anand Sarwate (Rutgers University), Vinod Vaikuntanathan (MIT), and Salil Vadhan (Harvard University).

Each theme was a mix of halfday, tutorialstyle talks and onehour talks, with plenty of time left over for discussions at the chalkboard. Thanks to the sponsorship of the Information Theory Society, we were able videotape nearly 200 talks and put them on YouTube (see <http://csnexus.info> for links). We are very grateful to all of the organizers for putting together engaging programs and to all of the speakers for giving great talks.

In between the second and third theme, we organized a week-long workshop that aimed to go beyond the four major themes described above, and to foster discussion and interaction between the theoretical computer science and information theory communities. There were twentyfour great talks, and all of the abstracts and videos can be found at our website.

We would like to thank all of our sponsors, which included the Centre National de la Recherche Scientifique (CNRS), the University Pierre et Marie Curie (UPMC), the National Science Foundation, Google, Huawei, and the Information Theory Society. Their financial support made it possible for us to provide travel support and post videos of the talks online. In particular, thanks to the CNRS and UPMC, we were pleased to be able to host the following longterm research visitors: Sidharth Jaggi, Soren Riis, Shun Watanabe, Christino Tamon, Himanshu Tyagi, Arkadev Chattopadhyay, Bobak Nazer, Anup Rao, Janos Körner, Grigori Kabatianski, Giacomo Como, and Olgica Milenkovic.

Finally, we are grateful to the IHP administrative staff’s efforts in making the trimester a resounding success. They kept track of every detail, big and small, and helped us wherever needed. In particular, we would like to express our heartfelt appreciation to Sylvie Lhermitte, Delphine Lépissier, and Nitdavanh Sritanakoul for their daytoday efforts in keeping the program running, and the kind and gracious help that they provided to all of our visitors.

In closing, we found IHP (and Paris) to be a stimulating environment for a longterm workshop, and we encourage other IT Society members to consider this as a potential venue for similar programs.

2016 IEEE IT Society Summer School. Indian Institute of Science

This is a report the 2016 IEEE IT Society Summer School held at the Indian Institute of Science, Bangalore, India.

Attendees of the 2016 Indian Summer School held at the Indian Institute of Science, Bangalore.

The 2016 Joint Telematics Group/IEEE Information Theory Society Summer School on Signal Processing, Communications and Networks was held at the Indian Institute of Science (IISc), Bangalore, during June 27–July 01, 2016.

The Summer School series started in 2009 as an initiative of the Joint Telematics Group (JTG). It has been covering contemporary research topics in signal processing, communications, information theory, and networks and has been mainly aimed at students and young researchers from all over India. While the Schools have been held annually since 2009, IEEE Information Theory Society's involvement as a financial and technical co-sponsor began in 2014.

This year, we made a departure from previous summer school formats. In the past, the school comprised of two short courses, each given by a leading expert on some topic within the broad realm of communications, signal processing, information theory and networks. It would span four days. This year, we had three courses, each of eight hours of lecture. The duration of the entire school was five days.

The three short courses comprising the 2016 Summer School were taught by B. V. Rao, Adjunct Professor, Chennai Mathematical Institute, Chennai, India, Upamanyu Madhow, Professor, University of California, Santa Barbara, USA, and Erdal Arıkan, Professor, Bilkent University, Ankara, Turkey. B. V. Rao's lectures were on concentration inequalities,

Upamanyu Madhow lectured on millimeter wave communication networks, and Erdal Arıkan spoke about Polar Coding.

B. V. Rao started with an overview of fundamental inequalities in probability including those by Chebyshev, Cramer, Chernoff, Hoeffding, Azuma and McDiarmid. He discussed the connections with the Johnson- Lindenstrauss lemma, and went on to discuss the Efron-Stein lemma, and its applications in graph theory, the VC theory, etc. Also discussed were the Curie-Weiss lemma, log-Sobolev inequalities, Talagrand's inequalities and their application to problems like the stochastic traveling salesman problem. The lectures concluded with a discussion of isoperimetric inequalities and their connection to Talagrand's inequalities.

Upamanyu Madhow began with an introduction to basic link-budget calculations involved in determining the feasibility of millimeter-wave communications and showed that the research domain is interesting with challenging questions and the mmWave technology a realizable one. He presented recent theory and algorithms



developed for large antenna arrays including compressive estimation and super-resolution (in particular, the newtonized orthogonal matching pursuit algorithm). A highlight of the discussion was the review of the Ziv-Zakai bound and related estimation-theoretic fundamental limits. He presented the key ideas involved in developing networks when one can have highly directional links, both for mesh networks and picocells. Then, he discussed important signal processing issues that need to be tackled for high bandwidth communication, including the challenges in using 1-bit ADCs (or those with a small number of bits). He also presented results from data collected over a 1km^2 area in Manhattan, which experimentally demonstrated that mmWave can potentially offer 1000x the data throughput when compared with LTE. The lectures concluded with a presentation of recent advances in short-range mmWave radar applications and a discussion on various open issues in the area.

Erdal Arikan started with a gentle introduction to the basic ideas in information theory such as the entropy, mutual information, discrete memoryless channels and the channel coding theorem. Then he discussed the fundamental idea behind channel polarization, namely channel combining and splitting, the conservation of capacity by such an operation. He then discussed about low complexity polarization, showed its recursive extension and presented the main polarization theorem from his 2007 paper. He discussed the encoding and decoding complexity in detail and presented several examples. Then, he discussed the performance of polar coding and compared it with the state-of-the-art codes. He presented different options for decoding including maximum likelihood, successive cancellation, belief propagation, list decoding and sphere decoding, and discussed their performance-complexity tradeoff. He also discussed practical aspects: implementation

performance measured in terms of chip area, throughput, energy efficiency and hardware efficiency. He concluded his lectures by giving an in-depth review of polar coding for band-limited channels and their future applications including 60 GHz wireless, optical access networks and 5G ultra-reliable low latency communications, machine communications at Gb/s throughput.

The lectures were very well received by the audience comprising students and faculty from various Indian engineering colleges and institutes, including the IITs, the Tata Institute of Fundamental Research (TIFR) and IISc, as well as researchers from the Defense Research Development Organisation (DRDO) in India. The number of registrations were limited by the seating capacity (120) of the venue, and so we had to close registrations quite early. Testimony to the quality of the lectures is the fact that a large majority of the attendees sat through the entire five day program. After the conclusion of the program, Erdal offered a special encore lecture to about 20 faculty and students on the finer details of some of the proofs.

Generous funding from the IEEE Information Theory Society made it possible for us to support the local accommodation of students coming from outside Bangalore. We would like to take this opportunity to thank the IT Society for its support.

Further information about the Summer School, lecture notes, and video recordings of all the lectures are available on the school's website: <http://www.ece.iisc.ernet.in/~jtg/2016/>

The 2017 JTG / IEEE IT Society Summer School will be held at the Indian Institute of Technology Bombay, Mumbai, India during the summer of 2017.

Seminar on Information—and Communication Theory on the Occasion of the Eightieth Birthday of Piet Schalkwijk

Han Vinck

Three major events stimulated the development of Information theory in the Netherlands: the 1970 IEEE Information Theory (ISIT) symposium organized by Louis Stumpers in Noordwijk; the appointment of Piet Schalkwijk as Professor at the Technical University of Eindhoven and the foundation of the Benelux community for Information Theory (WIC). In the year of the 100th birthday of Claude Shannon, the "father of the Information Theory", the 80th birthday of Piet Schalkwijk was celebrated with a scientific day filled with lectures by his former students highlighting the research results obtained by him, his students and colleagues. Schalkwijk is known for his research on feedback, especially the Schalk-



wijk-Kailath result for the Gaussian channel with feedback and the coding schemes for the two-way channel. About 50 former students and colleagues attended the ceremony on November 16, at the Technical University of Eindhoven, the Netherlands. Lectures were given by Han Vinck, Thijs Veugen, Stan Baggen, Frans Willems, Ludo Tollhuizen, Ben Smeets, Peter de With, Andries Hekstra and Kees Immink. Topics included: Feedback schemes; Two way channels; Source coding; constrained codes; big data and highly appreciated personal notes and anecdotes. After the lectures a reception and dinner concluded the very successful day. More information can be obtained from Han Vinck: han.vinck@uni-due.de.

IEEE Information Theory Society Board of Governors Meeting

Location: Universitat Pompeu Fabra, Barcelona, Spain

Date: 10 Jul 2016

Time: The meeting convened at 1:00 pm CEST (GMT+2); the meeting adjourned 6:30pm CEST.

Meeting Chair: Alon Orlitsky

Minutes taken by: Stark Draper

Meeting Attendees: Jeff Andrews, Andrew Barron, Matthieu Bloch, Helmut Bölcskei, Stark Draper, Michelle Effros, Elza Erkip, Abbas El Gamal, Frank Kschischang, Alon Orlitsky, Vincent Poor, Rüdiger Urbanke, Urbashi Mitra, Pierre Moulin, Krishna Narayanan, Anand Sarwate, Emina Soljanin, Daniela Tuninetti, Alexander Vardy, Emanuele Viterbo, Aylin Yener, Wei Yu

Guests: Alex Dimakis, Gerhard Kramer, Matt LaFleur, José Moura

Motion: Approve agenda. Passed unanimously.

1) **President's Report:** President Alon Orlitsky presented the President's report. Alon reported to the Information Theory Society (ITSoc) Board of Governors (BoG) that the Society's finances are in good shape. The 2016 surplus is projected to be USD \$66k. Revenues have declined slightly over the past few years. One factor is a drop in the numbers of clicks on Xplore, a second is a reduction in the number of subscriptions and memberships. Alon discussed research trends in core areas of information theory as well as related areas of research. He reflected on challenges and opportunities facing ITSoc and its members, and how the Society can respond and foster opportunities for its members. Alon designed the agenda to reserve one hour at end of the BoG meeting to discuss such issues.

2) **TAB Vice President (José Moura), first presentation:** Vice President of the Technical Activities Board (TAB) of the IEEE, José Moura (a professor at Carnegie Mellon University), next presented to the BoG. José started by summarizing some details of the IEEE: worldwide organization, membership in ~160 countries, organizes ~1600 conference per year, plays an important role in standardization efforts (e.g., IEEE 802.11, Zigbee), and a budget of ~\$500m about 80% of which is derived from TAB activities. TAB strategic goals for 2016 focus on education and building communities. He next discussed the finances of the IEEE. He noted that since 2011 expenses have surpassed revenues with deficits having been financed from investments. The IEEE budget is currently not projected to get into balance until 2018. José noted that while overall revenue to IEEE has increased, the amount of that revenue that the IEEE has distributed back to the societies to help finance their activities has been kept roughly constant.

3) **Treasurer's Report:** Treasurer Daniela Tuninetti next presented her report on the state of the Society's finances. Daniela presented the actuals of the ITSoc budget from 2015 (the actuals for each year typically firm up in March/April of the following year, by which point most conferences have closed their books), the state of the 2016 budget, and the budget for 2017.

Regarding the budget actuals for 2015, according to the 'society roll up' document, 58% of ITSoc revenue came from publications and 40% from conferences. Respectively, these two major

items accounted for 51% and 37% of the expenses. The Society realized an operational net in 2015, which may be spent in 2016 for 'New Initiatives' as part of the "50% rule"; some of this has been allocated already at the previous BoG meeting to support Shannon Day events worldwide. Other initiatives could be supported; Daniela solicited everyone for suggestions.

Daniela then reviewed the 2016 budget. The Society is on track, but is currently projected to have a reduction in net due to a revenue reduction forecast in publications.

Next Daniela reviewed the 2017 budget. The initial budget from IEEE aimed for a \$170k net, but for various reasons, in part because there will be only one ITW in 2017 (rather than two), the current projection is \$6k net. That revised budget is currently being reviewed by IEEE. In 2017 the Society has the possibility to include \$140k for 'New Initiatives' as part of the "3% rule"; this budget item is being reviewed by the TAB and, if approved, it may be included as part of the 2017 budget. Daniela solicited everyone to provide ideas, for and beyond continuation of the broad outreach of the Shannon centennial.

Daniela reviewed revenue lines: periodicals, conferences, and membership. In terms of periodicals the 'click' count from IEEE Xplore and the 'content' figure are down; the declining click count is perhaps due, in part, to posting on and downloading papers from Arxiv. Regarding conferences: the major schools are no longer classified as 'new initiatives' but rather are now part of the regular budget. This means that a sustainable source of funding to subsidize schools must be identified, perhaps from conference revenue.

4) **Nominations and Appointments (N&A) Committee:** N&A Committee Chair Abbas El Gamal presented the list of BoG candidates for 2017-19.

Motion: To approve the list. The motion passed unanimously.

Abbas next presented an amendment to the bylaws concerning the editorship of the Transactions. In particular, and as was proposed, discussed, and approved by the BoG at earlier board meeting, a new position of Transactions Executive Editor has been created. The last step is to consider and approve a modification of the necessary bylaws. The modified portion of the bylaws is provided in its entirety below. As the bylaw modification had been discussed at previous board meetings, there was only a small amount of discussion at this meeting, mostly describing the proposed "convolutional" structure of the EiC(s) and a comparison and contrast to what is done in other societies.

Article V. Standing Committees

Section 7. The Publications Committee shall consist of the Society Transactions Editor-in-Chief who serves as chairperson, the Transactions Executive Editor, the Associate Editors of the Society Transactions, the Publications Editors, and the Newsletter Editor. The President, First Vice President and Second Vice President of the Society are ex-officio members of the Committee. The Committee shall generate

yearly nominations for the Information Theory Society Paper Award, as per Article VII, Section 3, oversee the solicitation and review of papers for publication, and shall edit, prepare and publish the Transactions, Special Issues, Monographs, and Newsletter as directed by the Board, with the assistance of the IEEE Editorial Office. The Committee shall recommend changes in publication policy to the Board.

The terms of office of the Transactions Editor-in-Chief and the Transactions Executive Editor shall be eighteen months. At the end of a term of office, the Transactions Executive Editor shall assume the office of Transactions Editor-in-Chief, and a new Transactions Executive Editor shall be nominated by the Nominations and Appointments Committee and shall be appointed by the Board. The outgoing Transactions Editor-in-Chief is not eligible for immediate re-appointment as Transactions Executive Editor. Both the Transactions Editor-in-Chief and the Transactions Executive Editor shall be voting members of the Board.

Associate Editors are appointed by the Transactions Editor-in-Chief subject to approval by the Board. The Newsletter Editor shall be appointed by the Board, upon nomination by the Society President. The Senior Past President of the Society shall serve as Vice President of Publications.

Motion: To approve the change in bylaws. The motion passed unanimously.

Abbas presented a slate of candidates for officer positions on the BoG.

Motion: To nominate Alex Vardy as second vice-president. The motion passed unanimously. Voting will be conducted online.

Motion: To nominate Emina Soljanin as second vice-president. The motion passed unanimously. Voting will be conducted online.

There were no further nominations for the position of second vice-president.

Motion: To nominate Elza Erkip as first vice-president. The motion passed unanimously. Voting will be conducted online.

Motion: To nominate Rüdiger Urbanke as president. The motion passed unanimously. Voting will be conducted online.

- 5) **Report of the Awards Committee:** Prior to the BoG meeting the Awards Committee submitted its report reviewing candidate papers for the Information Theory Paper Award. The full committee consisted of Alexei Ashikhmin, Elza Erkip, Steven Hanley, Andrea Montanari, Chandra Nair, Yingbin Liang, Ertem Tuncel, Rüdiger Urbanke, Wei Yu, and Tsachy Weissman. Seven papers were considered for the award. The set was narrowed through multiple rounds of discussion. Committee members Ashikhmin and Nair did not participate in the decision process due to conflicts of interest. Committee member Yu joined only in later rounds after conflicts in early rounds had resolved. The Awards Committee recommended that the 2016 award be given to two papers on unrelated topics (in random order): (i) "The Capacity Region of the Two-Receiver Gaussian Vector Broadcast Channel With Private and Common Messages," Yanlin Geng and Chandra Nair, *IEEE Trans. on Information Theory*, April 2014 and (ii)

"Fundamental Limits of Caching," Mohammad Ali Maddah-Ali and Urs Niesen, *IEEE Trans. on Information Theory*, May 2014.

Motion: To accept the Committee report. There was a discussion of the recommendation to give the award to two papers. The paper award has most often been given to a single paper. On seven previous occasions it had been awarded to a pair of papers on closely related topics. Only once before, in 1973, was it awarded to two papers on unrelated topics. There was a variety of opinions on the BoG regarding the recommendation to give the award to two papers on unrelated topics. A motion was made to defer the acceptance of the report to provide the BoG more time to consider the recommendation.

Motion: To table (suspend consideration of) the motion to accept the report with the stipulation that a one-month deadline would be set to decide whether or not to accept the report. The motion was seconded. There were 3 votes in favor of the motion, the majority of the BoG was opposed. The motion failed.

The original motion was then voted on. The BoG was unanimous in its acceptance of the Award Committee's report.

Further discussion of the papers and of the recommendation to give the 2016 award to two papers on unrelated topics then ensued. There was a discussion of the instructions the BoG provides to the Awards Committee, including the two-year time-window of eligibility. The discussion is to be continued online.

Motion: To give the award to the two papers recommended by the Awards Committee. Voting was as follows: 12 BoG member voted in favor of the motion, 2 voted to oppose, 6 BoG members abstained. The motion passed.

- 6) **Membership Committee:** Membership Committee Chair Elza Erkip presented the Committee's report. Congratulations was given to Helmut Bölcskei, the 2016 Padovani Lecturer, and also to the Benelux Chapter of the Information Theory Society which was named Chapter of Year. Elza then reviewed the Distinguished Lecturer program and initiatives to increase program activity. Elza reviewed the student subcommittee and outreach committee activities. A new mentoring program event will be held at ISIT 2016: there will be nine round-table discussions on career-related topics led by experienced mentors. Elza then discussed Women in Information Theory (WITHITS) activities. There will be a WITHITS lunch event at ISIT 2016. Finally Elza discussed some possible changes to the structure of the Membership Committee with recommendations to come at the October BoG meeting.
- 7) **Conference Committee:** Conference Committee Chair Emanuele Viterbo reviewed the status of upcoming IT symposia. For the 2017 Aachen and 2019 Paris symposia, the budgets are in the works. The ISIT 2018 Vail budget is in order with an expected registration of \$790 (advanced price for IEEE + ITSoc members). There will be BoG votes on all three budgets which will be conducted by email in the next few weeks. Budgets for the 2015 ITWs (Jerusalem and Jeju Island) have both closed.

Motion: To approve co-sponsorship of the 9th Int. Symp. on Turbo Codes 2016. The motion passed unanimously.

Motion: To approve co-sponsorship of the 2017 CISS. The motion passed unanimously.

Next, bids for ISIT 2020 were discussed. Discussion of these bids was chaired by Elza Erkip due to Emanuele having a conflict of interest.

The proposal to hold ISIT 2020 in Los Angeles was presented by Babak Hassibi. Babak reviewed the strengths of LA as a host city for ISIT, the team, the venues, the hotels (conference rate \$279/night), and the registration fee (early @ \$790 USD). Housing for students (and others) will be available at USC for \$40-\$60/night and will include transport to the conference center. There was discussion of the venue, logistics within LA, and cost of attendance. ISIT was last held in California in 1990.

The proposal to hold ISIT 2020 in Melbourne was presented by Emanuele Viterbo. Emanuele reviewed the strengths of Melbourne as a host city for ISIT, the team, the registration fee (early @ \$675 USD), a grant of financial assistant from Melbourne of AU \$102,000 of cash and in-kind support. There was a discussion of airline connections to Australia (about \$1200-\$1500 from N. America or Europe); Qantas and United Airlines will provide discounts to attendees. ISITA was hosted at the venue in 2014.

There was a discussion amongst the BoG about the proposals and also the possibility of awarding two ISITs given (1) that there are two excellent and comparable proposals, (2) both proposals have come to the table multiple times — this is the fourth time for Melbourne and the third time for Los Angeles. Pros and cons of awarding both the 2020 and 2021 ISITs at this BoG meeting were discussed.

Motion: To award the ISIT 2020 and 2021 to both LA and Melbourne conditioned on similar terms with the order and other details to be determined later by the board. Voting was as follows: 11 BoG members voted in favor of the motion, 6 voted to oppose. The motion passed.

Motion: To select the order of the ISITs (whether LA or Melbourne would occur in 2020). The motion was tabled (placed on hold for later consideration).

The two organizing committees were informed.

8) **Online Committee:** Online Committee Chair Anand Sarwate reviewed the committee composition. Two new members have joined the Committee: Evyatar Hemo and Mine Alsan. The redesign has been completed. The site will shortly re-launch and will include new content and capabilities. Anand reviewed the new features (improved member profiles, improved stability, automated office/committee membership updates, archiving capabilities), and outlined plans going forward (including archiving of old materials, solicitation of materials from the DL program, organization of resources for use by students/learners). The BoG raised some points about the redesign, providing feedback. Anand noted that funding of \$45k was contributed to the redesign by the IEEE Technical Activities Board (TAB).

9) **Shannon Documentary:** Sergio Verdú spoke about the Shannon Documentary. The objective is to produce a one hour non-commercial film for the science, public relations, and STEM markets. The producer for the film is Mark Levinson who directed the documentary “Particle Fever”. Sergio described Mark’s vision for the film. A number of interviews have been completed and the script is in revision. A clip was played of Andrew Shannon playing the trumpet. The goal is to have the documentary completed in (roughly) one year’s time.

10) **Schools Subcommittee:** Parastoo Sadeghi presented the proposal for the 2017 Australian School of Information Theory. The school will be three days long and will be held in January 2017. Young-Han Kim and Krishna Narayan will both be lecturers, with two more lecturers to be invited at ISIT. The school is planned for Canberra. The target size is 50 students. Total support request from IT-Soc is \$15000. The school will be run in tandem with AusCTW’17.

Motion: There was a motion to approve the funding for the 2017 Australian School. The motion was passed unanimously.

11) **TAB Vice President (José Moura), second presentation:** IEEE TAB Vice President, José Moura, next followed up his earlier remarks by informing the BoG of an upcoming proposed amendment to the IEEE constitution. The amendment regards the separation of the roles of Director and Delegates, i.e., of individuals being elected as members of the Board of Directors and elected as Delegates to the IEEE Assembly.

If effected, the constitutional change will reduce the size of the board from about 32 to 15. The 15 would include six officers and nine members-at-large elected directly by the membership for 3-year terms. The intention is for the restructured board to become a more agile and strategic organization. It would be supported by an operational board that will include the current six IEEE Vice Presidents such as the Vice President of Technical Activities and Chair of TAB, as well as the Vice President of Member and Geographic Activities Board (MGA) among others. This new operational board will, for example, vote on budgets, initiate new initiatives, etc. On the current IEEE Board, eleven members accumulate their Board representation with activities in the TAB. Similarly, eleven members accumulate their Board representation with activities in MGA. If the amendment is approved, this representation will be reflected directly in the Assembly, while the at large Board members will be elected directly by the membership.

At the June TAB meeting motions were presented asking the Board to rescind the constitutional amendment proposals. A motion presented in June to the Board to delay voting on the proposed amendment was defeated. The amendment presented to the membership will include a supporting statement from the Board and five opponent statements presented by five IEEE members. Different Society Boards have taken positions on the amendment. By IEEE electioneering rules, any communication to the membership should be balanced and include both sides of the argument.

12) **Report on the Transactions:** EiC Frank Kschischang reported on the Transactions. Frank thanked the retiring AEs. He reported that Prakash Narayan started in March as the new Executive Editor (EE) of the Transactions. The EE is responsible for assigning submitted papers to AEs, while the EiC retains overall responsibility, including assembly of issues, following up with reviewers, and handling appeals. When the term of the present EiC ends (at the end of the 2016 calendar year), the EE will assume the position of EiC and a new EE will be appointed by the Nominations and Appointments Committee. Paper submissions to the Transactions have been fairly constant over the past few years. The lengthy review cycle remains a concern (median time to first decision among papers sent out for review is 196 days); however, certain new measures (reducing the default review period, increasing the

intensity of reminders) are being implemented in an attempt to reduce review times. The quality of the Transactions, as measured by Eigenfactor, remains strong. Frank presented a slate of 13 new associate editors.

Motion: To approve the list of new AEs presented by the EiC. The motion passed unanimously.

- 13) **Fellows Committee:** Fellows Committee Chair Helmut Bölcskei first thanked the previous committee chair Robert Calderbank and the members of the committee for their work. There are 16 nominees for IEEE Fellow in 2016. Results will be announced by the IEEE in November 2016.
- 14) **ITSoc Coordinator report:** ITSoc Coordinator Matt LaFleur introduced himself and his role at IEEE: interfacing with the ITSoc membership and BoG. Matt's top efforts this year have been: the Shannon Centennial, the website update, executing contracts, and helping with conference organization. Matt is a very available resource at the IEEE for ITSoc members.
- 15) **Shannon Centennial Committee:** Rüdiger Urbanke presented on behalf of Shannon Centennial Committee Chair Christina Fragouli. Rüdiger reviewed the many documents that had been created for the Centennial (many contributed by ITSoc members) – educational posters, logos, banners, etc. These are available for members' use. Rüdiger reviewed a list of Centennial events and requests for support.
- 16) **Online Instruction Initiative:** Suhas Diggavi reviewed for the BoG the goal of the Online Instructional Initiative. This is to create an online video forum for information theory and applications. Content could include expository lectures, an "IT hall of fame" to provide an historic perspective the field, nascent research including talks on new ideas to foster collaboration, new research directions, and non-academic outreach. Suhas then reviewed the mechanisms that would be established to support such an initiative: a steering committee, an organizing committee, and a financial committee. The initiative would aim to bring together much scattered content (some of which is already online) into a single portal. There was general approval. There was a question of whether the initiative could be folded into the Online Committee. There was an observation that the

Online Committee handles the presentation of content, while this initiative is concerned with the generation of content.

- 17) **New publications (JSTIIT):** Jeffrey Andrews presented a "pre-proposal" on a new ITSoc journal. The working idea is a journal named something like the "IEEE Journal on Special Topics in Information Theory" with 4-6 special issues each year, a sub-to-pub of under one year, featuring both core "hot" topics and intersections with other fields. Jeff outlined a number of technical, logistical, and financial benefits.
- 18) **New publications (IT Magazine):** Elza Erkip next discussed the possibility of an "Information Theory magazine". An IT Magazine could provide a natural place for tutorial style papers, could contain a blend of traditional IT areas and new directions, and could help expand the visibility of the IT Community by providing a venue for ITSoc members to write articles about IT in a way that is more accessible to technical communities other than ITSoc. The Magazine would play a distinct role from the Newsletter, especially as the latter is only available to ITSoc members and is not searchable.
- 19) **Future directions:** Matthieu Bloch presented a report he put together with Helmut Bölcskei and Aylin Yener. The report considered what is happening in ITSoc in terms of "hot" research areas, where our graduates are going, and interdisciplinary efforts in which many ITSoc members are involved. Matthieu observed that there are a number of forums in which collaborations between researchers in ITSoc and other communities are fostered, e.g., at the ITA conference, at the Nexus of Information and Computation workshop at IHP in spring 2016, via special sessions and plenaries at ISITs and ITWs. Matthieu posed the question about how the Society can structurally support such forums.

The past three initiatives were broadly supported by the BoG. An online discussion of the above conversations will be moderated by the respective presenters

- 20) **Chicago BoG Meeting:** Daniela Tuninetti outlined the schedule and planning for the 1 October BoG meeting.

Adjournment: The meeting was adjourned at 6:30 pm CEST.

In Memoriam: Robert Fano

Robert Mario (Bob) Fano (11/11/1917–7/13/2016) was an eminent professor of electrical engineering and computer science at the Massachusetts Institute of Technology from 1947 to 1984; he remained an active emeritus professor almost until his death. His early career was in microwave circuits, followed by a career as an information theorist, followed by a career as a computer scientist.

Bob came from a distinguished academic family in Torino, Italy, where his father was a professor of mathematics. His older brother, Ugo, was a theoretical physicist who worked with Fermi and Heisenberg. Bob studied engineering at Torino and

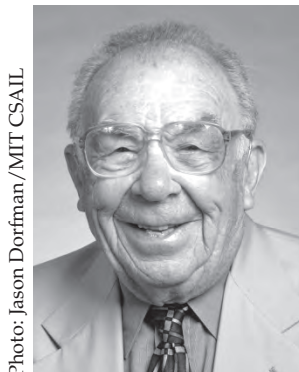


Photo: Jason Dorfman/MIT CSAIL

Robert Fano

Robert Gallager

was about to enter his senior year when fascism forced him to leave Italy in 1939. He finished his final year at M.I.T., earning an S.B. After continuing there as a teaching assistant and instructor, he joined the M.I.T. Radiation Lab in 1944 designing microwave circuits. After the war, he finished his ScD thesis in 1947 under the tutelage of the legendary circuit theorist Ernst Guillemin and then joined the MIT faculty.

At this time, MIT (including Lincoln Lab) was a major center for communication research. There was a great variety of work, ranging from pure research to practical development, in detection,

estimation, radar, electromagnetism, and microwave circuits. Much of this stemmed from wartime research, and there were important inputs from Norbert Wiener's research on fire control and on Cybernetics [6]. Bob had major interests in all these areas, and in looking for a new research area, was fascinated, as reported in several later interviews with Bob, by hearing Wiener say that "information is entropy."

Bob Fano had no idea what this meant at the time. Hartley and Nyquist, back in the 1920's, used the word information to describe the number of binary choices required to distinguish a message from its possible alternatives. Various classified documents during the war (including Claude Shannon's work on secrecy systems and Wiener's work on fire control) used probability to sharpen this notion of information and to allow a connection with the entropy formula from statistical mechanics.

Shannon had fully developed a mathematical theory of communication and data compression, including precise definitions of information, and information entropy, over a period of 8 years, culminating in the 1948 publication of his magnum opus, "A Mathematical Theory of Communication" [5]. Information theory, which was created in full bloom by this one publication, was publicly unknown in 1947.

Bob Fano, intrigued by Wiener's comments, started to explore how to represent probabilistic messages by binary choices, i.e., to construct binary codes. The result was a version [1] of what came to be called the Shannon-Fano code, an early way of both removing redundancy from discrete sources such as written language and also indicating that discrete entropy should describe the minimum required average number of encoded bits. Claude Shannon had developed a different version of this code as one of the starting points of his development of information theory. Bob attended an IRE conference in New York in March 1948 where Claude was talking about [5], including a discussion of this code. When Bob and Claude talked the next day, Claude was excited that someone else was thinking about these codes, and graciously included both his own version and Bob's version in [5]. From this interaction, Bob was primed to recognize that Shannon's fundamental set of ideas would form the unifying basis for the future of communication theory and practice.

Bob Fano quickly started gathering a group at MIT to study this new field and see how it connected with the other communication projects at MIT and Lincoln Labs. The group grew partly from faculty such as Peter Elias, hired from Harvard, but it grew even more from the doctoral students in the group (or closely related groups), some of whom, such as Bill Davenport, Jack Wozencraft, Dave Huffman, Irwin Jacobs, Bob Gallager, and Bob Kennedy, stayed on as faculty members after receiving their doctorates.

By 1957, Bob Fano was instrumental in bringing Claude Shannon himself to MIT. By this time, the group was quite sizable and well known, almost rivaling Bell Telephone Labs where Claude had been earlier. In fact over half of the first 25 winners of the Shannon Award (the primary prize of the IEEE Information Theory Society) were academic descendants of Bob, or were people who had done their major research at M.I.T.

Bob is well-known for his information theory research, and was the third recipient of the Shannon award after Shannon himself and

David Slepian. His Fano inequality, derived in his 1952 class notes for a graduate course on information theory, is a simple inequality relating the entropy of a random variable to its most probable sample value. This inequality implies that any code whose rate exceeds the capacity of the channel being used must have a probability of decoding error greater than a simple positive function of that rate difference.

Bob also supervised Jack Wozencraft's 1957 ScD thesis [7] on sequential decoding. For many years, this appeared to be the best practical choice for noisy channel coding when very low error probability was required. When Bob was on a sabbatical at Lincoln in 1961-62, his interest in sequential decoding was reawakened by a practical implementation called SECO being constructed there; this led him to invent an improved sequential decoding algorithm [3] that was vital both for that project and for later implementations. While at Lincoln, Bob also contributed to the development of the RAKE receiver, which is widely used in wireless communication.

Probably Bob's most important contribution in this era, rather than specific research, was the development and leadership of the information theory group at M.I.T. He was passionate and enthusiastic about his vision for the field, and his enthusiasm was contagious. At the same time, his vision encompassed a broad range of important topics, and he was supportive and encouraging toward a great variety of research. Claude Shannon played a different type of role in the group, constantly creating brilliant individual ideas over a wide variety of topics, whereas Bob was more conscious of the impact on communication technology. Together, their mentorship worked remarkably well.

There was a tendency among some information theorists to become overly mathematical, and among others to reject research with no immediate engineering applications. Bob helped moderate these extremes, recognizing that a combined focus on both basic understanding and future needs was important until solid state technology was sufficiently advanced for major applications.

For Bob Fano, the urge to publish individual research was always secondary to the urge to understand the field and to convey that understanding to others. He developed and taught the MIT graduate course in information theory for many years. A number of important results, such as Huffman coding [4], were developed in term papers for this course. Other results, such as the Fano inequality, were unpublished outside of his notes.

Bob recognized the need for expanding his notes into a textbook available for the burgeoning interest outside MIT, but he was also heavily involved in the modernization of MIT's undergraduate curriculum, and this led him to finish two undergraduate textbooks on electromagnetism, coauthored with Richard Adler and Lan Chu, first. Bob's passion for both undergraduate and graduate education remained strong throughout each of his careers and was recognized by receipt of the IEEE Education Medal in 1977.

The conversion of Bob's information theory notes into the textbook, *Transmission of Information* [2] was finally completed in 1961. Since the information theory texts of the day were either highly specialized or somewhat trivial, he chose to complete the

book quickly at this time rather than perfect it over several more years.

From 1960 to 1963, Bob Fano's restless mind was gradually turning its attention from information theory to computer science. Bob recognized that major direct applications of information theory would have to wait until digital hardware was more advanced. A more indirect result of information theory that occurred more quickly was the growing engineering recognition that all information sources could be efficiently converted to binary data, and this common binary interface could be used for communication, storage, and processing. Bob's emphasis on viewing theory and engineering together probably speeded this digital conversion, which in turn speeded the development of digital hardware.

The conventional view of computer usage in 1962 was that a computer's time was far more valuable than a user's time. Users would prepare punched cards which would enter a queue for access to the computer, which later printed out the results, more often than not an error message indicating a minor program error. Research had been proceeding for a few years to waste less user time by modifying computers to allow time-sharing between the programs of multiple users. Each such user would have an individual terminal with immediate access to the computer, sharing the resource but getting almost immediate feedback. The experiment in time-sharing at MIT at the time was called the Compatible Time-Sharing System (CTSS), led by Fernando Corbató.

As the cost of computers was decreasing, and the cost of talented researchers was increasing, there was general agreement at MIT that a major expansion of the CTSS experiment was necessary both as an important research topic in its own right and as a necessity to provide an appropriate environment for other researchers, both those in computer science and others requiring frequent computer resources. Such a community of researchers could also provide feedback to the time-sharing developers about how the system should work.

What was needed at this point was a leader who could pull together the needed government support, MIT top administrative support, and the support of what was to become a community of users. Bob Fano had always tried to avoid administrative jobs, but he was a natural leader and was trusted and supported by all the above groups, all of which recognized the need for such a project. He went ahead, with some trepidation. By late 1962, with great cooperation from everyone involved, and great tact, insight, and hard work on his own, Bob had pulled together the financial support, the space, and the personnel to start Project MAC.

Part of the plan for project MAC was to develop an experimental computer utility, MULTICS, whose function was viewed as

serving a broad set of user needs both reliably and conveniently rather than simply running programs. The project also supported the research of a broad community of users ranging from AI to the Theory of Computation group. Bob remained the director of Project MAC for 5 years in which the use of time-sharing on a computer utility was highly successful. The project also brought together into a community the many previously disparate users, designers, and theorists of computer systems; this community evolved into the MIT Laboratory for Computer Science (LCS) and then CSAIL.

Bob Fano's leadership in Project MAC was similar to that in information theory, but on a much larger scale. He promoted the same balance between research, mentoring, education, and community development. One might think that time-sharing on a computer utility would be a dead-end in the evolution to modern personal computers. A more accurate view is that the terminals of time-shared utilities evolved naturally into personal computers and the computer utility into the Internet. Bob Fano thus played an important role both in the development of communication and computation, the twin roots of today's information society.

The author gratefully acknowledges many helpful comments on this memorial from David Forney, Thomas Kailath, and Sergio Verdú.

References

- [1] R. M. Fano, "The Transmission of Information," MIT Research Laboratory of Electronics Technical Report, No.65, March 17, 1949.
- [2] R. M. Fano, *Transmission of Information: A Statistical Theory of Communications*. Cambridge MA: MIT Press and NY NY: Wiley, 1961
- [3] R. M. Fano, "A Heuristic Discussion of Probabilistic Decoding," *IEEE Trans. Inform. Theory*, **IT-9**, 64-74, 1963.
- [4] D. A. Huffman, "A Method for the Construction of Minimum-Redundancy Codes," *Proc. IRE*, **40**, 1098-1101, 1952.
- [5] C. E. Shannon, "A Mathematical Theory of Communication," *Bell System Technical Journal*, **27** 379-423 and 623-656, July and October, 1948. Also available on the web.
- [6] N. Wiener, *Cybernetics*. Cambridge MA: MIT Press and NY NY: Wiley, 1948.
- [7] J. M. Wozencraft, "Sequential Decoding for Reliable Communication," *National IRE Convention Record*, **5**, Part 2, 11-25, 1957.

In Memoriam: Dr. Titsa Panayota Papantoni-Kazakos

The unexpected and untimely passing on July 8, 2016 of our beloved and highly esteemed colleague, Dr. Titsa Panayota Papantoni-Kazakos, is a great loss to our professional global community of Electrical and Mechanical Engineers, and to her family and friends. It is difficult to describe accurately her contributions to the profession. The reason is that her illustrious career has been an inspiration to all women who aspire to contribute to society and to the Engineering profession, and to everyone to aspire to achieve excellence in science.



Titsa was born in Piraeus, Greece in 1945. She grew up in a society in which Engineering was a highly prestigious profession, possibly the most prestigious one. At the same time, it was highly dominated by males. This was a global, not Greek, tendency and attitude. Titsa was a highly motivated, talented, hard working and focused student. With the strong support of her parents, Thanassis and Helen, she succeeded in being admitted to the highly competitive School of Electrical and Mechanical Engineers of the National Technical University of Athens, Greece (NTUA). She was one of only two women in a freshman class of about 70. (The number of applicants exceeded 1000 for the 70 prestigious positions). Upon graduation with a Diploma in Electrical and Mechanical Engineering from NTUA in 1968, she started Graduate Studies with a full Graduate Research Assistantship at Princeton University. She received her Master's Degree in 1970, under the mentorship of Professor John Thomas, a legend in the field of Communication Theory. In 1969, she was married to Demetrios Kazakos, a fellow graduate student at the time. She then continued her Ph.D. studies at the University of Southern California, together with her husband, and under the inspired mentorship of the distinguished Communications researcher, Dr. Lee D. Davison. Titsa's daughter, Effie Kazakos, was born in 1971, while Titsa was completing her research for her Ph.D. As a tribute to her professionalism, and to the admirable support of her advisor, Lee Davison, Titsa continued her studies and she received her Ph.D. degree in Electrical Engineering in 1973. She was immediately offered the position of Assistant Professor at the Electrical Engineering Department of Rice University in July 1973. The distinguished Dr. Henry Bourne was the Chairman who hired her. *She was the first female Professor of Engineering at Rice University.* She remained in this position until 1977, when she longed to obtain industrial experience, thus she accepted the prestigious position as Member of the Technical Staff of the prestigious Bell Laboratories, where she remained for one year. During this one year at Bell Laboratories, she developed an algorithm for a distributed monitoring system for the reliable performance of high speed communication networks, using powerful statistical quality control monitoring algorithms. Her algorithm has been widely used by Bell Labs and AT&T in reliably operating data networks. But, after completing one year in industry, academia lured her back. The freedom to conduct advanced research and the mentoring of students were factors that convinced her to accept the position of Associate Professor at the *University of Connecticut, where, again, she was the first female professor of Engineering.* She remained in this position as Associate Professor until 1983, then promoted to Professor in 1983. She remained in this position until 1986. While on leave of absence from the University of Connecticut, she was for one year, 1981-1982 a program officer at the U.S. Office of Naval Research. In 1986 she moved to the position of Professor of Electrical Engineering at the *University of Virginia, and, again, became the first ever female Professor of the Department.* She was hired by the Department Chair, Dr. Edward Parrish, who was an inspired leader. He later became Dean of Engineering at Vanderbilt University and President of Worcester Polytechnic Institute. She remained in this position until 1993.

In 1993 she was appointed to the highly prestigious Canada Industrial Chair for High Speed Networks at the Electrical Engineering Department of the University of Ottawa, hired by the highly distinguished Dean of Engineering, Dr. Nicolas Georganas, recently deceased. Again, she was the first ever woman to be appointed to a Canada Industrial Chair position in the whole country. This chair was endowed by \$1,000,000 for a five year period. However, being very homesick for her adopted country, the United States, after only one year, in 1994, she was appointed to another Endowed Chair Professorship, at the University of Alabama. It was the

named Professorship: E.A. "Larry" Drummond Chair of Computer Engineering, within the Electrical Engineering Department. *Again, she was the first ever woman to hold an endowed Professorship in the Department.* She remained in this position until 2000, when she moved to become Professor and Department Chair at the Electrical Engineering Department of the University of Colorado at Denver. Being absorbed by her research, she stepped down from the position of Chair, and remained as Professor until her untimely passing. It was her passion for her field and her fearlessness that drove her to her great achievements. *It is evident that she was a pioneer in breaking the GLASS CEILING in ENGINEERING FACULTY POSITIONS FOR WOMEN, an incidental result of her passion for science and her drive for and achievement of excellence. She is an inspiration to us all.*

She received several honors:

- 1) Recipient of National Greek Fellowship throughout college (top 5 students get this)
- 2) Recipient of full graduate research fellowship at Princeton University and the University of Southern California throughout her graduate studies.
- 3) Awarded Fulbright Fellowship
- 4) **ELECTED FELLOW of the INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS in 1991 for: "Contributions to Communication Networks and to Detection and Communication Theory"**

She mentored many Ph.D. graduates and numerous M.S. graduates.

Her publication record was highly prolific. Based on her CV that dates up to June 2002, her publication record consists of two books, 65 refereed journal papers, 4 book chapters, and 151 refereed full conference proceedings papers.

She received many grants and contracts by Federal Agencies and Private Industry.

A TRAILBLAZER FOR WOMEN'S EQUALITY IN ENGINEERING AND AN EXCELLENT ROLE MODEL FOR EVERYONE.

She was a very enthusiastic and helpful advisor, working hard to be a role model to women and to all of her students. Hard working, dedicated, a great mother and wife, life and math teacher, best friend and inspiration to her adoring daughter, and a very supporting friend.

TITSA, THE WORLD WILL NOT BE THE SAME WITHOUT YOU!!!
REST IN PEACE!!! YOUR MEMORY WILL BE FOREVER WITH US.

Written by Demetrios Kazakos, ex husband of Titsa.
kazakosd@tsu.edu

From the Editor *continued from page 2*

a prominent and long time member of our society, who passed away on July 8th. Thanks to Robert Gallager and to Demetrios Kazakos for preparing the tributes.

Continuing our remembrance and honoring of Sol Golomb, an extraordinary scholar and long time newsletter contributor, a second collection of Sol's earlier puzzles appear in this issue. Solutions to the collection given here, and to that presented in the previous issue of the newsletter, will appear in the upcoming two newsletter issues.

Please help to make the newsletter as interesting and informative as possible by sharing with me any ideas, initiatives, or potential newsletter contributions you may have in mind. I am in the process of searching for contributions outside our community, which may introduce our readers to new and exciting problems and, as such, broaden the influence of our society. Any ideas along this line will also be very welcome.

Announcements, news, and events intended for both the printed newsletter and the website, such as award announcements, calls

for nominations, and upcoming conferences, can be submitted at the IT Society website <http://www.itsoc.org>. Articles and columns can be e-mailed to me at mikel@buffalo.edu with a subject line that includes the words "IT newsletter."

The next few deadlines are:

Jan. 10, 2016 for the issue of March 2017.

April. 10, 2016 for the issue of June 2017.

Please submit plain text, LaTeX, or Word source files; do not worry about fonts or layout as this will be taken care of by IEEE layout specialists. Electronic photos and graphics should be in high resolution and sent as separate files.

I look forward to hearing your suggestions and contributions.

*With best wishes,
Michael Langberg
mikel@buffalo.edu*

President's column *continued from page 1*

communication systems that will be deployed and ubiquitously utilized over the next indiction (turns out, 15 years). In addition to maintaining much of the existing information-theoretic infrastructure, 3GPP announced that it will utilize two new information-theoretic inventions. LDPC codes will power the data channels, while Polar codes will be used for the up-link control channel.

LDPC and Polar codes are information-theory's poster-kinder. Straight out of Shannon's playbook (now movie script), they were invented by theorists Robert Gallager and Erdal Arikan who sought conceptual beauty and mathematical elegance. Ingenious code designs and powerful decoding techniques developed by gifted information theorists turned them into practical algorithms and efficient circuits. And now major corporations will incorporate the codes into billions of devices that the whole world will constantly use to talk, watch, surf, and play.

It is quite impressive how our small society keeps benefiting society at large. No wonder that in my daydreams, where instead of companies, true science is rewarded, some slogans get reworded: each of the 1.2 billion cellphones sold annually bears the "IT inside" logo, and all 10 billion daily cell-calls end with "Thank you for using information theory". We definitely "Just do IT". Again and again.

But as we celebrate these significant milestones, we should keep in mind that even laureates can't long rest on their laurels. Emboldened by our industrial communication and storage success, why not venture out even more actively and impact addi-

tional fields? The theory that Shannon founded and our society members have built is a universal, powerful, and effective tool for measuring, analyzing, and processing any form of information. The information age around us is rife with important and beautiful problems that call for a disciplined approach proven to provide useful insights and optimal algorithms. Our society could be further invigorated by fresh problems, interaction with new communities, and an expanded bag of tricks. And finally, our cadre of students, equipped with deep fundamental education and broad practical training would be hard to beat. Let's do IT.

And so as I, like another US-based president, make way for our master-communicating, fun-show-moderating, best-book-selling, successfully-polarizing, make-IT-great-again successor, let me thank those who have made my POTITS year so enjoyable and rewarding. Our board members whose wisdom, wit, and collegiality kept our meetings constructive, engaging, and occasionally, timely. Our selfless volunteers who in theory chose information over evolution, diverting precious time and energy from numero uno to help numerous others they may not even know. And mostly our members in both academia and industry whose outstanding research and practical contributions have educated generations of engineers and empowered crucial technologies. I have been truly fortunate to be part of this exceptional society, and thank you for the year-long opportunity to serve, observe, and quarterly pontificate.

Wishing you a prosperous, peaceful, and productive 2017.

GOLOMB'S PUZZLE COLUMN™ COLLECTION, Part 2

Beyond his extraordinary scholarly contributions, Sol Golomb was a long time newsletter contributor enlightening us all, young and old, with his beautiful puzzles. In honor of Sol's immense contribution

to the newsletter, a collection of his earlier puzzles dated back to 2001 appears in 4 compiled parts over previous, current, and upcoming issues. Part 2 is given below. He will be greatly missed.

Reprinted from Vol. 54, No. 1, March 2004 issue of Information Theory Newsletter

GOLOMB'S PUZZLE COLUMN™

AN INVERSE PROBLEM

Soloman W. Golomb



Suppose there is a set S of n distinct positive real numbers which you are asked to determine, given only the set T consisting of the $\binom{n}{k}$ sums of all the k -element subsets of S . (You are not told which sum corresponds to which subset.) For many values of n and k the reconstruction of the elements of S is unique. It is also possible to have two different solutions for S , given T , or even to have a continuum of values for the elements of S , given T , for certain pairs n and k . In the first four problems, find all possible sets S consistent with the given set T .

1. $n = 4, k = 2, T = \{24, 28, 30, 32, 34, 38\}$.

2. $n = 5, k = 2, T = \{21, 26, 28, 29, 31, 34, 36, 37, 42, 44\}$.

3. $n = 6, k = 2, T = \{32, 35, 37, 39, 41, 43, 44, 45, 48, 49, 51, 52, 54, 58, 62\}$.

4. $n = 6, k = 3, T = \{49, 54, 56, 57, 58, 60, 61, 65, 66, 67, 68, 69, 70, 74, 75, 77, 78, 79, 81, 86\}$.

The next four problems are more general.

5. Show that the problem of reconstructing S from T for given n and k is precisely equivalent (procedurally) to the corresponding problem for n and $k' = n - k$.

6. For $k = 2$ and each $n \geq 2$, how many solutions are there for S ? (There are different answers for different values of n .)

7. How many solutions are there for S if $n = k > 1$?

8. For what pairs n and k are there exactly two reconstructions for S ?

GOLOMB'S PUZZLE COLUMN™

Some Prime Number Properties



Solomon W. Golomb

We let p_n denote the n^{th} prime number ($p_1 = 2, p_2 = 3, p_3 = 5$, etc.), and $\pi(x)$ is the number of primes $\leq x$, for any positive real number x . Note that $\pi(p_n) = n$. The "Prime Number Theorem" of 1896 states that $\pi(x) \sim x/\log x$ as $x \rightarrow \infty$, where "log" is the natural logarithm. In particular, $\lim_{x \rightarrow \infty} \frac{\pi(x)}{x} = 0$, and $\lim_{n \rightarrow \infty} p_n = \infty$.

1. Prove that the ratio $\frac{n}{\pi(n)}$, for $n \geq 2$, takes every integer value > 1 at least once.
2. Let $\{s_n\} = \{n + \pi(n)\}$ and let $\{t_n\} = \{n + p_n - 1\}$, for all $n \geq 1$. Prove that the union of the sequences $\{s_n\}$ and $\{t_n\}$ is the set of all the positive integers, while the intersection of $\{s_n\}$ and $\{t_n\}$ is empty.
3. Given positive integers a and b , show that there exists a positive integer c such that infinitely many numbers of the form $an + b$ (n a positive integer) have all their prime factors $\leq c$.
4. (a) What is the largest integer N such that, if $1 < k < N$ and k has no prime factor in common with N , then k is prime?
 (b) What is the largest *odd* integer N such that, if $1 < k < N$ and k has no prime factor in common with $2N$, then k is prime?
5. For what positive integers n is it true that $\sum_{p \leq \pi(n)} p = n$?
6. Let $a_1 < a_2 < a_3 < \dots$ be an increasing, infinite sequence of positive integers.
 - (a) Construct such a sequence $\{a_k\}$ having the property that, for *every* integer n (positive, negative, or zero) the sequence $\{a_k + n\}$ contains only finitely many prime numbers.
 - (b) Is there such a sequence $\{a_k\}$ and a constant $B > 0$ such that, for every integer n (positive, negative, or zero) the sequence $\{a_k + n\}$ contains no more than B prime numbers?

GOLOMB'S PUZZLE COLUMN™

Countable or Uncountable

Solomon W. Golomb



A set S is *countably infinite* if its members can be put in 1-to-1 correspondence with the positive integers. If S is an infinite set whose members cannot be put in 1-to-1 correspondence with the positive integers, then S is *uncountably infinite*.

You may use each of the following well-known facts in solving the current set of problems.

- The set of real numbers on any interval (a, b) of the real line, with $a < b$, is uncountably infinite.
- The set of all k -tuples of the positive integers is countably infinite.
- The set of *all* subsets (or, all subsequences) of the positive integers is uncountably infinite.
- The set of all *finite* subsets of the positive integers is countably infinite.

In each of the following problems, S is a collection of infinite subsets (or, infinite subsequences) A_i of the positive integers. (The subscript " i " does not necessarily come from the set of positive integers. It can just as well come from an uncountably infinite set.) In each problem you are to indicate whether it is possible for S to be uncountably infinite. If so, you are to exhibit a construction for an uncountable set of A_i 's meeting the conditions for belonging to S . If S can be (at most) countably infinite, you must prove that S cannot be uncountably infinite.

- The subsets A_i in S are pairwise disjoint.
- The intersection of any two distinct subsets A_i and A_j in S is finite.
- The intersection of any two distinct subsets A_i and A_j in S contains at most m elements, for some positive integer m .

GOLOMB'S PUZZLE COLUMN™

A QUADRATIC SEQUENCE

Solomon W. Golomb



Let $s_n = 2n^2 + 2n + 1$ for all integers $n \geq 0$. Thus, $S = \{s_n\} = \{1, 5, 13, 25, 41, 61, 85, 113, 145, 181, 221, 265, \dots\}$. Some knowledge of elementary number theory will be helpful in addressing the following questions.

- Prove that if p is a prime number that divides any term of the sequence S , then $p = 4m + 1$ for some positive integer m .
- Show that *every* prime p of the form $4m + 1$ divides terms of the sequence S .
- Show further that for each prime p of the form $4m + 1$, there are two residue classes, a and b , modulo p , such that p divides s_n for all $n \equiv a \pmod{p}$ and for all $n \equiv b \pmod{p}$, where $a + b \equiv -1 \pmod{p}$ and $a \neq b$. (For example, with $p = 5$, we can take $a = 1$ and $b = 3$.)

4. Note that $s_0 = 1^2$, $s_3 = 5^2$, and $s_{20} = 29^2$. Find all the values of n for which s_n is a square integer.

5. In the previous problem, consider the sequence $c = \{c_n\} = \{1, 5, 29, \dots\}$ of the numbers whose squares occur (in increasing order) in the sequence S . Find a recursion relation satisfied by the terms of C , and determine $\lim_{n \rightarrow \infty} \left(\frac{c_{n+1}}{c_n} \right)$.

*6. Are any of the terms of S perfect cubes or higher powers?

*7. What can you say about the frequency of prime numbers in the sequence S ?

(Complete solutions to the starred problems may exceed the current state of knowledge.)

GOLOMB'S PUZZLE COLUMN™

Perfect Powers and Powerful Numbers

Solomon W. Golomb



The *perfect powers* are the squares, cubes, and higher powers of the positive integers. They form the set $P = \{1, 4, 8, 9, 16, 25, 27, 32, 36, 49, 64, 81, 100, 121, 125, 128, 144, 169, 196, 216, 225, 243, 256, 289, \dots\}$.

The *powerful numbers* are those positive integers n such that, if the prime p divides n , then p^2 divides n . The set Q of powerful numbers contains all members of P , but also such numbers as 72, 108, 200, 288, 392, 500, 675, etc.

For some of these problems, you will need to be familiar with the Riemann Zeta Function, $\zeta(s)$, which for real values of $s > 1$, satisfies

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{\text{all } p} \left(1 - \frac{1}{p^s}\right)^{-1},$$

where the product is taken over all prime numbers p .

Here are the problems.

1. The relation between the sets P and Q is given by:

- (a) $Q = P \times P$, the direct product of P with itself
- (b) $Q = P + P$, the direct sum of P with itself
- (c) $Q = \{\text{set of all finite products of elements of } P\}$
- (d) None of the foregoing.

2. Which of the following is equal to $\sum_{n \in Q} \frac{1}{n}$, the sum of the reciprocals of the powerful numbers?

- (a) $\zeta(2) + \zeta(3) - \zeta(6)$
- (b) $\zeta(2)\zeta(3) - \zeta(6) + 1$

(c) $\zeta(2)\zeta(3)/\zeta(6)$

(d) None of the foregoing.

3. Which of the following is equal to $\sum_{n \in P} \frac{1}{n}$, the sum of the reciprocals of the perfect powers?

- (a) $\sum_{k=2}^{\infty} (-1)^k \zeta(k)$
- (b) $-\sum_{k=2}^{\infty} \mu(k) \zeta(k)$
- (c) $\sum_{k=1}^{\infty} \mu(k) \zeta(2k)$
- (d) None of the foregoing.

(Here $\mu(k)$ is the Möbius mu-function.)

4. Which of the following is equal to $\sum_{\substack{n \in P \\ n > 1}} \frac{1}{n-1}$, where the sum is taken over all perfect powers greater than 1?

- (a) 1
- (b) $\log_e 2$
- (c) $\frac{\pi}{4}$
- (d) None of the foregoing.

5. Prove that there are infinitely many pairs of consecutive powerful numbers, such as (8, 9). (*Note.*) Unless you include (0, 1), the pair (8, 9) is the only example of consecutive perfect powers.)

GOLOMB'S PUZZLE COLUMN™

Some Matrix Questions

Solomon W. Golomb



1. Is it possible to find 2×2 real matrices A and B such that A is similar to B but AB is not similar to BA ?
2. The **hermitian** of a complex $n \times n$ matrix M , denoted M^H , is $(M^T)^* = (M^*)^T$, where M^T is the **transpose** of M and M^* is the **complex conjugate** of M . If U and N are complex $n \times n$ matrices with $U^H = U^{-1}$ and $NN^H = N^H N$, then U is called **unitary** and N is called **normal**. Prove or disprove: "If, for a given complex $n \times n$ matrix M , there exists a unitary matrix U such that $U^{-1}MU = \Lambda$, where Λ is a diagonal matrix, then M is normal."
3. Prove or disprove: "If N_1 and N_2 are normal $n \times n$ matrices, then their product $N_1 N_2$ is normal."
4. Using 2×2 matrices over $GF(2)$ as elements, form a four-element ring R which has two "left identities" but no "right identities". (A **left identity** e_L has the property that $e_L \cdot a = a$ for all a in R . A **right identity** e_R has $a \cdot e_R = a$ for all a in R .)
5. If the n^2 elements of an $n \times n$ matrix A are integers chosen independently and at random, what is the probability that $|A|$, the determinant of A , is odd?

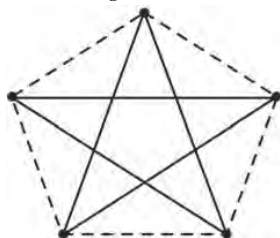
GOLOMB'S PUZZLE COLUMN™

Ramsey's Triangles

Solomon W. Golomb



The original **Ramsey Theorem** is often stated as follows: In any collection of six people, there will always be either three people mutually acquainted, or three mutually unacquainted. In graph theory terms, this says that if K_6 is the "complete graph" on 6 points (i.e.~there is an edge between each pair of points, for a total of $\binom{6}{2} = 15$ edges), if two colors are used to color the 15 edges there must always be a solid-color triangle (3 points connected by 3 edges of the same color). In contrast, the $\binom{5}{2} = 10$ edges of K_5 can be 2-colored without forming a solid-color triangle, as shown:



(Here the two colors are represented by solid or dotted lines.)

1. How many of the 15 edges of K_6 must be deleted so that the remaining edges can be 2-colored without forming a solid-color triangle?

solid-color triangle?

2. How many of the $\binom{10}{2} = 45$ edges of K_{10} must be deleted so that the remaining edges can be 2-colored without forming a solid-color triangle?
3. It is known that if the $\binom{17}{2} = 136$ edges of K_{17} are colored using 3 colors (i.e.~3-colored), a solid-color triangle must be formed, but that it is possible to 3-color the $\binom{16}{2} = 120$ edges of K_{16} without forming a solid-color triangle. How many edges of K_{17} must be deleted so that the remaining edges can be 3-colored without forming a solid-color triangle?
4. Let $r = r(c)$ be the smallest positive integer such that, if the $\binom{r}{2}$ edges of K_r are colored using c colors, then there must be a solid-color triangle. How many of the edges of K_r must be deleted so that the remaining edges can be c -colored without forming a solid-color triangle anywhere? (Surprisingly, the answer to this question does not depend on knowing the value of r for the given value of c .)

GOLOMB'S PUZZLE COLUMN™

Simple Probabilities



Solomon W. Golomb

1. Five cards are dealt at random from a standard 52-card bridge deck. The first four are observed to all be hearts. What is the probability that the fifth card will also be a heart?
2. Five cards are dealt at random from a standard 52-card bridge deck. If at least four of the cards are hearts, what is the probability that all five are hearts?
3. Six "ideal" dice are tossed. What is the probability that a) at least one shows a 5?, b) exactly one shows a 5?
4. Six "ideal" dice are tossed. What is the probability that of the six numbers shown, all are a) the same?, b) different?
5. In a certain game show, there is a large prize behind one of four doors, but nothing behind the other three. You are told to guess which door conceals the prize. The emcee (as a standard procedure on this show) will then eliminate two of the wrong doors, but not the one you originally guessed (whether right or wrong). You then are given the opportunity to change your original guess to the other remaining door. Your best strategy is a) stick with your original guess, b) switch, or c) it makes no difference. (You win the prize if and only if your final choice is correct.)
6. A hat contains five seemingly identical half-dollar coins, but only four are "honest". The fifth coin has *heads* on both sides. You are blindfolded, and instructed to extract one of the five coins at random, and place it flat on a tabletop. The blindfold is removed, and you see that the coin shows *heads*. What is the probability that the other side is also *heads*?
7. On average, how many times must a pair of dice be tossed to show, for the first time, a total of k , for each k from 2 to 12?
8. A positive real number x , selected at random, is written on a card in one sealed envelope, and the number $2x$ is on a card in a second sealed envelope. You select one of the two envelopes. You will receive the amount, in dollars and cents (rounded to the nearest cent, two places after the decimal point) of the envelope you select. However, *after* you open the envelope and see a number y , you are allowed to change your mind and pick the other envelope. You reason as follows: The original envelope you picked shows an amount y . The other envelope is equally likely to show $\frac{1}{2}y$ or $2y$, for an expected value of $\frac{1}{2}(\frac{1}{2} + 2)y = \frac{5}{4}y$; so your expectation increases by 25% if you switch. Is your reasoning correct?

GOLOMB'S PUZZLE COLUMN™

Mini-Sudoku



Solomon W. Golomb

As everyone by now is surely aware, the normal Sudoku puzzle requires the solver to complete a 9×9 Latin square, using the symbols 1 through 9, with the added requirement that each of the nine 3×3 subsquares uses each of the nine symbols exactly once. (The "Latin square" requirement is that each row, and each column, uses each of the symbols exactly once.) A Sudoku puzzle is properly posed if and only if there is one and only way to complete the 9×9 array, consistent with the symbols already filled in.

An analogous "generalized Sudoku" puzzle can be defined on any $n^2 \times n^2$ array, using n^2 distinct symbols, and requiring that each row, each column, and each of the n^2 subsquares of size $n \times n$ contain each of the symbols exactly once. Normal Sudoku uses $n = 3$. The challenge clearly increases as n gets larger. Instead, we will look at the case $n = 2$. This "Mini-Sudoku" is played on a 4×4 array, using four distinct symbols (say 1, 2, 3, 4), where each row, each column, and each quadrant must contain each of the four symbols exactly once. Here are some Mini-Sudoku questions.

1. How many distinct Mini-Sudoku solutions (i.e. filled-in arrays) are there? (Here we consider two solutions *distinct* unless they are identical.)
2. Can you find a Mini-Sudoku solution in which the two diagonals also contain each of the four symbols exactly once?
3. What is the minimum number of cells in the 4×4 array which must be filled in to guarantee a unique Mini-Sudoku solution? Exhibit an example of such a minimum configuration.
4. The partial array

1			
			2
	3		

does not guarantee a unique solution. However, show what entry *must* appear in the lower right-hand corner.

5. What is the maximum number of cells in the 4×4 array which can be filled in such that the Mini-Sudoku solution is not unique? Exhibit an example of such a configuration.
6. Two $n \times n$ Latin squares are called *orthogonal* if the n^2 ordered pairs of corresponding entries are all distinct. Find a pair of orthogonal Mini-Sudoku solutions.
7. The 4×4 Magic Square

0	5	10	15
14	11	4	1
7	2	13	8
9	12	3	6

contains each of the numbers 0, 1, 2, ..., 15 exactly once. Each row, column, and diagonal sums to 30. So too do the four Mini-Sudoku 2×2 subsquares, and the four Mini-Sudoku "anti-subspaces" indicated by the letters A, B, C, D in

A	B	B	A
C	D	D	C
C	D	D	C
A	B	B	A

Can you explain how I generated this Magic Square from Mini-Sudoku solutions? (*Hint*: Look at problems 2 and 6.)

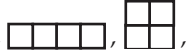

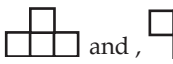
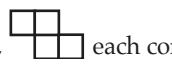
GOLOMB'S PUZZLE COLUMN™

Classic Mathematical Quickies

Solomon W. Golomb



What these problems have in common is that in each case there is a simple way to arrive at the solution, with minimal computation.

- Suppose that 163 people enter a singles tennis elimination tournament. In the first round, 81 matches are played, and one player has a bye. In the next round, the 81 first-round winners and the bye-holder are paired, and 41 matches are played. In each subsequent round, winners advance, losers are eliminated, and bye-holders (if any) also advance to the next round. Eventually a single overall winner emerges. How many actual matches (not counting byes) are played in the entire tournament?
- There are 200 green marbles in a green jar, and 200 red marbles in a red jar. Thirty green marbles are taken from the green jar and inserted into the red jar, which is then thoroughly shaken. Then thirty marbles are taken from the shaken red jar and put into the green jar. Are there now more red marbles in the green jar, or green marbles in the red jar?
- A cubic ice cube, 2 cm on each edge, is floating in a level cylindrical jar of water, filled to the brim, at a temperature of 4°C. The inner dimensions of the jar are that the circular base has an 8 cm diameter, and the height is 6 cm. When the ice cube has melted completely, how much water (in cm³) will have spilled over the rim of the jar?
- You bought 650 shares of ZYX Corp. at \$86.50 per share. Over the next three months, the stock declined in value by exactly 20%. However, over the following three months, the stock then went up by 25%. Six months after your original purchase, by how much (in dollars) are you now ahead (ignoring any commissions for buying or selling)?
- John and his grandmother both celebrate their birthdays on January 16. Next year, on their common birthday, John's age will be exactly half that of his grandmother's. When will John be as old as his grandmother was on the day that John was born?
- Evaluate the product $(x-a)(x-b)(x-c)\cdots(x-z)$ in the case that $a = 1, b = 2, c = 3, \dots, z = 26$.
- Mr. and Mrs. Jones have invited five other (heterosexual) couples to a dinner party. Their rectangular dinner table has one chair at each narrow end, and five chairs along each of the two long sides. Mr. and Mrs. Jones wish to sit at the two narrow ends of the table, and to seat their guests along the two long sides in such a way that men and women alternate all around the four sides of the table. In how many ways can this seating be accomplished?
- The five *tetrominoes* are the five shapes, , ,  and  each consisting of four unit squares. Can you assemble these shapes to form a 4 × 5 rectangle? (The shapes can be rotated and turned over as you wish.)

GOLOMB'S PUZZLE COLUMN™

Classic Mathematical Quickies

Solomon W. Golomb



We consider the following four quadratic matrix equations.

A) $M^2 = M$

B) $M^2 = -M$

C) $M^2 = I$

D) $M^2 = -I$

where M is an $n \times n$ matrix with elements from a field F . Here F may be the real number field R , the complex number field C , or the integers modulo p , Z_p , for any prime number $p > 2$.

The following questions should be answered separately for each of the four matrix equations.

1. What are the possible values of $|M|$, the determinant of M ?
2. If $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, what are the possible values of $Tr(M)$, the trace of M ?
3. If $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, what are the possible characteristic polynomials for M ? What are the corresponding eigenvalues? (The eigenvalues will either lie in the field F , or a "quadratic extension" of F .)
4. With $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, find the general solution for M that satisfies the given equation. This solution should be given as explicitly as possible. (For example, the general solution of $M = -M^T$ would be $M = \begin{pmatrix} 0 & b \\ -b & 0 \end{pmatrix}$, where M^T is the transpose of M .) The general solution may be a union of two or more cases.

Reprinted from Vol. 56, No. 4, December 2006 issue of Information Theory Newsletter

GOLOMB'S PUZZLE COLUMN™

The $3X + 1$ Problem

Solomon W. Golomb



The notorious " $3X + 1$ problem" is usually described as a mapping T from Z^+ (the positive integers) into Z^+ , where $T(n) = 3n + 1$ if n is odd while $T(n) = n/2$ if n is even. The most important conjecture is that no matter what positive integer m you start with, if you perform the mapping T repeatedly you will ultimately arrive at the number 1. (The logical alternatives are that you may end up in a "limit cycle" of some period $c > 1$, or that from some starting integer m , all elements of the sequence $\{m, T(m), T^2(m), T^3(m), \dots\}$ are distinct and therefore tend toward infinity. Extensive computation has failed to discover either the limit cycle $c > 1$ case or the "tending toward infinity" case, but these have not been theoretically ruled out.)

I would like to propose a trivial modification to speed up the process. Let M be the mapping from U^+ (the positive odd integers) into U^+ given by $M(n) =$ the largest odd divisor of $3n + 1$, for each n in U^+ . (Thus, $M(n) = (3n + 1)/2^k$, where the denominator is the highest power of 2 that divides $3n + 1$.)

For example, if we start with $n = 9$, the sequence $\{n, M(n), M^2(n), \dots\}$ becomes $\{9, 7, 11, 17, 13, 5, 1\}$.

All questions in this column can be answered fairly easily,

and most of them involve the inverse mapping $M^{-1}(n)$ concerning the predecessors of n with respect to the mapping M .

1. Starting with $n = 27$, calculate the sequence $\{n, M(n), M^2(n), M^3(n), \dots\}$ until you end up at "1".
2. Determine the set Q of positive odd integers with no predecessors with respect to M . (That is, for n in Q there is no m with $M(m) = n$.)
3. For what positive odd integers t is $M(t) = 1$?
4. Show that any positive odd integer n not in the set Q has infinitely many distinct predecessors with respect to M .
5. Are there any positive odd integers that have "parents" (i.e. predecessors) but no "grandparents" with respect to M ?
6. Prove that there are no non-trivial two-cycles, i.e. values of $n > 1$ with $M(M(n)) = n$.

GOLOMB'S PUZZLE COLUMN™

Calculator Magic



Solomon W. Golomb

For these questions, you will need a simple hand-held calculator with a ten-decimal-digit display that has the operations $+$, $-$, \times , \div , x^2 , and \sqrt{x} . (In a few cases, it will save time if you can also calculate x^n directly.) The first three questions involve integer answers, without roundoff. The remaining questions want answers rounded to ten significant decimal digits.

1. What is the largest integer n for which the digits of 2^n are all distinct?
2. Consider the values of n^8 for all n with $1 < n < 18$.
 - (a) Which of these numbers have all their digits distinct?
 - (b) Which of these numbers have their two most significant digits the same (in order) as their two least significant digits?
 - (c) Which two values of n^8 have the same three most significant digits *and* the same two least significant digits?
3. Find a five-digit number A , having no 0's among its digits, such that the ten digits of A^2 contain only two *distinct* digits, each occurring more than three times.
4. What four-digit whole number has a square root which displays all 10 decimal digits?
5. For what value of n does $n/(n+1)$ display all ten decimal digits, in an easily recognized order? (Consider $0 < n < 100$.) What happens when this value of $n/(n+1)$ is multiplied by k , for $0 < k < 10$?
6. Consider the numbers $(10n/9)^2$ for all n , $1 \leq n \leq 30$, and look at the ten displayed digits.
 - (a) For which values of n are all 10 displayed digits the same?
 - (b) For which values of n are all 10 displayed digits distinct?
 - (c) What patterns do you observe among the 10 displayed digits in part b?
7. Look at the decimal expansion of a/b for $0 < a < b < 30$. Are any of these "pan-digital"? (That is, do you see all ten distinct decimal digits?)
8. Enter 2143. Divide by 22. Take the square root twice. (That is, calculate $(2143/22)^{\frac{1}{4}}$). What do you now see?

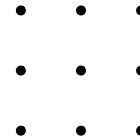
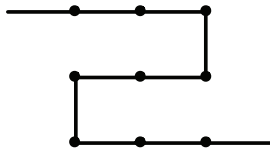
GOLOMB'S PUZZLE COLUMN™

CONNECT THE DOTS

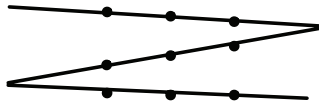
Solomon W. Golomb



A familiar puzzle presents the solver with a 3×3 square array of dots, and asks for a continuous path ("without lifting the pen from the paper") consisting of only 4 straight-line segments, that goes through all 9 points. An attempt that uses 5 segments is

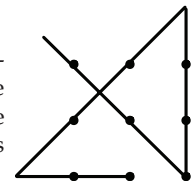


Assume that we are dealing with ideal mathematical points and lines, with no thickness, and that the points are perfectly aligned, to rule out such attempts as



which "succeeds" with only 3 line segments.

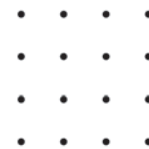
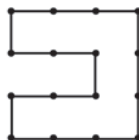
The well-known solution to the puzzle problem is as shown, and is unique except for rotations and reflections of the pattern. This solution violates three limitations which many solvers subconsciously impose: line segments are not limited to horizontal and vertical; line segments may intersect (and not even at one of the 9 points); and the solution requires "thinking outside the box" -- quite literally -- in that the segments extend beyond the convex hull of the 9 original points.



We generalize this puzzle to larger arrays. On an $n \times n$ square array of regularly placed dots, for $n > 3$, we ask for a *closed path* (a *circuit*), consisting of $2n - 2$ segments, which goes through all n^2 points, and returns to the starting point.

1. Find a 6-segment *closed path* that goes through all 16 points of the 4×4 array:

For full credit, find *all four* inequivalent solutions. (An unsuccessful attempt is



since it uses 8 segments instead of 6.)

2. Find an 8-segment closed path that goes through all 25 points of the 5×5 square array of dots: How many inequivalent solutions can you find? (There is no requirement that a solution must possess any symmetry.)
3. On the 6×6 array of dots, find a 10-segment circuit. Among your solutions, can you find one that stays within the convex hull of the 36 points?
4. A "queen's tour" of the 8×8 chessboard, in 14 moves, requires a chess queen, starting on one of the 64 squares of the board, making a sequence of 14 "queen moves" (horizontal, vertical, or with slope ± 1) which passes through or lands on every square on the board, and returns to the starting square. Can you find such a queen's tour?
5. Find a closed path (a circuit) of five connected line segments that goes through all 12 of the dots in a 3×4 array and returns to the starting point. The solution is unique (up to symmetries of the rectangle), and the five "turning points", where two segments meet, are all distinct from the 12 points of the array.



GOLOMB'S PUZZLE COLUMN™

EASY PROBABILITIES

- Five of the ten decimal digits 0, 1, 2, 3, 4, 5, 6, 7, 8, 9 are selected at random, and arranged in ascending order as $a < b < c < d < e$. What is the probability that $a + b + c > d + e$?
- You have n red marbles and n green marbles, with $n > 1$, which you will put into two jars in any way you like. A blindfolded contestant will select one of the two jars at random, and then select one marble from that jar at random. How should you distribute the $2n$ marbles into the two jars to maximize the probability that the selected marble will be green, and what is this maximized probability?
- At the bridge table, when all 52 cards have been dealt, is it more likely that you and your partner together have all 13 hearts or none of the hearts?
- You will play three tennis matches against two opponents, A and B, where A is a stronger player than B. You may choose to play them in either the sequence ABA or BAB.

Solomon W. Golomb



Which sequence gives you the better chance of winning two matches in a row?

- The passenger next to you on the airplane (whom you never previously met) tells you she has two children. What is the probability that they are both girls if she says "yes" to:
 - Is at least one of them a girl?
 - Is the older one a girl?

(Here we assume that boys and girls are equally likely *a priori*, and that you have no information beyond the truthful answer to Question *a* or to Question *b*).

- An opaque jar contains one marble, known to be either black or white (equally likely *a priori*). A white marble is now placed into the jar, which is shaken, and a marble is removed "at random" and observed to be white. What is the probability that the marble still in the jar is white?

Call for Nominations

(ordered by deadline date)

Thomas M. Cover Dissertation Award

The IEEE Information Theory Society Thomas M. Cover Dissertation Award, established in 2013, is awarded annually to the author of an outstanding doctoral dissertation.

NOMINATION PROCEDURE: Nominations and letters of endorsement must be submitted by **January 15, 2017**. All nominations should be submitted using the online nomination forms. Please see <http://www.itsoc.org/cover-award> for details.

IEEE Joint ComSoc/ITSoc Paper Award

The Communications Society/Information Theory Society Joint Paper Award recognizes outstanding papers that lie at the intersection of communications and information theory. Any paper appearing in a ComSoc or ITSoc publication during the preceding three calendar years is eligible for the award.

NOMINATION PROCEDURE: Nominations and letters of endorsement must be submitted by **February 15, 2017**. All nominations should be submitted using the online nomination forms. Please see <http://www.itsoc.org/honors/comsoc-information-theory-joint-paper-award/comsoc-itsoc-paper-award-nomination-form> for details. Please include a statement outlining the paper's contributions.

IEEE Information Theory Society Claude E. Shannon Award

The IEEE Information Theory Society Claude E. Shannon Award is given annually to honor consistent and profound contributions to the field of information theory.

NOMINATION PROCEDURE: Nominations and letters of endorsement must be submitted by **March 1, 2017**. All nominations should be submitted using the online nomination forms. Please see <http://www.itsoc.org/shannon-award> for details.

IEEE Information Theory Society Aaron D. Wyner Distinguished Service Award

The IT Society Aaron D. Wyner Service Award honors individuals who have shown outstanding leadership in, and provided long standing exceptional service to, the Information Theory community.

NOMINATION PROCEDURE: Nominations and letters of endorsement must be submitted by **March 1, 2017**. All nominations should be submitted using the online nomination forms. Please see <http://www.itsoc.org/wyner-award> for details.

IEEE Fellow Program

Do you have a colleague who is a senior member of IEEE and is deserving of election to IEEE Fellow status? If so, please submit a nomination on his or her behalf to the IEEE Fellow Committee. The deadline for nominations is **March 1 2017**.

IEEE Fellow status is granted to a person with an extraordinary record of accomplishments. The honor is conferred by the IEEE Board of Directors, and the total number of Fellow recommendations in any one year is limited to 0.1% of the IEEE voting membership. For further details on the nomination process please consult: <http://www.ieee.org/web/membership/fellows/index.html>

IEEE Information Theory Society Paper Award

The Information Theory Society Paper Award is given annually for an outstanding publication in the fields of interest to the Society appearing anywhere during the preceding two calendar years. The purpose of this Award is to recognize exceptional publications in the field and to stimulate interest in and encourage contributions to fields of interest of the Society.

NOMINATION PROCEDURE: Nominations and letters of endorsement must be submitted by **March 15, 2017**. All nominations should be submitted using the online nomination forms. Please see <http://www.itsoc.org/honors/information-theory-paper-award/itsoc-paper-award-nomination-form> for details. Please include a statement outlining the paper's contributions.

IEEE Information Theory Society James L. Massey Research & Teaching Award for Young Scholars

The purpose of this award is to recognize outstanding achievement in research and teaching by young scholars in the Information Theory community. The award winner must be 40 years old or younger and a member of the IEEE Information Theory Society on January 1st of the year nominated.

NOMINATION PROCEDURE: Nominations and supporting materials must be submitted by **April 30, 2017**. All nominations should be submitted using the online nomination forms. Please see <http://www.itsoc.org/honors/massey-award/nomination-form> for details.

IEEE Awards

The IEEE Awards program pays tribute to technical professionals whose exceptional achievements and outstanding contributions have made a lasting impact on technology, society and the engineering profession. For information on the Awards program, and for nomination procedures, please refer to <http://www.ieee.org/portal/pages/about/awards/index.html>

Recent Publications

IEEE Transactions on Information Theory

Table of content for volumes 62(9), 62(10), 62(11).

Vol. 62(9): Sep. 2016.

	CODING THEORY	
<i>L. Wei, D. G. M. Mitchell, T. E. Fuja, and D. J. Costello, Jr.</i>	Design of Spatially Coupled LDPC Codes Over $GF(q)$ for Windowed Decoding	4781
<i>Y. Cassuto, S. Kvatinsky, and E. Yaakobi</i>	Information-Theoretic Sneak-Path Mitigation in Memristor Crossbar Arrays	4801
<i>Y. Zhang and G. Ge</i>	Snake-in-the-Box Codes for Rank Modulation under Kendall's τ -Metric in S_{2n+2}	4814
<i>D. Cullina, N. Kiyavash, and A. A. Kulkarni</i>	Restricted Composition Deletion Correcting Codes	4819
<i>C. Tian and T. Liu</i>	Multilevel Diversity Coding With Regeneration	4833
<i>J. Li and X. Tang</i>	Optimal Exact Repair Strategy for the Parity Nodes of the $(k+2, k)$ Zigzag Code	4848
<i>H.-H. Tang, C.-H. Wang, and M.-C. Lin</i>	Further Exploration of Convolutional Encoders for Unequal Error Protection and New UEP Convolutional Codes	4857
<i>A. S. Castellanos, A. M. Masuda, and L. Quoos</i>	One- and Two-Point Codes Over Kummer Extensions	4867
	SHANNON THEORY	
<i>M. Alsan and E. Telatar</i>	A Simple Proof of Polarization and Polarization for Non-Stationary Memoryless Channels	4873
<i>B. Nazer, V. R. Cadambe, V. Ntranos, and G. Caire</i>	Expanding the Compute-and-Forward Framework: Unequal Powers, Signal Levels, and Multiple Linear Combinations	4879
<i>A. Vahid and R. Calderbank</i>	Two-User Erasure Interference Channels With Local Delayed CSIT	4910
<i>M. Ashok Kumar and I. Sason</i>	Projection Theorems for the Rényi Divergence on α -Convex Sets	4924
<i>R. Kolte, A. Özgür, and H. Permuter</i>	Multicoding Schemes for Interference Channels	4936
	COMMUNICATION NETWORKS	
<i>S. L. Fong and V. Y. F. Tan</i>	Strong Converse Theorems for Classes of Multimessage Multicast Networks: A Rényi Divergence Approach	4953
<i>S. Saeedi Bidokhti, V. M. Prabhakaran, and S. N. Diggavi</i>	Capacity Results for Multicasting Nested Message Sets Over Combination Networks	4968
	GAUSSIAN NETWORKS	
<i>M. Cardone, D. Tuninetti, and R. Knopp</i>	The Two-User Causal Cognitive Interference Channel: Novel Outer Bounds and Constant Gap Result for the Symmetric Gaussian Noise Channel in Weak Interference	4993
	SECURE COMMUNICATION	
<i>W. Wang, L. Ying, and J. Zhang</i>	On the Relation Between Identifiability, Differential Privacy, and Mutual-Information Privacy	5018
	COMMUNICATIONS	
<i>A. L. Moustakas, P. Mertikopoulos, and N. Bambos</i>	Power Optimization in Random Wireless Networks	5030
<i>A. Pastore, M. Joham, and J. R. Fonollosa</i>	A Framework for Joint Design of Pilot Sequence and Linear Precoder	5059
	SOURCE CODING	
<i>M. Benammar and A. Zaidi</i>	Rate-Distortion Function for a Heegard-Berger Problem With Two Sources and Degraded Reconstruction Sets	5080
<i>I. E. Bocharova, A. Guillén i Fàbregas, B. D. Kudryashov, A. Martínez, A. Tauste Campo, and G. Vázquez-Vilar</i>	Multi-Class Source-Channel Coding	5093
<i>R.-A. Pitaval, L. Wei, O. Tirkkonen, and J. Corander</i>	Volume of Metric Balls in High-Dimensional Complex Grassmann Manifolds	5105
	SIGNAL PROCESSING AND ESTIMATION	
<i>C. A. Metzler, A. Maleki, and R. G. Baraniuk</i>	From Denoising to Compressed Sensing	5117
<i>M. E. Lopes</i>	Unknown Sparsity in Compressed Sensing: Denoising and Inference	5145
<i>M. Unser, J. Fageot, and H. Gupta</i>	Representer Theorems for Sparsity-Promoting ℓ_1 Regularization	5167
<i>M. Broniatowski and A. Decurninge</i>	Estimation for Models Defined by Conditions on Their L-Moments	5181

	BOOLEAN FUNCTIONS AND SEQUENCES	
<i>G. Gao, Y. Guo, and Y. Zhao</i>	Recent Results on Balanced Symmetric Boolean Functions	5199
<i>A. Çeşmelioglu, W. Meidl, and A. Pott</i>	There Are Infinitely Many Bent Functions for Which the Dual Is Not Bent	5204
<i>J. Bao and L. Ji</i>	New Families of Optimal Frequency Hopping Sequence Sets	5209
<i>M. Fickus, D. G. Mixon, and J. Jasper</i>	Equiangular Tight Frames From Hyperovals	5225
<i>D. J. Katz</i>	Aperiodic Crosscorrelation of Sequences Derived From Characters	5237
	QUANTUM INFORMATION THEORY	
<i>R. Duan, S. Severini, and A. Winter</i>	On Zero-Error Communication via Quantum Channels in the Presence of Noiseless Feedback	5260

Vol. 62(10): Oct. 2016.

	CODING THEORY	
<i>A. Giurgiu, N. Macris, and R. Urbanke</i>	Spatial Coupling as a Proof Technique and Three Applications	5281
<i>T. Westerbäck, R. Freij-Hollanti, T. Ernvall, and C. Hollanti</i>	On the Combinatorics of Locally Repairable Codes via Matroid Theory	5296
<i>P. Nelson and S. H. M. van Zwam</i>	The Maximum-Likelihood Decoding Threshold for Cycle Codes of Graphs	5316
<i>W. Zhou, S. Lin, and K. A. S. Abdel-Ghaffar</i>	On the Maximum True Burst-Correcting Capability of Fire Codes	5323
<i>S.-J. Lin, T. Y. Al-Naffouri, and Y. S. Han</i>	FFT Algorithm for Binary Extension Finite Fields and Its Application to Reed-Solomon Codes	5343
<i>A. Zeh and S. Ling</i>	Spectral Analysis of Quasi-Cyclic Product Codes	5359
<i>C. H. Chan and M. Xiong</i>	Construction of Partial-Unit-Memory MDS Convolutional Codes	5375
	SHANNON THEORY	
<i>Q. Chen and R. W. Yeung</i>	Partition-Symmetrical Entropy Functions	5385
<i>W. Huleihel, N. Weinberger, and N. Merhav</i>	Erasure/List Random Coding Error Exponents Are Not Universally Achievable	5403
<i>G. Han and J. Song</i>	Extensions of the I-MMSE Relationship to Gaussian Channels With Feedback and Memory	5422
<i>A. Samorodnitsky</i>	On the Entropy of a Noisy Function	5446
	SOURCE CODING	
<i>J. Østergaard, Y. Kochman, and R. Zamir</i>	Colored-Gaussian Multiple Descriptions: Spectral and Time-Domain Forms	5465
<i>A. No and T. Weissman</i>	Rateless Lossy Compression via the Extremes	5484
<i>K. Watanabe and S. Ikeda</i>	Rate-Distortion Functions for Gamma-Type Sources Under Absolute-Log Distortion Measure	5496
	COMMUNICATION NETWORKS	
<i>J. Han and C.-C. Wang</i>	General Capacity Region for the Fully Connected Three-Node Packet Erasure Network	5503
<i>K. Shanmugam, M. Ji, A. M. Tulino, J. Llorca, and A. G. Dimakis</i>	Finite-Length Analysis of Caching-Aided Coded Multicasting	5524
<i>C. Chen, S. J. Baek, and G. de Veciana</i>	Opportunistic Scheduling of Randomly Coded Multicast Transmissions at Half-Duplex Relay Stations	5538
	GAUSSIAN NETWORKS	
<i>Y. Liu and E. Erkip</i>	Capacity and Rate Regions of a Class of Broadcast Interference Channels	5556
<i>C. Wang, H. Sun, and S. A. Jafar</i>	Genie Chains: Exploring Outer Bounds on the Degrees of Freedom of MIMO Interference Networks	5573
<i>A. Gholami Davoodi and S. A. Jafar</i>	Aligned Image Sets Under Channel Uncertainty: Settling Conjectures on the Collapse of Degrees of Freedom Under Finite Precision CSIT	5603
<i>M. Ashraphijuo, A. Tajer, C. Gong, and X. Wang</i>	A Receiver-centric Approach to Interference Management: Fairness and Outage Optimization	5619
<i>M. Yemini, A. Somekh-Baruch, and A. Leshem</i>	On the Multiple Access Channel With Asynchronous Cognition	5643
<i>P. Mohapatra and C. R. Murthy</i>	On the Capacity of the Two-User Symmetric Interference Channel With Transmitter Cooperation and Secrecy Constraints	5664
	SECURE COMMUNICATION AND CRYPTOGRAPHY	
<i>F. Oggier, P. Solé, and J.-C. Belfiore</i>	Lattice Codes for the Wiretap Gaussian Channel: Construction and Analysis	5690
<i>S. C. Ramanna and P. Sarkar</i>	Efficient Adaptively Secure IBBE From the SXDH Assumption	5709

ESTIMATION, LEARNING, AND SIGNAL RECOVERY		
<i>G. C. Enss, M. Kohler, A. Krzyżak, and R. Platz</i>	Nonparametric Quantile Estimation Based on Surrogate Models	5727
<i>N. Le Bihan, F. Chatelain, and J. H. Manton</i>	Isotropic Multiple Scattering Processes on Hyperspheres	5740
<i>Z. J. Towfic, J. Chen, and A. H. Sayed</i>	Excess-Risk of Distributed Stochastic Learners	5753
<i>J. Heydari, A. Tajer, and H. V. Poor</i>	Quickest Linear Search over Correlated Sequences	5786
<i>D. Yang, G. Tang, and M. B. Wakin</i>	Super-Resolution of Complex Exponentials From Modulations With Unknown Waveforms	5809
<i>Y. Kozachenko and A. Olenko</i>	Aliasing-Truncation Errors in Sampling Approximations of Sub-Gaussian Signals	5831
<i>Z. Allen-Zhu, R. Gelashvili, and I. Razenshteyn</i>	Restricted Isometry Property for General p-Norms	5839
<i>Q. Qu, J. Sun, and J. Wright</i>	Finding a Sparse Vector in a Subspace: Linear Sparsity Using Alternating Directions	5855
<i>Y. Chen, C. Suh, and A. J. Goldsmith</i>	Information Recovery From Pairwise Measurements	5881
<i>V. Kanade, E. Mossel, and T. Schramm</i>	Global and Local Information in Clustering Labeled Block Models	5906
<i>B. Hajek, Y. Wu, and J. Xu</i>	Achieving Exact Cluster Recovery Threshold via Semidefinite Programming: Extensions	5918
QUANTUM INFORMATION THEORY		
<i>H. W. Chung, S. Guha, and L. Zheng</i>	Superadditivity of Quantum Channel Coding Rate With Finite Blocklength Joint Measurements	5938
<i>H.-C. Cheng and M.-H. Hsieh</i>	Concavity of the Auxiliary Function for Classical-Quantum Channels	5960
COMMENTS		
<i>L. Yu, H. Li, and W. Li</i>	Comments on “Approximate Characterizations for the Gaussian Source Broadcast Distortion Region”	5966

Vol. 62(11): Nov. 2016.

SHANNON THEORY		
<i>I. Sason and S. Verdú</i>	f -Divergence Inequalities	5973
<i>F. Matúš and L. Csirmaz</i>	Entropy Region and Convolution	6007
<i>C. D. Charalambous and P. A. Stavrou</i>	Directed Information on Abstract Spaces: Properties and Variational Equalities	6019
<i>I. Kontoyiannis and M. Skoularidou</i>	Estimating the Directed Information and Testing for Causality	6053
<i>Y. Han, O. Ordentlich, and O. Shayevitz</i>	Mutual Information Bounds via Adjacency Events	6068
<i>S. Satpathy and P. Cuff</i>	Secure Cascade Channel Synthesis	6081
<i>N. Cai</i>	List Decoding for Arbitrarily Varying Multiple Access Channel Revisited: List Configuration and Symmetrizability	6095
SOURCE CODING		
<i>V. Kostina and S. Verdú</i>	Nonasymptotic Noisy Lossy Source Coding	6111
<i>G. Koliander, G. Pichler, E. Riegler, and F. Hlawatsch</i>	Entropy and Source Coding for Integer-Dimensional Singular Random Variables	6124
<i>T. Koch</i>	The Shannon Lower Bound Is Asymptotically Tight	6155
<i>G. Böcherer and B. C. Geiger</i>	Optimal Quantization for Distribution Synthesis	6162
IDENTIFICATION, SECURE COMMUNICATION AND CRYPTOGRAPHY		
<i>F. Farhadzadeh and F. M. J. Willems</i>	Identification Rate, Search and Memory Complexity Tradeoff: Fundamental Limits	6173
<i>K. Kittichokechai and G. Caire</i>	Secret Key-Based Identification and Authentication With a Privacy Constraint	6189
<i>A. Agarwal and A. Mazumdar</i>	Security in Locally Repairable Storage	6204
<i>K. Huang, U. Parampalli, and M. Xian</i>	Security Concerns in Minimum Storage Cooperative Regenerating Codes	6218
<i>O. O. Koyluoglu, R. Soundararajan, and S. Vishwanath</i>	State Amplification Subject to Masking Constraints	6233
<i>D. Aggarwal and U. Maurer</i>	Breaking RSA Generically Is Equivalent to Factoring	6251
<i>C. J. Mitchell</i>	On the Security of 2-Key Triple DES	6260

CODING THEORY		
<i>P. Huang, E. Yaakobi, H. Uchikawa, and P. H. Siegel</i>	Binary Linear Locally Repairable Codes	6268
<i>S.-J. Lin, T. Y. Al-Naffouri, Y. S. Han, and W.-H. Chung</i>	Novel Polynomial Basis With Fast Fourier Transform and Its Application to Reed–Solomon Erasure Codes	6284
<i>C. Carvalho and V. G. L. Neumann</i>	The Next-to-Minimal Weights of Binary Projective Reed–Muller Codes	6300
<i>S. E. Anderson and G. L. Matthews</i>	Stopping Sets of Hermitian Codes	6304
<i>X. Wang, H. Wei, C. Shangguan, and G. Ge</i>	New Bounds and Constructions for Multiply Constant-Weight Codes	6315
<i>L. Lan, Y. Chang, and L. Wang</i>	Cyclic Constant-Weight Codes: Upper Bounds and New Optimal Constructions	6328
<i>Y. Fan and H. Liu</i>	Quasi-Cyclic Codes of Index $1\frac{1}{3}$	6342
<i>J. Borges, C. Fernández-Córdoba, and R. Ten-Valls</i>	$\mathbb{Z}_2\mathbb{Z}_4$ -Additive Cyclic Codes, Generator Polynomials, and Dual Codes	6348
<i>K. Bibak, B. M. Kapron, and V. Srinivasan</i>	The Cayley Graphs Associated With Some Quasi-Perfect Lee Codes Are Ramanujan Graphs	6355
COMMUNICATION NETWORKS		
<i>S. Unal and A. B. Wagner</i>	A Rate–Distortion Approach to Index Coding	6359
<i>S. L. Fong</i>	Cut-Set Bounds for Multimessage Multicast Networks With Independent Channels and Zero-Delay Edges	6379
<i>C.-Y. Wang, S. H. Lim, and M. Gastpar</i>	Information-Theoretic Caching: Sequential Coding for Computing	6393
<i>A. Ghorbel, M. Kobayashi, and S. Yang</i>	Content Delivery in Erasure Broadcast Channels With Cache and Feedback	6407
COMMUNICATIONS		
<i>D. Stotz and H. Bölcskei</i>	Characterizing Degrees of Freedom Through Additive Combinatorics	6423
<i>D. Shaviv, P.-M. Nguyen, and A. Özgür</i>	Capacity of the Energy-Harvesting Channel With a Finite Battery	6436
SIGNAL PROCESSING, CLASSIFICATION, AND RECOVERY		
<i>F. Renna, L. Wang, X. Yuan, J. Yang, G. Reeves, R. Calderbank, L. Carin, and M. R. D. Rodrigues</i>	Classification and Reconstruction of High-Dimensional Signals From Low-Dimensional Features in the Presence of Side Information	6459
<i>Y. Xia and S. Li</i>	Analysis Recovery With Coherent Frames and Correlated Measurements	6493
<i>L. Baldassarre, N. Bhan, V. Cevher, A. Kyrillidis, and S. Satpathi</i>	Group-Sparse Model Selection: Hardness and Relaxations	6508
<i>R. Sun and Z.-Q. Luo</i>	Guaranteed Matrix Completion via Non-Convex Factorization	6535
<i>Y. Hur and F. Zheng</i>	Prime Coset Sum: A Systematic Method for Designing Multi-D Wavelet Filter Banks With Fast Algorithms	6580
<i>T. L. Molloy and J. J. Ford</i>	Asymptotic Minimax Robust Quickest Change Detection for Dependent Stochastic Processes With Parametric Uncertainty	6594
QUANTUM INFORMATION THEORY		
<i>M.-H. Hsieh and S. Watanabe</i>	Channel Simulation and Coded Source Compression	6609
<i>S. Akibue and M. Muraö</i>	Network Coding for Distributed Quantum Computation Over Cluster and Butterfly Networks	6620
<i>T. Zhang and G. Ge</i>	Quantum Codes Derived From Certain Classes of Polynomials	6638
SEQUENCES		
<i>L. Qu</i>	A New Approach to Constructing Quadratic Pseudo-Planar Functions Over \mathbb{F}_{2^n}	6644

Foundations and Trends® in Communications and Information Theory

Volume 13, Issue 2–3:
 Multiterminal Secrecy by Public Discussion.
 by Prakash Narayan and Himanshu Tyagi.

IWCIT 2017

Iran Workshop on
Communication and Information Theory
Sharif University of Technology, Tehran, Iran

*“ There was the Door to which I found no Key, There was the Veil through which I might not see:
Some little talk awhile of Me and Thee; There was - and then no more of Thee an Me*

Omar Khayyam, Persian mathematician astronomer, philosopher, and poet.

3-4 May 2017

Call for Papers

The fifth Iran Workshop on Communication and Information Theory will take place at Sharif University of Technology, on May 3rd and May 4th 2017, Tehran, Iran. Interested authors are encouraged to submit their original and previously unpublished contributions to the following fields. This conference highly appreciates interdisciplinary related research not necessarily included below.

Shannon Theory

- Complexity theory
- Information theoretic security
- Multi-terminal information theory
- Quantum information theory

Communication Theory

- Cognitive radio systems
- Cooperative communications
- Network resource sharing and scheduling
- Molecular and Nano communications
- Optical and Quantum communication theory

Coding Theory

- Compressed sensing
- Data compression
- Network coding

Applications of Information Theory

- Information theoretic learning
- Information theory and data mining
- Information theory and signal processing
- Information theory and statistics
- Information theory in biology
- Information theory in networks
- Information theory in practice

Important Dates:

- Paper Submission:
January 11th, 2017
- Notification of Acceptance:
March 15th, 2017
- Camera Ready Submission:
April 15th, 2017

General Chairs:

- Aref, M. R.

Sharif University of Technology

- Salehi, J. A.

Sharif University of Technology

Technical Program Chair:

- Sharafat, A. R.

Tarbiat Modares University

Executive Chairs:

- Gohari, A.

Sharif University of Technology

- Seyfe, B.

Shahed University



IEEE
IRAN SECTION

Contact Us :

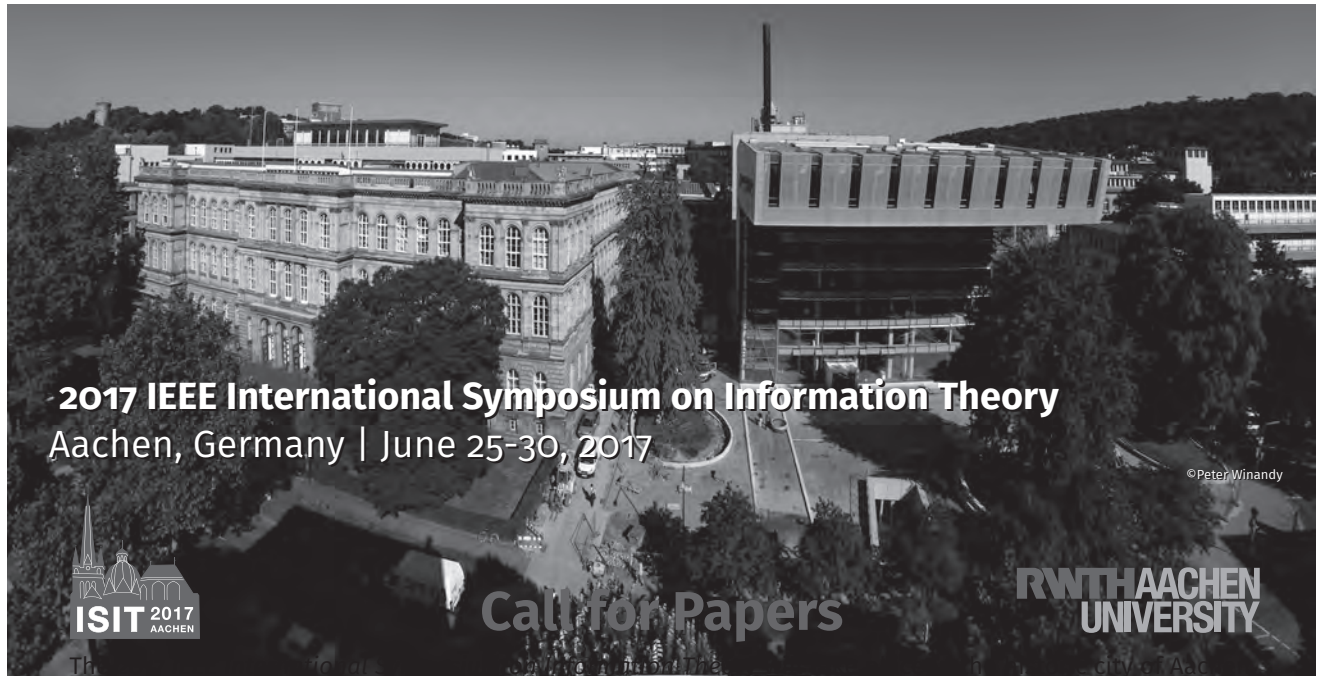
• Emails:

iwcit@sharif.ir

• Address:

Secretariat of IWCIT 2017 Rom 503 Dept. of Electrical Engineering
Sharif University of Technology Tehran, Iran
Tel : +98 21 66165910

WWW . IWCIT . COM



Germany, from June 25 to 30, 2017.

Interested authors are encouraged to submit previously unpublished contributions from a broad range of topics related to information theory, including but not limited to the following areas:

Topics

- ▶ Big Data Analytics
- ▶ Coding for Communication and Storage
- ▶ Coding Theory
- ▶ Communication Theory
- ▶ Complexity and Computation Theory
- ▶ Compressed Sensing and Sparsity
- ▶ Cryptography and Security
- ▶ Detection and Estimation
- ▶ Emerging Applications of IT
- ▶ Information Theory and Statistics
- ▶ Information Theory in Biology
- ▶ Network Coding and Applications
- ▶ Network Information Theory
- ▶ Optical Communication
- ▶ Pattern Recognition and Machine Learning
- ▶ Physical Layer Security
- ▶ Quantum Information and Coding Theory
- ▶ Shannon Theory
- ▶ Signal Processing
- ▶ Source Coding and Data Compression
- ▶ Wireless Communication and Networks

Researchers working in emerging fields of information theory or on novel applications of information theory are especially encouraged to submit original findings.

The submitted work and the published version are limited to 5 pages in the standard IEEE conference format. Submitted papers should be of sufficient detail to allow for review by experts in the field. If full proofs cannot be accommodated due to space limitations, authors are encouraged to post a publicly accessible complete paper elsewhere and to provide a specific reference. Authors should refrain from submitting multiple papers on the same topic.

Information about when and where papers can be submitted will be posted on the conference web page. The paper submission deadline is January 16, 2017, at 11:59 PM, Eastern Time (New York, USA). Acceptance notifications will be sent out by March 31, 2017.

We look forward to your participation in ISIT 2017.

General Co-Chairs
Rudolf Mathar
Gerhard Kramer

TPC Co-Chairs
Sennur Ulukus
Stephen Hanly
Martin Bossert
Stephan ten Brink

Finance
Meik Dörpinghaus
Volker Schanz

Publications
Giuseppe Durisi
Christoph Studer

5TH INTERNATIONAL CASTLE MEETING ON CODING THEORY AND APPLICATIONS

PRELIMINARY CALL FOR PAPERS



This is the first announcement of the Fifth International Castle Meeting on Coding Theory and Applications (5ICMCTA), which will take place in Vihula Manor, Estonia, from Monday, August 28th, to Thursday, August 31st, 2017. Information about the 5ICMCTA can be found at <http://www.castle-meeting-2017.ut.ee/> .

We solicit submissions of previously unpublished contributions related to coding theory, including but not limited to the following areas: *Codes and combinatorial structures, Algebraic-geometric codes, Network coding, Codes for storage, Quantum codes, Convolutional codes, Codes on graphs, Iterative decoding, Coding applications to cryptography and security, Other applications of coding theory.*

Organization:

General chair: *Vitaly Skachek*

Scientific Committee co-chairs: *Ángela Barbero* and *Øyvind Ytrehus*

Publicity: *Yauhen Yakimenka*

Scientific Committee

Alexander Barg • Irina Bocharova • Eimear Byrne • Joan-Josep Climent • Gerard Cohen • Olav Geil • Marcus Greferath • Tor Hellesteth • Tom Høholdt • Camilla Hollanti • Kees S. Immink • Frank Kschischang • Boris Kudryashov • San Ling • Daniel Lucani • Gary McGuire • Sihem Mesnager • Muriel Médard • Diego Napp • Frederique Oggier • Patric Östergard • Raquel Pinto • Paula Rocha • Joachim Rosenthal • Eirik Rosnes • Moshe Schwartz • Vladimir Sidorenko • Patrick Sole • Leo Storme • Rüdiger Urbanke • Pascal Vontobel • Dejan Vukobratovic • Jos Weber • Gilles Zémor

Important dates:

Paper submission:	May 1, 2017
Notification of decision:	June 12, 2017
Final version paper submission:	July 3, 2017

Call-for-Papers
IEEE Transactions on Information Theory
 Special Issue on
**Shift-Register Sequences, Codes and Cryptography in Memory of
 Solomon W. Golomb**

A special issue of the IEEE Transactions on Information Theory is devoted in memory of Solomon W. Golomb for his revolutionary work on shift-register sequences, coding theory, and cryptography as well as their applications to communications.

The scope of the special issue encompasses all aspects of shift-register sequences, coding, cryptography, combinatorics and games, and their applications to communications. Original research papers are sought in those areas, and a few invited expository and survey papers related to Solomon Golomb's work are intended. The expected publication date will be by the beginning of 2018.

The topics of interest include but are not limited to:

- Nonlinear and linear feedback shift register sequences
- Periodic or aperiodic correlation and linear complexity
- Error correcting codes
- Symmetric cryptography
- Puzzles and games with an information-theoretic flavor
- Information theory and genome-related applications
- Pseudorandomness
- Sequences for wireless communication and radar
- Aspects of finite fields, combinatorics, and exponential sums related to sequences

Important Dates:

Manuscript submission: May 31, 2017

Completion of first round of reviews: September 30, 2017

Revised manuscript submission: October 31, 2017

Notification of final decision: November 30, 2017

Final manuscript submission: December 31, 2017

All submissions to the Special Issue should be made online through the usual submission site (<https://mc.manuscriptcentral.com/t-it>) and must include a cover letter that directs the paper to the Special Issue.

Guest Editors

Guang Gong, University of Waterloo, Canada

Tor Hellesteth, University of Bergen, Norway

Vijay Kumar, Indian Institute of Science, India

All enquiries about the special issue should be sent to: ggong@uwaterloo.ca.

Conference Calendar

DATE	CONFERENCE	LOCATION	WEB PAGE	DUE DATE
December 4–8, 2016	IEEE GLOBECOM.	Washington DC, USA	http://globecom2016.ieee-globecom.org/	Passed
December 4, 2016	Workshop on Network Coding and Applications (IEEE Globcom NetCod 2016).	Washington DC, USA	http://www.netcod16.org/	Passed
December 4–8, 2016	Signal Processing for Big Data in Wireless Network (Globcom'16 workshop).	Washington DC, USA	http://comp.uark.edu/~wuj/spbd	Passed
December 7–9, 2016	IEEE Global Conference on Signal and Information Processing (GlobalSIP). Symposium on Information Theoretic Approaches to Security and Privacy.	Washington DC, USA	http://www.ieeeglobalsip.org/	Passed
January 16–19, 2017	SIAM: ACM-SIAM Symposium on Discrete Algorithms (SODA).	Barcelona, Spain	https://www.siam.org/meetings/da17/	Passed
March 19–22, 2017	IEEE Wireless Communications and Networking Conference (WCNC).	San Francisco, CA	http://wcnc2017.ieee-wcnc.org/	Passed
March 22–24, 2017	Conference on Information Sciences and Systems (CISS).	Baltimore, Maryland	http://ciss.jhu.edu/	Dec. 11, 2016
May 8–11, 2017	2017 European School of Information Theory (ESIT).			
May 3–4, 2017	Iran Workshop on Communication and Information Theory (IWCIT).	Teheran, Iran	http://www.iwcit.ir/	January 11, 2017
May 8–11, 2017	European School of Information Theory (ESIT).	Madrid, Spain	http://www.itsoc.org/conferences/schools/european-school-2017	
May 15–19, 2017	International Symposium on Modeling and Optimization of Mobile, Ad-Hoc, and Wireless Networks (WiOpt).	Telecom, Paris, Spain	wiopt.telecom-paristech.fr	Dec. 22, 2016
May 21–25, 2017	IEEE International Conference on Communications (ICC).	Paris, France	icc2017.ieee-icc.org	Passed
June 25–30, 2017	IEEE International Symposium on Information Theory (ISIT).	Aachen, Germany	http://www.isit2017.org	January 16, 2017
August 28–31, 2017	5th International Castle Meeting on Coding Theory and Applications (5ICMCTA).	Vihula Manor, Estonia	http://www.castle-meeting-2017.ut.ee/	May 1, 2017

Major COMSOC conferences: <http://www.comsoc.org/confs/index.html>