IEEE Information Theory Society Newsletter

Vol. 65, No. 3, September 2015 Editor: Michael Langberg ISSN 1059-2362

Editorial committee: Frank Kschischang, Giuseppe Caire, Meir Feder, Tracey Ho, Joerg Kliewer, Anand Sarwate, Andy Singer, and Sergio Verdú

President's Column

Michelle Effros

It is the middle of July as I sit down to write this column. With one school year over and another not yet begun, it is a good time to reflect on recent events and look forward to those to come.

The Board of Governors held its annual meeting in early June. Nominations made at that meeting led to elections for the 2016 President, First Vice President, and Second Vice President. The Board chose Alon Orlitsky, Ruediger Urbanke, and Elza Erkip to hold those posts. Please join me in congratulating and thanking them for taking on these important leadership roles. The election for incoming members of the Board, also nominated at that meeting, is now underway.

Another major objective of the ISIT Board meeting was to choose future locations for the International Symposium on Information Theory (ISIT). This year, colleagues from around the world presented bids for ISIT 2018 and 2019. With five exceptionally strong bids, competition was fierce. The Board chose Vail, Colorado, and Paris, France, as the sites for ISIT 2018 and ISIT 2019, respectively.

Reports were given by many of the Society's committees. The Online Committee proposed a major update to the IT Society webpage; the Committee secured funds to begin this work from both the Society and from an IEEE fund for Special Initiatives. The ISIT Schools Sub-Committee of the Membership Committee sought and secured funds for the 2016 North American and Australian Information Theory Summer Schools, to be held at Duke University in Durham, North Carolina, and Monash University in Melbourne, Australia, respectively. The Broader Outreach Committee described the emerging details of events related to the 2016 Shannon centenary. These include both a proposal to create a documentary about Shannon's life and work and efforts currently underway to help fuel public Shannon Day events around the world.

ISIT 2015 followed immediately after the Board of Governor's meeting. For me, ISIT is an annual treat. We catch up with old friends, hear about recent advances, and have the conversations that will surprise us, intrigue us, fuel new questions, and—perhaps—spur us to new solutions. Thanks to the organizing committee, this year's conference, held in Hong Kong, ran without a hitch. Highlights included a welcome reception with a spectacular view of the city, a magnificent floating banquet in Aberdeen Harbour, an array of fascinating plenary talks, and Rob Calderbank's Shannon Lecture. At the Awards Lunch, the community celebrated both technical contributions and service. This year's Chapter of the Year Award went to our local hosts from the IEEE Hong Kong Chapter of the Information Theory Society for their "consistent promotion of information theory education and research." A representative from IEEE presented two Technical Field Awards: the IEEE Eric E. Sumner Award to Sanjoy Mitter and the IEEE Leon K. Kirchmayer Graduate Teaching Award to Dan Costello. The second annual Thomas M. Cover Dissertation Award was received by Adel Javanmard for his thesis "Inference and Estimation in High-dimensional Data Analysis." The 2014 Jack Keil Wolf ISIT Student Paper Awards, announced at ISIT 2014 and delivered at ISIT 2015, went to Artyom Sharov for the paper "New Upper Bounds for Grain-Correcting and Grain Detecting Codes" and to Christoph Bunte for the paper "A Proof of the Ahlswede-Cai-Zhang Conjecture." The 2015 Communications and Information Society Joint Paper Award went to the 2012 paper "Completely Stale Transmitter Channel State Information is Still Very Useful" by Mohammad Ali Maddah-Ali and David Tse. The 2014 IT Society Paper Award, announced at ISIT 2014 and awarded at ISIT 2015, went to Marco Dalai for the 2012 paper "Lower Bounds on the Probability

continued on page 28

From the Editor

Michael Langberg

Dear colleagues,

As the summer comes to an end I hope you will find this fall newsletter both stimulating and informative. I would like to start by joining our society President Michelle Effros in congratulating our fellow colleagues for their outstanding research accomplishments and service recognized by our own and other IEEE societies. A number of additional awards (granted recently) appear in the body of the newsletter.

This issue is packed with several excellent contributions. Following recent efforts in our community to reach out and influence societies beyond on own, we are glad to have an intriguing article by M. Braverman, R. Oshman, and O. Weinstein on the connections between information theory and communication complexity. The article summarizes the tutorial "Information and Communication Complexity" given at the recent ISIT in Hong Kong. Also from ISIT, we are delighted to include the details from the plenary talk "Something Old, Something New, Something Borrowed, and Something Proved" prepared by S. Kudekar, S. Kumar, M. Mondelli, H. D. Pfister, E. Sasoglu, and R. Urbanke. The article presents a beautiful proof for the performance of Reed-Muller codes on the Binary Erasure Channel, with an elegant combination of ideas from coding theory and the theory of Boolean functions. We conclude our technical contributions with an implementation of Fourier-Motzkin elimination for information theoretic inequalities by I. B. Gattegno Z. Goldfeld and H. H. Permuter. The open source implementation enhances the standard techniques by adding Shannon-type inequalities to the simplification process.

In addition to the excellent and ongoing contributions of Tony Ephremides and Sol Golomb that we all eagerly anticipate, this issue includes two new initiatives that we hope to feature regularly. The first is a student column lead by the IT student subcommittee Deniz Gündüz, Osvaldo Simeone, Jonathan Scarlett and edited by Parham Noorzad. The column is an attempt to bring forward contributions "by students—for students" (and students at heart). This issue includes an initial call for contributions encouraging students to share their experiences and perspective on our community. The second is a column reporting from our chapters "in the field" on exciting local events and initiatives. The first offering is from the members of the IEEE Hong Kong Section Chapter (Chee Wei Tan, Lin Dai, and Kenneth Shum) which received the 2015 IEEE Information Theory Society Chapter Award.

The body of this issue also includes several reports and announcements. Christina Fragouli, Michelle Effros, Lav Varshney, and Ruediger Urbanke are kicking

continued on page 30

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.

Table of Contents

Awards

Syed Jafar, Professor of Electrical Engineering and Computer Science, University of California, Irvine, has received the **2015 Blavatnik National Award for Young Scientists.**

The Award, given annually by the Blavatnik Family Foundation and administered by the New York Academy of Sciences, honors the nation's most exceptional young scientists and engineers, celebrating their extraordinary achievements and recognizing their outstanding promise while providing an unparalleled prize of $250,000 to each National Laureate. The prize is the largest unrestricted cash award given to early career scientists.

Dr. Jafar was selected for his discoveries in interference alignment in wireless networks, changing the field's thinking about how these networks should be designed.

"Syed Jafar revolutionized our understanding of the capacity limits of wireless networks. He demonstrated the astounding result that each user in a wireless network can access half of the spectrum without interference from other users, regardless of how many users are sharing the spectrum. This is a truly remarkable result that has a tremendous impact on both information theory and the design of wireless networks." – Dr. Paul Horn, Senior Vice Provost for Research, New York University and a member of the 2015 National Jury.

Vijay Bhargava of the University of British Columbia in Vancouver, Canada was the recipient of the 2015 **Killam Prize in Engineering by Canada Council for the Arts**, presented by His Excellency the Right Honourable David Johnston, Governor General of Canada at the Rideau Hall on May 12, 2015. At the ceremony Vijay was introduced by Frank Kschischang (2010 President of the IEEE Information Theory Society). The Killam prizes are administered by the Canada Council of the Arts and are funded by a private endowment supporting creativity and innovation. Vijay received $100,000 in recognition of his exceptional career achievements in engineering.

Vijay has also received a Humboldt Research Award from the Alexander von Humboldt Foundation and will spend the 2015–2016 academic year cooperating on research projects with Robert Schober of the Friedrich-Alexander-Universitat Erlangen-Nurnberg.

Vijay Bhargava was President of the IEEE Information Theory Society during 2000 and of the IEEE Communications Society during 2012–2013.

Vijay Bhargava: Rideau Hall

The 2016 IEEE Technical Field Award Recipients:

Among the recipients of 2016 IEEE Technical Field Awards were several members of the Information Theory community.

The **IEEE Eric. E. Sumner Award** recognizes outstanding contributions to communications technology. The 2016 co-recipients are **SHUO-YEN ROBERT LI**, Professor, Chinese University of Hong Kong, **RAYMOND W. YEUNG**, Professor, Chinese University of Hong Kong, and **NING CAI**, Professor, Xidian University, "for pioneering contributions to the field of network coding."

The **IEEE Koji Kobayashi Computers and Communication Award** recognizes outstanding contributions to the integration of computers and communications. The 2016 recipient is **LEANDROS TASSIULAS**, Professor, Yale University, "for contributions to the scheduling and stability analysis of networks."

The **IEEE James L. Flanagan Speech and Audio Processing Award** recognizes outstanding contribution to the advancement of speech and/or audio signal processing. The 2016 recipient is **TAKEHIRO MORIYA**, Head of Moriya Research Lab, Atsugi, Kanagawa, Japan, "for contributions to speech and audio coding algorithms and standardization."

Congratulations to the award recipients!

Information and Communication Complexity

ISIT 2015 Tutorial

Mark Braverman, Rotem Oshman†, and Omri Weinstein‡*
July 26, 2015

Abstract

The study of interactive communication (known as communication complexity in the computer science literature) is one of the most important and successful tools for obtaining unconditional lower bounds in computational complexity. Despite its natural connection to classical communication theory, the usage of information theoretic techniques is relatively new within the study of interactive communication complexity. Their development is relatively recent and very much an ongoing project.

This survey provides a brief introduction to information complexity — which can be viewed as the two-party interactive extension of Shannon's classical information theoretic notions. We highlight some of its connections to communication complexity, and the fascinating problem of compressing interactive protocols to which the study of information complexity naturally leads.

*Department of Computer Science, Princeton University. Supported in part by an NSF CAREER award (CCF-1149888), a Packard Fellowship in Science and Engineering, and the Simons Collaboration on Algorithms and Geometry.

†Department of Computer Science, Tel Aviv University. Supported by the I-CORE Program of the Planning and Budgeting Committee and the Israel Science Foundation, Grant No. 4/11.

‡Department of Computer Science, Courant Institute, New York University. Supported by a Simons Society Junior Fellowship and a Siebel Scholarship.

1 Introduction

The main goal of computational complexity theory is mapping out the computational hardness of problems on different computational models. In the last 45+ years it has achieved remarkable success in understanding the *relative* hardness of problems. For example, using concepts such as **NP**-completeness and polynomial-time reductions between problems, one can identify a large class of "**NP**-complete" problems which are all roughly of the same computational difficulty. This classification effort has been quite productive, leading to a rich "complexity zoo" of problem classes.

One of the key challenges to the field has been the difficultly of obtaining *absolute* (unconditional) results about the computational hardness of problems. For example, an **NP**-complete problem is known to be computationally hard *assuming* **P**≠**NP**. However, proving that **P**≠**NP** and many other unconditional separation results currently appears to be out of reach. With some notable exceptions, even today, the unconditional separation results we have rely on the same diagonalization technique of Cantor which Turing used in his original 1936 paper to show that the Halting Problem is undecidable. This contrasts sharply with the state of affairs in the field of one-way communication, where results dating back to Shannon not only establish the asymptotic cost of various transmission problems, but even allow one to compute the leading constant (and sometimes more) in the transmis-

sion cost of various problems.

Communication complexity studies the amount of communication resources two or more parties with a distributed input need to utilize in order to compute a function that jointly depends on their inputs. In this note we will focus on the two-party setting. There are two parties (traditionally named Alice and Bob), Alice is given an input x and Bob is given an input y. Their goal is to compute a function $f(x, y)$.[1] They communicate by sending messages back and forth — formalized by a notion of a *communication protocol*. Communication is assumed to be over a noiseless[2] binary channel.

The situation in communication complexity is somewhere between that of computational complexity and that of one-way communication. Since its introduction [Yao79], several techniques have been developed to obtain *unconditional* (often tight) bounds on the communication complexity of problems. Surveys on these techniques include [KN97, LS]. These techniques are typically less tight than the ones made possible by Shannon's theory in one-way communication. Still, unconditional lower bounds in communication complexity yield a key method for obtaining unconditional lower bounds in other models of computation. These include VLSI chip design, data structures, mechanism design, property testing and streaming algorithms [Wac90, PW10, DN11, BBM12]. Developing new tools in communication complexity is a promising approach for making progress within computational complexity, and in particular, for proving strong circuit lower bounds that appear, in principle, within reach — such as Karchmer-Wigderson games [KW88] and $\mathbf{ACC}^0$ lower bounds [BT91].

[1] More generally, they may need to perform a task $T(x, y)$ that is not necessary a function; for example, producing a sample from a distribution $\mu_{x,y}$.

[2] Communication complexity over noisy channels has been receiving much attention in recent years in the TCS community, we will return to discussing it in the Open Problems section.

Disjointness and Equality. Two of the most studied functions in the context of communication complexity are the Disjointness and Equality functions. In both cases, the inputs $x, y \in \{0,1\}^k$ are two binary strings. In the case of the Equality function EQ_k, Alice and Bob would like to know whether $x = y$. In the case of the Disjointness function $DISJ_k$, the strings are viewed as representing subsets of $\{1, \ldots, k\}$, and Alice and Bob would like to know whether they have an element in common. In other words, $DISJ_k(x, y) = 0$ iff there is an index i such that $x_i = y_i = 1$. Note that in both cases the output of the problem is a single bit: while the instance size increases with k, the output size remains constant at 1. Therefore, in contrast with data transmission problems, simple information-theoretic considerations yield no non-trivial bounds in this case.

It is not hard to show [KN97] that if Alice and Bob are required to solve either problem correctly with probability 1, then the best they can do is for Alice to send x to Bob, and for Bob to send the value of the function to Alice (or vice-versa). Thus the tight communication complexity bound is $k + 1$ bits. What if a small probability of error (e.g. $1/k$) is allowed? By comparing random hashes of x and y Alice and Bob can compute $EQ_k(x, y)$ correctly with high probability using only $O(\log k)$ communication (indeed, this is how the distributed equality problem is solved in practice). On the other hand, one of the early successes of communication complexity was proving that solving $DISJ_k$ requires $\Omega(k)$ bits of communication even if a constant (say, 1/3) probability of error is allowed [KS92, Raz92].

Streaming lower bounds. A simple but instructive example is in applying communication complexity lower bounds to the study of the *streaming model* of computation [BYJKS04]. The streaming model studies a scenario where a large data stream x of length N is being processed by a unit which only has $m \ll N$ bits of memory. The goal is to compute (or ap-

proximate) a function $f(x)$ — for example, 'the number of distinct elements in x'. This models, for example, a router that attempts to maintain statistics on the packets being routed through it.

How does communication complexity enter the picture? Split the stream x into two parts x_1 and x_2 of length $N/2$ each, and let $f(x_1, x_2) := f(x_1 \circ x_2)$. Then if $f(x)$ can be computed in the streaming model, then Alice and Bob can compute $f(x_1, x_2)$ using only a single m-bit message: Alice will execute the streaming computation on x_1 and then "pass the torch" to allow Bob to continue of x_2. Passing control from Alice to Bob requires Alice to send Bob the content of the memory, which takes m bits. Note that if one extends the model to allow k passes over the data, the reduction is still meaningful and leads to $f(x_1, x_2)$ being computable using $2km$ bits of communication. For example, if the function $f(x)$ is the answer to the question "are all the elements in x distinct?", then it is not hard to see that $f(x_1, x_2)$ solves $DISJ_{N/2}$, and therefore one must have $km = \Omega(N)$.

Information complexity and its connection to communication complexity. Shannon's information theory has been the primary tool for analyzing communication problems in the simpler (one-way) data transmission problems for over 60 years [Sha48]. Indeed, Shannon's noiseless coding theorem revealed the tight connection between communication and information, namely, that the amortized description length of a random one-way message (M) is equivalent to the amount of information it contains

$$\lim_{n\to\infty} \frac{C(M^n)}{n} = H(M), \tag{1}$$

where M^n denotes n i.i.d observations from M, C is the minimum number of bits of a string from which M^n can be recovered (w.h.p), and $H(\cdot)$ is Shannon's entropy function. In the 65 years that elapsed since then, information theory has been widely applied and developed, and has become the primary mathematical tool for analyzing communication problems.

For a given function f and a distribution μ of inputs, let $\mathsf{D}_\mu(f, \varepsilon)$ denote the (worst-case) number of bits Alice and Bob need to exchange to compute $f(x, y)$ with probability $\geq 1 - \varepsilon$. Here the letter D stands for "distributional" communication complexity.[3] Furthermore, by analogy to $C(M^n)$, we can denote by $\mathsf{D}_{\mu^n}(f^n, \varepsilon)$ the communication complexity of computing n independent copies of f, where each copy is distributed according to μ and Alice and Bob are required to be correct with probability $\geq 1 - \varepsilon$ *on each copy*.

Even though much of communication complexity is about the single shot cost of the function f, the quantity $\mathsf{D}_{\mu^n}(f^n, \varepsilon)$ has received a fair amount of attention, since many problems can be decomposed into smaller pieces, and thus represented as f^n for an appropriately chosen f. Of particular interest has been the *direct sum problem*: understanding the relationship between $\mathsf{D}_{\mu^n}(f^n, \varepsilon)$ and $\mathsf{D}_\mu(f, \varepsilon)$. It is clear that $\mathsf{D}_{\mu^n}(f^n, \varepsilon) \leq n \cdot \mathsf{D}_\mu(f, \varepsilon)$, but what can be said in the opposite direction?

Following equation (1), we can define the information complexity of f as

$$\mathsf{IC}_\mu(f, \varepsilon) := \lim_{n\to\infty} \frac{\mathsf{D}_{\mu^n}(f^n, \varepsilon)}{n}. \tag{2}$$

The limit in (2) exists by a simple sub-additivity argument. As it turns out by the "Information = Amortized Communication" theorem [BR11, MI11], the quantity $\mathsf{IC}_\mu(f, \varepsilon)$ can be characterized directly as the smallest *amount of information about their inputs* Alice and Bob need to exchange to solve a *single copy* of f with probability $\geq 1 - \varepsilon$:

$$\mathsf{IC}_\mu(f, \varepsilon) = \inf_{\substack{\pi \text{ a protocol} \\ \text{solving } f \\ \text{w.p. } \geq 1-\varepsilon}} I(\Pi; Y|X) + I(\Pi; X|Y). \tag{3}$$

[3] As discussed below, one can also talk about *randomized* or "worst case" communication complexity, where Alice and Bob are required to output the correct value of $f(x, y)$ with probability $\geq 1 - \varepsilon$ on each input pair. The two notions are closely related by a minimax argument.

Here $(X, Y) \sim \mu$ are the random variables representing the inputs (x, y), and Π is the random variable representing the transcript of the protocol π. Thus, for example, $I(\Pi; Y|X)$ represents the amount of information the protocol teaches Alice (who knows x) about Bob's input y.

The right-hand-side of (3) can be viewed from a completely different angle motivated by security. Alice and Bob do not trust each other but wish to compute a function $f(x, y)$ of their inputs. A famous toy example is the "Two Millionaires" problem [Yao82] where x and y represent the players' net worth, and their goal is to evaluate whether $x < y$ without revealing any additional information to each other. In the context of information-theoretic security (as opposed to cryptographic security, where one makes assumptions about the players' computational capacity), expression (3) represents the smallest amount of information Alice and Bob must reveal to each other to solve the problem. In fact, to the best of our knowledge, the first time the expression in (3) has been written in the context of theoretical computer science, was in this security context [BYCKO93, Kla04]. For three or more parties there are information-theoretically secure protocols that reveal nothing to the participants except for the value of the function being computed [BOGW88], but this is almost never the case in the two-party setting [Kus92].

An important observation is that the inf in (3) is essential: the limit value might not be realizable by any finite protocol. In fact, this is not an obscure possibility: this is already the case for the two bit AND function where $x, y \in \{0, 1\}$ and $f(x, y) = x \wedge y$.

Exact communication complexity bounds. One of the most impressive features of Shannon's information theory is its ability to give precise answers to questions surrounding the communication cost of transmission problems. For example, a stream of n uniformly distributed symbols $X_i \in_U \{1, \ldots, 5\}$ would cost Alice $H(X_i) \cdot n + o(n) = (\log_2 5)n + o(n)$ bits to transmit. Moreover, her success probability will be exponentially small if she attempts to use an asymptotically smaller number of bits. Moreover, if we suppose that Bob has a stream of uniform inputs $Y_i \in_U \{1, \ldots, 5\} \setminus \{X_i\}$, then we can still estimate the transmission cost at $H(X_i|Y_i) \cdot n + o(n) = 2n + o(n)$. Can the same level of precision be attained for two-way communication problems? As discussed above, the communication complexity of equality EQ_k with a small error scales as $o(k)$, but can we find the constant in front of k in the communication complexity of $DISJ_k$ (as a function of the input distribution)?

Note that unlike the transmission problems we have just mentioned, $DISJ_k$ looks like a single instance of a problem and not like a "stream" of instances. In particular, its output consists of a single bit and not of k bits. As a warmup, consider the related *Set Intersection* problem INT_k, where the inputs $x, y \in \{0, 1\}^k$ still represent subsets of $\{1, \ldots, k\}$, but now Alice and Bob wish to output the intersection of $x \cap y$. In other words, Alice and Bob wish to compute the bit-wise AND of their inputs. In the zero-error regime, the expected communication complexity of this problem behaves as $(\log_2 3) \cdot k \pm o(k)$ [AC94]. When an error $\varepsilon > 0$ (going down to 0 with k — not too fast so that $\varepsilon > 2^{-o(k)}$), the communication complexity of the problem with respect to the worst possible distribution is still at least k (because of the case when $x = 1 \ldots 1$, forcing Bob to send Alice his input), but could potentially be smaller than $(\log_2 3) \cdot k \approx 1.585 \cdot k$. Let us denote it by $C_{INT} \cdot k$, where $C_{INT} \in [1, \log_2 3]$ is a constant we need to find out.

Since INT_k is just k instances of the two bit AND function, the connection given by Theorem (3), with a little bit of work yields:

$$C_{INT} = \max_{\mu} \mathsf{IC}_{\mu}(AND, 0), \qquad (4)$$

where the maximum is taken over all distributions over $\{0, 1\} \times \{0, 1\}$. Unfortunately, the formula (3) does not immediately allow one to

compute the limit in (2), since the range of the inf is not finite: even for as simple a function as the two-bit AND the space of possible interactive protocols is infinite! The intuitive explanation for this fact (made more concrete in the next subsection) is that obtaining the information-optimal protocol requires the parties to reveal information very slowly, in a very careful manner, thus utilizing an arbitrarily large number of rounds. In fact, only recently the information complexity $\mathsf{IC}_\mu(f,0)$ has been shown to be computable from the truth table of f and a description of μ [BS15].

Fortunately, in the specific case of the two-bit AND function one can guess the optimal protocol π^*, and then use the properties of the function $\Psi(\mu) := \mathsf{IC}_\mu(AND,0)$ on the space of distributions μ to prove the optimality of π^*. As mentioned earlier, π^* is not in fact a protocol, but it can be approximated by a family of protocols $\{\pi^r\}_{r=2}^\infty$, where π^r has r rounds. It can be shown that the inherent loss in this case of using an r-round protocol vanishes with r at a rate of $\Theta(1/r^2)$.

A brief description of π^* [BGPW13]. Next, let us sketch the optimal protocol π^* for computing $AND(x,y)$ with 0-error for any given distribution $(x,y) \sim \mu$ on $\{0,1\}\times\{0,1\}$. For convenience, we will assume that the distribution μ is *symmetric*, i.e., $\mu(x=0) = \mu(y=0)$ (otherwise, the player that is more likely to have a 0 can send a (noisy) signal which will either finish the execution with the output "$x \wedge y = 0$" or symmetrize the resulting posterior distribution).

The protocol π^* proceeds as follows: Each player holds a private number (R_A and R_B respectively). If $x = 1$, Alice sets R_A to "1", and otherwise ($x = 0$), she sets R_A to be a *uniformly random number* in the interval $[0,1]$ (chosen using her *private* randomness, to which Bob has no access!). Bob sets R_B symmetrically according to the value of his input y. The protocol proceeds by incrementing, using shared *public randomness*, a continuous[4] "counter" C, starting at "0" and rising to "1"; The protocol terminates when one of the players declares that the counter has reached his private number (i.e., when $C = \min\{R_A, R_B\}$). The players output "1" iff $C = 1$.

Clearly, this protocol has 0-error for computing $AND(x,y)$, since the output of the protocol is "1" iff $\min\{R_A, R_B\} = 1$, exactly whenever $x = y = 1$. Why does π^* intuitively have low information cost? Since the protocol is 0-error, it is not hard to see that at least one of the players must learn the other player's input value. If one of the players (say Alice) has a "1", it is inevitable that she will learn y, since in this case $y = x \wedge y$. Thus the goal of a low-information protocol is to reveal as little information as possible to Alice whenever she has a "0". In this case, we want to take advantage of the fact that it is possible that the players learn that Alice has a "0", but Alice is left with some uncertainty about the value of y. Indeed, if the protocol terminates at time $R_A < 1$, then Bob learns that $x \wedge y = x = 0$. At the same time, while Alice's posterior is more inclined towards $y = 1$ (since she learns that $R_B \notin [0, R_A)$), she is left with quite a bit of entropy in $H(Y|R_B > R_A)$. A rigorous analysis proves that this amount is indeed optimal.

By maximizing $I(\Pi^*;Y|X) + I(\Pi^*;X|Y)$ over all possible priors μ, by (4) one obtains that $C_{INT} \approx 1.4922 < \log_2 3$.

From intersection to disjointness. The analysis above relied on the fact that the set intersection function INT_k is a k-output function structured as a k-wise repetition of the 2-bit AND. It is not immediately apparent whether the discussion is helpful in computing C_{DISJ} such that the communication complex-

[4] Technically, this step can be implemented only in the limit, since an infinite amount of interaction would be needed. As mentioned in the earlier paragraph, this step can be approximated arbitrarily well by an r-round protocol using a natural discretization process, by having discrete increments of the "counter".

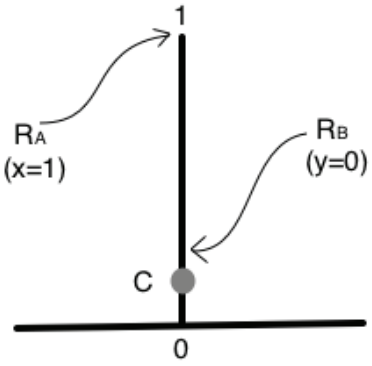


Figure 1: An illustration of the protocol π^* where Alice has input "1" and Bob has input "0". The counter C is depicted in grey. The protocol will terminate when C reaches R_B.

ity of $DISJ_k$ with respect to the worst possible distribution is $C_{DISJ} \cdot k \pm o(k)$. Note that $C_{DISJ} \in (0, 1]$, since it is known that the communication complexity of $DISJ_k$ is linear in k, and it is at most $k + 1$ by the trivial protocol.

The function $DISJ_k$ still looks like a k-wise repetition of the two-bit AND, except Alice and Bob only want to find out whether *one* of the ANDs outputs "1". If there are many coordinates on which the value of the AND is 1 (i.e. if the sets have a large intersection), then this would be a very easy instance of $DISJ_k$ (Alice and Bob will find an intersection by looking at a subsample of the coordinates). Therefore, the hard instances of $DISJ_k$ are ones where the probability that $x_i \wedge y_i = 1$ is very small. Using an analysis similar to [BYJKS04] one obtains that an equation analogous to (4) holds:

$$C_{DISJ} = \max_{\mu:\mu(1,1)=0} \mathsf{IC}_\mu(AND, 0). \qquad (5)$$

By plugging in π^* and maximizing $I(\Pi^*; Y|X) + I(\Pi^*; X|Y)$ over all possible priors μ with $\mu(1, 1) = 0$, one obtains that $C_{DISJ} \approx 0.4827$ [BGPW13].

The remainder of the survey. The discussion so far has served as an informal introduction to communication and information complexity. In the next sections we will define the relevant models more formally. We will then focus on one of the main open problems in the area: understanding the relationship between information and communication complexity, also known as the problem of "interactive compression". It is an easy exercise to show that for all f, $\mathsf{IC}_\mu(f, \varepsilon) \leq \mathsf{D}_{\mu^n}(f^n, \varepsilon)$. Continuing the analogy of $\mathsf{IC}_\mu(f, \varepsilon)$ being the interactive analogue of Shannon's entropy, this fact corresponds to the fact that $H(X) \leq C(X)$, where $C(X)$ is the (expected) number of bits needed to transmit a sample of X. Huffman's *"one-shot"* compression scheme (aka Huffman coding, [Huf52]), can be viewed as a data compression result showing that a low-entropy X can be communicated using few bits of communication (overhead of at most +1):

$$H(X) \leq C(X) \leq H(X) + 1. \qquad (6)$$

The extent to which $\mathsf{D}_{\mu^n}(f^n, \varepsilon)$ can be bounded from above by $\mathsf{IC}_\mu(f, \varepsilon)$, i.e. the extent to which low information "conversations" can be compressed remains a tantalizing open problem. We will discuss partial progress towards this problem.

2 Model and Preliminaries

This section contains basic definitions and notations used throughout the remainder of the article. For a more detailed overview of communication and information complexity, see e.g., [Bra12b].

2.1 Communication Complexity

As discussed above, the two-party communication complexity model consists of two players (Alice and Bob) who are trying to compute some joint function $f(x, y)$ of their inputs using a communication protocol. More formally, let $\mathcal{X}, \mathcal{Y}$ denote the set of possible inputs to the two players. A *private coins communication protocol* π for computing a function $f : \mathcal{X} \times \mathcal{Y} \to \mathcal{Z}$ is a

rooted tree, where each node is either owned by Alice or by Bob, and is labeled with two children ("0" and "1"). At each round of the protocol, the (possibly randomized) message of the speaker only depends on his input and the history of the conversation (and possibly on private randomness). A more formal description is given in Figure 2.

From the definition in Figure 2, it is clear that the sequence of messages of a protocol forms a *Markov Chain* in the sense that, if (say) Alice is the speaker in round i, then $Y \to M_{<i}, X \to M_i$. This structural property of protocols plays a central role in the analysis of the communication complexity model.

The *communication cost* of the protocol π is defined as the maximum number of bits transmitted in any execution of π (i.e., the depth of the tree of π). We stress that this is a "one-shot" complexity measure and not an amortized one, as typical in classical information theory settings. This distinction is motivated by applications such as those mentioned in the introduction, and by the *direct sum* problem whose essence is quantifying the relationship between single-shot and amortized computation.

A *public coin protocol* is a distribution on private coins protocols, run by first using shared randomness to sample an index R and then running the corresponding private coin protocol π_R. Every private coin protocol is thus a public coin protocol. The protocol is called *deterministic* if all distributions labeling the nodes have support size 1.

For a distribution μ over $\mathcal{X} \times \mathcal{Y}$, and a parameter $\varepsilon > 0$, $\mathsf{D}_\mu(f, \varepsilon)$ denotes the *distributional communication complexity* of f, i.e., the communication cost of the cheapest deterministic protocol computing f on inputs sampled according to μ with error ε. $\mathsf{R}(f, \varepsilon)$ denotes the *randomized communication complexity* of f, i.e., the cost of the cheapest *randomized* public coin protocol which computes f with error at most ε, for *all* possible inputs $(x, y) \in \mathcal{X} \times \mathcal{Y}$. When measuring the communication cost of a particular protocol π, we sometimes use the notation $\|\pi\|$ for brevity.

A cornerstone result in communication complexity relates the two aforementioned complexity measures:

Theorem 2.1 (Yao's Minimax Theorem, [Yao79]). *For every $\varepsilon > 0$,*

$$\max_\mu \mathsf{D}_\mu(f, \varepsilon) = \mathsf{R}(f, \varepsilon).$$

The results described in this article are mostly stated in the *distributional* communication model (since information complexity is meaningless without a prior distribution on inputs), but results can be extended to the randomized model via Theorem 2.1.

2.2 Interactive Information complexity

Given a public coin communication protocol π, $\pi(x, y)$ denotes the concatenation of the public randomness (denoted R) with all the messages that are sent during the execution of π. We call this the *transcript* of the protocol. When referring to the random variable denoting the transcript, rather than a specific transcript, we will use the notation $\Pi(x, y)$ — or simply Π when x and y are clear from the context.

The *information cost* of a protocol π captures how much (additional) information the two parties learn about each other's inputs by observing the protocol's transcript[5].

Definition 2.2 (Internal Information Cost [BBCR10]). *The (internal) information cost* of a protocol over inputs drawn from a distribution μ on $\mathcal{X} \times \mathcal{Y}$, is given by:

$$\mathsf{IC}_\mu(\pi) := I(\Pi; X|Y) + I(\Pi; Y|X). \qquad (7)$$

For example, the information cost of the trivial protocol in which Alice and Bob simply exchange

[5]Note that in the definition below and throughout the paper, we swap the the order of (2) and (3) above: We define IC using the single-letter expression (3), and later prove theorem (2) (the operational meaning).

Generic Communication Protocol

1. Set v to be the root of the protocol tree.
2. If v is a leaf, the protocol ends and outputs the value in the label of v. Otherwise, the player owning v samples a child of v according to the distribution associated with her input for v and sends the label to indicate which child was sampled.
3. Set v to be the newly sampled node and return to the previous step.

Figure 2: A communication protocol.

their inputs, is simply the sum of their conditional marginal entropies $H(X|Y) + H(Y|X)$ (notice that, in contrast, the *communication* cost of this protocol is $|X| + |Y|$ which can be arbitrarily larger than the former quantity).

Another information measure which makes sense at certain contexts is the *external* information cost of a protocol [CSWY01], $\mathsf{IC}^{\mathsf{ext}}_{\mu}(\pi) := I(\Pi; XY)$, which captures what an *external* observer learns on average about both player's inputs by observing the transcript of π. This quantity will be of minor interest in this article (though it playes a central role in many applications). The external information cost of a protocol is always at least as large as its (internal) information cost, since intuitively an external observer is "more ignorant" to begin with. It is not hard to see that when μ is a *product* distribution, then $\mathsf{IC}^{\mathsf{ext}}_{\mu}(\pi) = \mathsf{IC}_{\mu}(\pi)$.

One can now define the *information complexity* of a function f with respect to μ and error ε as the least amount of information the players need to reveal to each other in order to compute f with error at most ε:

Definition 2.3. *The Information Complexity* of f with respect to μ (and error ε) is

$$\mathsf{IC}_{\mu}(f, \varepsilon) := \inf_{\pi\colon \Pr_{\mu}[\pi(x,y) \neq f(x,y)] \leq \varepsilon} \mathsf{IC}_{\mu}(\pi).$$

What is the relationship between the information and communication complexity of f? This question is at the core of the remainder of our discussion. The answer to one direction is easy: Since one bit of communication can never reveal more than one bit of information, the communication cost of any protocol is always an upper bound on its information cost over *any* distribution μ:

Lemma 2.4 ([BR11])**.** *For any distribution μ, $\mathsf{IC}_{\mu}(\pi) \leq \|\pi\|$.*

The answer to the other direction, namely, whether any protocol can be compressed to roughly its information cost, will be partially given in the remainder of this article.

Remark 2.5 (The role of private randomess)**.** *A subtle but vital issue when dealing with information complexity, is understanding the role of private vs. public randomness. In public-coin communication complexity, one often ignores the usage of private coins in a protocol, as they can always be simulated by public coins. When dealing with* information complexity*, the situation is somewhat the opposite: The usage of private coins is crucial for minimizing the information cost, and fixing these coins is prohibitive (once again, for communication purposes in the distributional model, one may always fix the entire randomness of the protocol, via the averaging principle). An instructive example is the following protocol: Alice sends Bob her 1-bit input $X \sim Ber(1/2)$, XORed with some random bit Z. If Z is private, Alice's message clearly reveals* 0

bits of information to Bob about X. However, for any fixing of Z, this message would reveal an entire bit(!). The guiding intuition is that private randomness is a useful resource for the parties to "conceal" their inputs and reveal information carefully.

2.3 Additivity of Information Complexity

One useful property of information complexity is that it is *additive*: the information cost of solving several independent tasks is the sum of the information costs of the individual tasks. This property is helpful when using information complexity to prove *lower bounds* on the communication cost of "modular" tasks that can be decomposed into independent sub-tasks. It was used implicitly in the works of [Raz08, Raz98] and more explicitly in [BBCR10, BR11, Bra12b].

In the following, $T(f^n, \varepsilon)$ denotes the task of computing f^n, the function that maps the tuple $((x_1, \ldots, x_n), (y_1, \ldots, y_n))$ to $(f(x_1, y_1), \ldots, f(x_n, y_n)))$, with marginal error at most ε on each coordinate. That is, for each $i \in [n]$ we require the protocol to compute $f(x_i, y_i)$ correctly with probability at least $1 - \varepsilon$, independent of the other coordinates.

Theorem 2.6 (Additivity of Information Complexity)**.** $\mathsf{IC}_{\mu^n}(T(f^n, \varepsilon)) = n \cdot \mathsf{IC}_{\mu}(f, \varepsilon)$.

The $(\leq)$ direction of the theorem is easy: to compute n independent copies of f, we can take a protocol that solves f and apply it independently to each copy. It is not difficult to see that since the copies are independent, the information cost will be n times the information cost of solving an individual copy.

For the $(\geq)$ direction, we will show the converse: if we can solve n copies of f with information cost I, then we can solve a single copy of f with information cost I/n.

So, suppose we have a protocol π that solves $T(f^n, \varepsilon)$ with information cost I. Given input (u, v) for f, we wish to construct a protocol π' that somehow uses π to compute $f(u, v)$, with $1/n$ the information cost of π.

Since π solves $T(f^n, \varepsilon)$, if we set $x_i = u,\ y_i = v$ for some coordinate i, and sample the rest of the coordinates independently from μ^{n-1}, then the output of π in coordinate i will be $f(u, v)$ except with probability ε. The question is: which coordinate i should we embed the input u, v in? And how should we sample the remaining coordinates?

It is fairly clear that picking some fixed i in advance, and always embedding u, v in coordinate i, is not a good idea. For example, suppose (x_i, y_i) are uniform bits and the protocol π we are working with just sends x_i, y_i. In this case our constructed protocol π' sends u, v, and its information cost is equal to the information cost of π (both are equal to 2) instead of being $1/n$. To avoid this issue, we pick i uniformly random over $[n]$, so that, informally speaking, π "cannot know which coordinate we care about".

As for the remaining coordinates, we cannot just have Alice sample the x_j's and Bob sample the y_j's privately, because μ might not be a product distribution. Thus, for each $j \neq i$, we will publicly sample either x_j or y_j, and the remaining input (y_j or x_j, respectively) will be privately sampled by the player that owns the input from the marginal distribution μ *given* the publicly-sampled input. It remains to specify which of the inputs, x_j or y_j, is publicly sampled at each coordinate $j \neq i$.

It is tempting to simply say: let us publicly sample x_j at *all* coordinates $j \neq i$, and have Bob privately sample y_j everywhere. However, this would not yield a low information cost protocol π'. Suppose, for example, that in π, Alice sends the bitwise-XOR of x. Then in π' she would do the same, and since x_{-i} is public, by sending the bitwise-XOR of x she would be revealing $x_i = u$. Again, instead of $1/n$ the information cost, π' would have the same information cost as π.[6]

[6] The same problem occurs if one tries to forgo private randomness altogether and sample all the missing (x_j, y_j) publicly.

However, this idea is not entirely without merit — it is easy to see that in this construction, while Alice leaks the same amount of information in π' and in π, *Bob* leaks only $1/n$ the information he leaks under π, or less. Similarly, if we sampled y_j publicly everywhere, then Alice would leak at most $1/n$ her information cost in π, but Bob would potentially leak too much information.

It turns out that the solution is to *combine* the two approaches in equal measure (in expectation): in the coordinates $j < i$, we sample x_j publicly, and in coordinates $j > i$, we sample y_j publicly. The missing coordinates are then sampled privately. This yields the correct information cost for π'; for the information leaked by Alice, we get:

$$\begin{aligned}
\mathrm{I}(U;\Pi'|V) &= \mathrm{I}(X_i; i, X_{<i}, Y_{>i}, \Pi | Y_i) \\
&\overset{(*)}{\leq} \mathrm{I}(X_i; \Pi | i, Y_{\geq i}, X_{<i}) \\
&\overset{(**)}{\leq} \mathrm{I}(X_i; \Pi | i, Y, X_{<i}) \\
&= \frac{1}{n} \sum_{i=1}^{n} \mathrm{I}(X_i; \Pi | Y, X_{<i}) \\
&= \frac{1}{n} \mathrm{I}(X; \Pi | Y).
\end{aligned}$$

In $(*)$ we used the fact that $\mathrm{I}(A;B,C|D) \leq \mathrm{I}(A;B|C,D)$, and in $(**)$ the fact that when C is independent of A given D, $\mathrm{I}(A;B|D) \leq \mathrm{I}(A;B|C,D)$. The last equality is by the Chain Rule.

The information leaked by Bob is bounded in a similar manner, and together we have $\mathsf{IC}_{\mu}(\pi') \leq \mathsf{IC}_{\mu^n}(\pi)/n$.

3 Interactive Compression: the Current State of the Art

In this section we present the two state-of-the-art compression schemes for unbounded-round communication protocols, the first due to Barak et al., and the second due to Braverman [BBCR10, Bra12b].

One natural idea approach to compress a multi-round protocol is to compress each round separately: whenever a player, say Alice, wants to send a message M to Bob, we can compress M using techniques from classical one-way compression [Huf52, HJMR07, BR11]. Unfortunately, any such compression scheme would send at least one bit of communication per round, even if the information conveyed in this round is much smaller than one bit. Therefore, if we try to compress a communication protocol with R rounds and information cost I, the resulting compressed protocol would have communication at least R, even if $I \ll R$. This approach is nevertheless useful in cases where $I \geq R$, e.g., in [BR11, BRWY13].

To compress protocols with $I \ll R$, we need an approach that does not depend on the number of rounds, only on the overall communication and information of the protocol.

3.1 Braverman's Compression Scheme

We begin with Braverman's compression scheme [Bra12b], which takes a protocol with information cost I and produces a protocol with communication $2^{O(I)}$, regardless of the communication of the original protocol. While the exponential loss incurred appears quite large, it turns out to be optimal in light of the recent lower bounds of [GKR14, GKR15].

The compression scheme is based on the following idea: In the protocol tree, neither player knows the true distribution on leaves of the protocol, but each player knows "part" of the distribution — the part corresponding to nodes it owns — and can estimate the other player's part. The smaller the information cost of the protocol, the better the players' estimates. In the compression scheme we describe here, the players use their estimates to jointly sample a leaf of the protocol from the correct distribution, and the communication they pay corresponds to how good their estimates are.

Product structure of protocols. We begin by formalizing what it means that a player knows "part" of the distribution: it turns out that protocols have a product structure, where one term in the product depends only on Alice's input, and the other depends only on Bob's input.

Denote by π_{xy} the true distribution of the transcript $\Pi(x,y)$, and by π_x (resp. π_y) the conditional marginal distribution $\Pi|X=x$ ($\Pi|Y=y$) of the transcript from Alice's (Bob's) point of view. The probability of reaching a leaf (path) $\ell \in \{0,1\}^C$ of π is

$$\pi_{xy}(\ell) = p_x(\ell) \cdot p_y(\ell) \tag{8}$$

where $p_x(\ell) = \prod_{w \subseteq \ell, w \text{ belongs to Alice}} p_{x,w}$ is the product of the transition probabilities in the protocol tree on nodes owned by Alice along the path from the root to ℓ, and $\pi_y(\ell)$ is analogously defined on the Bob's nodes. We think of p_x as "Alice's part of the distribution" and of p_y as "Bob's part of the distribution".

Estimating the other player's part. Let $q_x(\ell)$ (resp. $q_y(\ell)$) be the product of Alice's priors q_u on the transition probabilities at nodes u owned by Bob (resp. Alice). It is not difficult to see that $\pi_x(\ell) = p_x(\ell) \cdot q_x(\ell)$, and similarly, $\pi_y(\ell) = q_y(\ell) \cdot p_y(\ell)$.

Estimate quality vs. information cost. Intuitively, the less information the protocol leaks, the closer q_A, q_B are to p_A, p_B (respectively). And indeed,

$$\begin{aligned}
&\mathsf{IC}_\mu(\pi) = \mathrm{I}(\Pi; X|Y) + \mathrm{I}(\Pi; Y|X) \\
&= \mathbb{E}_{(x,y)\sim\mu} \left[\mathbb{D}\left(\pi_{xy} \| \pi_y\right) + \mathbb{D}\left(\pi_{xy} \| \pi_x\right) \right] \\
&= \mathbb{E}_{x,y,\ell\sim\pi_{x,y}} \left[\log \frac{\pi_{xy}(\ell)}{\pi_y(\ell)} + \log \frac{\pi_{xy}(\ell)}{\pi_x(\ell)} \right] \\
&= \mathbb{E}_{x,y,\ell\sim\pi_{x,y}} \left[\log \frac{p_x(\ell)}{q_y(\ell)} + \log \frac{p_y(\ell)}{q_x(\ell)} \right]. \qquad (9)
\end{aligned}$$

So, the expected log-ratio between p_x and q_y, and the expected log-ratio between p_y and q_x, are both bounded by the information cost of π. A Markov-style argument shows that for some constant $c > 1$, with high probability over x, y and $\ell \sim \pi_{x,y}$ we have both $\log\left(p_x(\ell)/q_y(\ell)\right) \leq c \cdot \mathsf{IC}_\mu(\pi)$ and $\log\left(p_y(\ell)/q_x(\ell)\right) \leq c \cdot \mathsf{IC}_\mu(\pi)$. (The log-ratio may be negative, so we cannot use Markov directly, but it can be shown that the contribution of the negative terms to the expectation is small.) To simplify the presentation, in the sequel we assume this event.

Rejection sampling. Now we describe how the players use their knowledge of p_x, q_x (for Alice) and p_y, q_y (for Bob) to sample a leaf $\ell \sim \pi_{x,y}$.

The approach is based on a simple form of *rejection sampling*: in order to sample from a distribution η over domain $\mathcal{U}$, we can throw uniformly random "darts" $(X_1, P_1), (X_2, P_2), \ldots \in_U \mathcal{U} \times [0,1]$, select the first dart i that falls under the curve of η, that is, has $P_i < \eta(X_i)$, and output X_i. This generates the correct distribution, and in addition, the expected number of darts thrown until we find a good one is $|\mathcal{U}|$.

In our case, the distribution from which we wish to sample is $\pi_{x,y} = p_x \cdot p_y$. Adapting the idea above, we can sample from this distribution by throwing "three-dimensional darts" $(L_1, A_1, B_1), (L_2, A_2, B_2), \ldots \in_U \{0,1\}^C \times [0,1] \times [0,1]$, selecting the first dart i that has both $A_i < p_x(L_i)$ and $B_i < p_y(L_i)$, and outputting L_i (see illustration in Figure 3). Here C is the length of the protocol being simulated. As before, we need roughly $\Theta(2^C)$ darts before we find a good one.

Since Alice knows p_x and Bob knows p_y, we can implement the sampling by using public randomness to generate the darts and having Alice compute the set of darts $\mathcal{A} = \{i : A_i < p_x(L_i)\}$ that satisfy her constraint and Bob compute the set of darts $\mathcal{B} = \{i : B_i < p_y(L_i)\}$. The first dart in the intersection $\mathcal{A} \cap \mathcal{B}$ is the one we need to output.

Unfortunately, the sets $\mathcal{A}, \mathcal{B}$ can be very large, and we cannot afford to have the players send them to each other in order to compute their intersection. This is where the players use the estimates q_x, q_y to narrow down the possibilities.

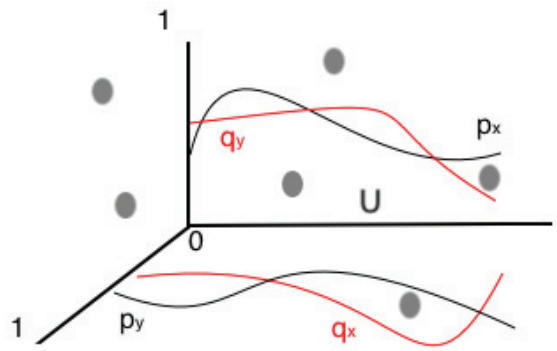


Figure 3: An illustration of the rejection sampling scheme from Braverman's compression protocol. The grey points represent random darts (L_i, A_i, B_i) which the players draw using shared randomness. The goal of the players is to output the first dart that falls simultaneously under both black curves (p_x and p_y).

Restricting the candidate darts. Recall that we expect to have $p_x/q_y, p_y/q_x \leq 2^{\Theta(I)}$. Under this assumption, any dart that satisfies $A_i < p_x(L_i)$ also satisfies $A_i < 2^{\Theta(I)} \cdot q_y(L_i)$, and similarly for p_y and $2^{\Theta(I)} \cdot q_x$. Therefore, Alice and Bob can narrow down their candidates: Alice considers the set $\mathcal{A}' = \mathcal{A} \cap \{i : B_i < 2^{\Theta(I)} \cdot q_x(L_i)\}$, and Bob considers $\mathcal{B}' = \mathcal{B} \cap \{i : A_i < 2^{\Theta(I)} \cdot q_y(L_i)\}$.

Initially we threw $\Theta(2^C)$ darts, each satisfying both constraints $A_i < p_x(L_i), B_i < p_y(L_i)$ with probability $1/2^C$. It is not hard to see that each dart also satisfies $A_i < q_y(L_i)$ with probability $1/2^C$ and $B_i < q_x(L_i)$ with probability $1/2^C$, so we expect to have a constant number of such darts. Since we scaled up the curves q_x, q_y by a factor of $2^{\Theta(I)}$, the probability of a dart satisfying the scaled constraints goes up by the same factor, and we have $|\mathcal{A}'|, |\mathcal{B}'| \leq 2^{\Theta(I)}$ in expectation and w.h.p. This is a manageable number of candidates, since we are trying to compress to $O(2^I)$.

Describing the candidates. Even though we now have a reasonable number of candidates, we still cannot afford to send the sets $\mathcal{A}', \mathcal{B}'$ as-is, because each transcript L_i requires C bits to encode and we might have $2^I \ll C$. Instead of directly writing out all the candidates for each player and taking the intersection, for each $L_i \in \mathcal{A}'$ we use the public randomness to generate $O(I)$ hash functions, Alice applies the hash functions to L_i and sends the resulting $O(I)$ bits to Bob. On his side, Bob applies all hash functions to the transcripts in $\mathcal{B}'$, and checks if there is a transcript $L_j \in \mathcal{B}'$ that matches all $O(I)$ hashes sent by Alice; if so, he outputs L_j. Otherwise they move on to the next candidate in $\mathcal{A}'$.

Because $|\mathcal{A}'|, |\mathcal{B}'| \leq 2^{O(I)}$ w.h.p., and we use $O(I)$ hashes for each candidate, the probability of a false match in $\mathcal{B}'$ is very small for each candidate, and a union bound shows that the overall probability of a false match is also small. So with high probability the players correctly identify the first dart in $\mathcal{A}' \cap \mathcal{B}'$. Since we also argued that w.h.p. we have $\mathcal{A} \cap \mathcal{B} \subseteq \mathcal{A}' \cap \mathcal{B}'$, this is the dart we want.

Conclusion. Overall, by carefully controlling the error probabilities in the procedure above, we obtain the following result:

Theorem 3.1 ([Bra12b]). *Let π be a protocol executed over inputs $x, y \sim \mu$, and suppose $\mathsf{IC}_\mu(\pi) = I$. Then for every $\varepsilon > 0$, there is a protocol τ which ε-simulates π, where $\|\tau\| = 2^{O(I/\varepsilon)}$.*

Notice that the parameters do not depend on the communication cost C of the protocol being compressed. Also, the resulting compressed protocol is *one-way*: Alice sends her hash values to Bob, who then compares them to his candidates and outputs the answer.

3.2 The Compression Scheme of Barak et al.

In this section we describe the compression scheme of Barak et al. [BBCR10], which compresses a protocol with communication cost C and information cost I to a protocol with communication $\approx \sqrt{I \cdot C}$.

The compression scheme from the previous section does not depend on the communication cost C of the protocol being compressed, but it does well only when $2^I \ll C$. Its weakness is that it samples a leaf in one shot (it is a one-way protocol). The candidates considered by each player are "scattered" all over the tree, even when the other player's distribution may be very narrow and restricted to a small number of leafs. As an extreme example, consider the deterministic protocol where Alice simply sends her input x, which is uniform over $\{0,1\}^n$, to Bob. A priori, Bob knows nothing about x, so his candidates will be (and *must* be) all transcripts in $\{0,1\}^n$. This simple protocol, which has $C = I = n$, will be blown up to $O(2^n)$ by the scheme from [Bra12b]. If instead we proceeded gradually and sampled a path to a leaf in smaller steps, we could do better; and this is the approach taken in [BBCR10].

The basic idea is as follows. The players use their priors π_x, π_y to sample two paths in the protocol tree in a *correlated* way, such that at any node u, the probability that the paths diverge at this node is $|p_u - q_u|$ (where p_u is the correct distribution on children at u, q_u is the prior of the player who doesn't own the node, and $|\cdot|$ denotes L_1-distance). The goal is to *agree* on a single path to a leaf distributed according to the p_u's. After sampling the two paths, the players find the first place where the paths diverge, fix the mistake by selecting the child sampled by the owner at that node, and repeating until they have agreed on one joint path to a leaf. Since in each step the process selects the child sampled by the owner of the node, the process outputs a node distributed according to the correct distribution.

The key to the performance of this sampling scheme is that sampling correlated paths can be done using only public randomness, no communication; so the cost is determined by (a) the cost of finding the first place where the paths sampled diverge, and (b) the number of mistakes (places of disagreement) encountered before we reach a leaf. We will now describe the correlated sampling procedure and how to find the first point of divergence efficiently, and then analyze the number of mistakes.

Correlated sampling. The main building block of the sampling procedure is the following simple setting. Alice and Bob have two Bernoulli distributions $\mathrm{Ber}(a), \mathrm{Ber}(b)$, respectively, for $a, b \in [0,1]$, and want to produce samples $A \sim \mathrm{Ber}(a), B \sim \mathrm{Ber}(b)$ (respectively) such that $\Pr[A \neq B] = |a - b|$. To do this, they publicly sample a number $W \sim_U [0,1]$; Alice outputs 1 iff $W \leq a$, and Bob outputs 1 iff $W \leq b$. The samples have the correct distributions, and in addition, since Alice and Bob only disagree if $a \leq W \leq b$ or $b \leq W \leq a$, we have $\Pr[A \neq B] = |a - b|$.

In the protocol tree, at each node u, the distribution on children p_u and the prior q_u are Bernoulli random variables (since the tree is binary). To sample two paths (leafs) $\ell_A \sim \pi_x, \ell_B \sim \pi_y$, we use correlated sampling to sample a child at each node, with the player that owns the node sampling from p_u and the other from q_u. The probability of disagreeing at this node is $|p_u - q_u|$.

Finding the first difference. Now we have two paths ℓ_A, ℓ_B, and the players need to find the first node where ℓ_A and ℓ_B disagree. We think of ℓ_A, ℓ_B as binary strings of C bits each (where "0" represents descending to the left child and "1" to the right).

A naive way to find the first difference is to use binary search. First, Alice computes $\log C$ publicly-random hashes of the first half of ℓ_A and sends them to Bob, who compares them to the first half of ℓ_B. If the hashes agree, then w.h.p. the first halves of ℓ_A, ℓ_B are the same, and the players continue searching for the first divergence point in the second half. Otherwise they look for the first divergence point in the first half. We continue in this way until we have found the exact place where the first difference occurs. The total number of bits spent is $O(\log^2 C)$.

This approach can be improved to $O(\log C)$ bits by decreasing the number of hashes sent at each point to $O(1)$ [FPRU94]. As a result, we now make a *mistake* with constant probability, as the probability of a false match is constant. Nevertheless, adding some redundancy to find mistakes, and backtracking upon finding them, ensures that we will reach the right location, and a clever random walk argument shows that the total number of steps will still be $O(\log C)$.

Number of mistakes. How many points of disagreement will be encounter and fix before we reach a leaf? As we said, the probability of disagreeing at node u is $|p_u - q_u|$, and by Pinsker's inequality, this is bounded by $O(\sqrt{\mathbb{D}(p_u \parallel q_u)})$. Therefore, the expected number of mistakes is bounded by the expected sum of $\sqrt{\mathbb{D}(p_u \parallel q_u)}$ at nodes u along the path we sample.

We can relate this to the information cost. In expectation, the divergences at the nodes add up to the information cost of the protocol:

$$\mathsf{IC}_\mu(\pi) = \mathbb{E}_{x,y,\ell\sim\pi_{x,y}}\left[\sum_{u\in\ell}\mathbb{D}(p_u \parallel q_u)\right].$$

The total depth of the tree is C; by Cauchy-Schwarz and linearity of expectation, the total number of mistakes is bounded by $O(\sqrt{I\cdot C})$.

Conclusion. Putting the parts together, we obtain the following:

Theorem 3.2 ([BBCR10])**.** *Let π be a protocol executed over inputs $x, y \sim \mu$, and suppose $\mathsf{IC}_\mu(\pi) = I$ and $\|\pi\| = C$. Then for every $\varepsilon > 0$, there is a protocol τ which ε-simulates π, where*

$$\|\tau\| = O\left(\sqrt{C\cdot I}\cdot(\log(C/\varepsilon)/\varepsilon)\right). \qquad (10)$$

The analysis we outlined above is tight for this compression scheme, which we can see by looking at extremal cases for the Pinsker and Cauchy-Schwartz inequalities. Pinsker is tight for, e.g., $\mathrm{Ber}(1/2\pm\varepsilon)$ vs. $\mathrm{Ber}(1/2)$; and Cauchy-Schwartz is tight when all terms in the summation are equal (that is, information is leaked at a constant right over the rounds of the protocol).

In light of this, suppose Alice has a uniform C-bit string $X = X_1 \dots X_C$ where $X_i \sim \mathrm{Ber}(1/2)$, and consider the C-bit protocol π in which Alice sends, at each round i, an independent sample M_i such that

$$M_i \sim \begin{cases} \mathrm{Ber}(1/2+\varepsilon) & \text{if } X_i = 1 \\ \mathrm{Ber}(1/2-\varepsilon) & \text{if } X_i = 0 \end{cases}$$

for $\varepsilon = 1/\sqrt{C}$. Since Bob has a perfectly uniform prior on X_i, we have $I(M_i; X_i|M_{<i}) \le I(M_i; X_i) = \mathbb{D}\left(\mathrm{Ber}(1/2+\varepsilon)\|\mathrm{Ber}(1/2)\right) = O(\varepsilon^2)$, so the total information cost of π is $O(\varepsilon^2\cdot C) = O(1)$ by choice of $\varepsilon = 1/\sqrt{C}$. On the other hand, the probability of making a "mistake" at step i of the simulation above is the total variation distance $|\mathrm{Ber}(1/2\pm\varepsilon) - \mathrm{Ber}(1/2)| = 2\varepsilon$. Therefore, the expected number of mistakes conditioned on any values of the X_i's is $C\cdot 2\varepsilon = 2\sqrt{C}$.

4 Open Problems

Let us conclude by suggesting several open problems and research directions. More open problems can be found in [Bra12a], although several of the problems in that survey have been already solved.

Problem 1: The limits of one-shot interactive compression. Based on the discussion in Section 3, an important open problem is to see to what extent interactive compression can be improved. Given a protocol π with information cost I and communication cost C, how much communication suffices to simulate π by an equivalent protocol π'?

The answer we currently have is $\min(2^{O(I)}, \tilde{O}(\sqrt{I\cdot C}))$. The results of [GKR14, GKR15] currently rule out a compression scheme whose cost is independent of C and subexponential in I. However, a scheme whose

cost is, for example, $(I \log C)^{O(1)}$, remains a tantalizing possibility.

Another direction that only recently received attention [TVVW15] is mapping out the dependence of the communication cost (particularly worst-case communication cost) of the compression on the simulation error.

Problem 2: The scaling limit of zero-error communication. The "Information = Amortized Communication" theorem ($\mathsf{IC}_\mu(f,\varepsilon) = \lim_{n\to\infty} \frac{\mathsf{D}_{\mu^n}(f^n,\varepsilon)}{n}$) only holds for computation with non-zero error that vanishes not faster than 2^{-n}, since the compression step in the $\geq$ direction of the proof inevitably introduces error. A natural question is whether there is, nevertheless, an analogues information-theoretic quantity that characterizes the scaling limit of the *average case, zero-error* communication complexity of a function $\mathsf{D}_\mu(f,0)$. In other words,

$$\text{what is } \lim_{n\to\infty} \frac{\mathsf{D}^{ave}_{\mu^n}(f^n,0)}{n}?$$

A plausible conjecture is that the limit is the external information complexity $\mathsf{IC}^{\mathsf{ext}}_\mu(f,0)$ of f that we've mentioned earlier. For example, the external information complexity of the two-bit AND can be shown to be $\log_2 3$, and, indeed, the zero-error communication complexity of set intersection scales as $(\log_2 3)\cdot n$ [AC94].

It is known that this conjecture is false when μ does not have full support [KMSY14], so one needs to assume that μ has full support (or, alternatively, that "zero-error" means being correct even on inputs outside of μ's support). Also, it is not hard to show that

$$\mathsf{IC}^{\mathsf{ext}}_\mu(f,0) \geq \lim_{n\to\infty} \frac{\mathsf{D}_{\mu^n}(f^n,0)}{n},$$

so the question is about whether the $\leq$ direction holds.

There are several examples where this conjecture holds, but in all of them a simple *fooling set* argument from communication complexity [KN97] applies. A specific function for which proving or disproving the conjecture would be interesting is the following $f:\{0,1,2\}\times\{0,1,2\}\to\{0,1\}$: $f(x,y) = (x=y=0)\vee(x=y=1)$.

Problem 3: The rate of convergence of bounded-round information complexity. As noted earlier, the characterization (3) falls short of allowing one to compute the limit (2) of the amortized communication complexity of a given function f, since the formula contains an inf over an unbounded set of protocols. It is possible to evaluate the infimum over *bounded-round* protocols, which involve at most r rounds of interaction [MI11]. If we denote

$$\mathsf{IC}^r_\mu(f,\varepsilon) := \inf_{\substack{\pi \text{ an } r\text{-round}\\ \text{protocol}\\ \text{solving } f\\ \text{w.p. } \geq 1-\varepsilon}} I(\Pi;Y|X) + I(\Pi;X|Y),$$

then, by definition,

$$\mathsf{IC}^r_\mu(f,0) \searrow \mathsf{IC}_\mu(f,0), \tag{11}$$

but the rate of convergence of this limit remains open. For a function f on the domain $\{1,\ldots,N\}\times\{1,\ldots,N\}$, it has been shown that to get δ-close to $\mathsf{IC}_\mu(f,0)$ it suffices to take $r = (N/\delta)^{O(N)}$. While it is clear that the rate of convergence should depend on N, it is quite plausible that the dependence is of the form $Q(N)/\delta^{O(1)}$. Better bounds on the rate of convergence would readily translate into better algorithms for computing the information complexity of problems.

Note that from the analysis of the two-bit AND function, where $N=2$, we know that the convergence cannot be faster than $1/r^2$, i.e. $\Omega(\delta^{-1/2})$ rounds are needed to get within δ of $\mathsf{IC}_\mu(f,0)$. A plausible conjecture is that

$$\mathsf{IC}^{Q(N)/\sqrt{\delta}}_\mu(f,0) - \mathsf{IC}_\mu(f,0) < \delta, \tag{12}$$

where $Q(N)$ is a function of N but not of δ. It would be interesting to prove or disprove (12).

Problem 4: Interactive coding theory. The next two problems are less concrete and have to do with theory building. The first direction is further developing interactive coding theory. The discussion in this survey can be viewed as an extension of Shannon's Source Coding to the interactive (two-party) setting. It would be interesting to further connect it to noisy channels.

The area of noisy interactive coding has seen a surge of activity recently, and it is beyond the scope of this paper to survey it. Some recent works include [Sch96, BR14, GMS14, BK12, BN13, BE14, GHS14, GH14]. Still, many open problems remain, particularly around optimal coding rates and understanding interactive channel capacity [KR13, Hae14], as well as its interplay with information complexity.

Problem 5: Extending information complexity to more than two parties. Finally, it remains to be seen to what extent two-party information can be extended to a greater number of parties. For example, in the 3-party model, Alice, Bob, and Charlie are given (possibly correlated) inputs $(x, y, z) \sim \mu$. Their goal is to compute a function $f(x, y, z)$ with probability $\geq 1 - \varepsilon$ using communication on a public board ("the broadcast model"). Denote by $\mathsf{D}^3_\mu(f, \varepsilon)$ the three-party (distributional) communication complexity. Many properties of communication complexity with 3+ parties are currently open. In the context of the present survey we can define similarly to (2):

$$\mathsf{IC}^3_\mu(f, \varepsilon) := \lim_{n\to\infty} \frac{\mathsf{D}^3_{\mu^n}(f^n, \varepsilon)}{n}. \qquad (13)$$

It would be very useful to have a simple information-theoretic characterization of $\mathsf{IC}^3_\mu(f, \varepsilon)$ in the spirit of (3). One apparent obstacle to such a definition is the existence of secure 3-party protocols which leak nothing to the participants except for the final value of the function [BOGW88]. This foils a naïve extension of the 2-party formula to the multiparty setting.

References

[AC94] Rudolf Ahlswede and Ning Cai. On communication complexity of vector-valued functions. *Information Theory, IEEE Transactions on*, 40(6):2062–2067, 1994.

[BBCR10] Boaz Barak, Mark Braverman, Xi Chen, and Anup Rao. How to compress interactive communication. In *Proceedings of the 2010 ACM International Symposium on Theory of Computing*, pages 67–76, 2010.

[BBM12] Eric Blais, Joshua Brody, and Kevin Matulef. Property testing lower bounds via communication complexity. *Computational Complexity*, 21(2):311–358, 2012.

[BE14] Mark Braverman and Klim Efremenko. List and unique coding for interactive communication in the presence of adversarial noise. In *Foundations of Computer Science (FOCS), IEEE 55th Annual Symposium on*, pages 236–245, 2014.

[BGPW13] Mark Braverman, Ankit Garg, Denis Pankratov, and Omri Weinstein. From information to exact communication. In *Proceedings of the Forty-fth Annual ACM Symposium on Theory of Computing*, STOC '13, pages 151–160, New York, NY, USA, 2013. ACM.

[BK12] Zvika Brakerski and Yael Tauman Kalai. Efficient interactive coding against adversarial noise. *Foundations of Computer Science (FOCS), IEEE Annual Symposium on*, pages 160–166, 2012.

[BN13] Zvika Brakerski and Moni Naor. Fast algorithms for interactive coding. In *Proceedings of the 24th Annual ACM-SIAM Symposium on Discrete Algorithms*, SODA '13, pages 443–456, 2013.

[BOGW88] Michael Ben-Or, Shafi Goldwasser, and Avi Wigderson. Completeness theorems for non-cryptographic fault-tolerant distributed computation (extended abstract). In *STOC*, pages 1–10, 1988.

[BR11] Mark Braverman and Anup Rao. Information equals amortized communication. In Rafail Ostrovsky, editor, *FOCS*, pages 748–757. IEEE, 2011.

[BR14] Mark Braverman and Akhila Rao. Toward coding for maximum errors in interactive communication. *Information Theory, IEEE Transactions on*, 60(11):7248–7255, 2014.

[Bra12a] Mark Braverman. Coding for interactive computation: progress and challenges. In *50th Annual Allerton Conference on Communication, Control, and Computing*, 2012.

[Bra12b] Mark Braverman. Interactive information complexity. In *Proceedings of the 44th symposium on Theory of Computing*, STOC '12, pages 505–524, New York, NY, USA, 2012. ACM.

[BRWY13] Mark Braverman, Anup Rao, Omri Weinstein, and Amir Yehudayo. Direct product via roundpreserving compression. *Electronic Colloquium on Computational Complexity (ECCC)*, 20:35, 2013.

[BS15] Mark Braverman and Jon Schneider. Information complexity is computable. *CoRR*, abs/1502.02971, 2015.

[BT91] Richard Beigel and Jun Tarui. On ACC. In *FOCS*, pages 783–792, 1991.

[BYCKO93] R. Bar-Yehuda, B. Chor, E. Kushilevitz, and A. Orlitsky. Privacy, additional information and communication. *Information Theory, IEEE Transactions on*, 39(6):1930–1943, 1993.

[BYJKS04] Ziv Bar-Yossef, T. S. Jayram, Ravi Kumar, and D. Sivakumar. An information statistics approach to data stream and communication complexity. *Journal of Computer and System Sciences*, 68(4):702–732, 2004.

[CSWY01] Amit Chakrabarti, Yaoyun Shi, Anthony Wirth, and Andrew Yao. Informational complexity and the direct sum problem for simultaneous message complexity. In *Proceedings of the 42nd Annual IEEE Symposium on Foundations of Computer Science*, pages 270–278, 2001.

[DN11] Shahar Dobzinski and Noam Nisan. Limitations of vcg-based mechanisms. *Combinatorica*, 31(4):379–396, 2011.

[FPRU94] Uriel Feige, David Peleg, Prabhakar Raghavan, and Eli Upfal. Computing with noisy information. *SIAM Journal on Computing*, 23(5):1001–1018, 1994.

[GH14] Mohsen Ghaari and Bernhard Haeupler. Optimal Error Rates for Interactive Coding II: Efficiency and List Decoding. In *Foundations of Computer Science (FOCS), IEEE 55th Annual Symposium on*, pages 394–403, 2014.

[GHS14] Mohsen Ghaari, Bernhard Haeupler, and Madhu Sudan. Optimal error rates for interactive coding I: Adaptivity and other settings. In STOC '14: *Proceedings of the 46th Annual ACM Symposium on Theory of Computing*, pages 794–803, 2014.

[GKR14] Anat Ganor, Gillat Kol, and Ran Raz. Exponential separation of information and communication. In *Foundations of Computer Science (FOCS), 2014 IEEE 55th Annual Symposium on*, pages 176–185. IEEE, 2014.

[GKR15] Anat Ganor, Gillat Kol, and Ran Raz. Exponential separation of information and communication for boolean functions. In *Proceedings of the Forty-Seventh Annual ACM on Symposium on Theory of Computing, STOC 2015*, Portland, OR, USA, June 14–17, 2015, pages 557–566, 2015.

[GMS14] Ran Gelles, Ankur Moitra, and Amit Sahai. Efficient coding for interactive communication. *Information Theory, IEEE Transactions on*, 60(3):1899–1913, March 2014.

[Hae14] Bernhard Haeupler. Interactive channel capacity revisited. In *Foundations of Computer Science (FOCS), IEEE 55th Annual Symposium on*, pages 226–235, 2014.

[HJMR07] Prahladh Harsha, Rahul Jain, David A. McAllester, and Jaikumar Radhakrishnan. The communication complexity of correlation. In *IEEE Conference on Computational Complexity*, pages 10–23. IEEE Computer Society, 2007.

[Huf52] D.A. Human. A method for the construction of minimum-redundancy codes. *Proceedings of the IRE*, 40(9):1098–1101, 1952.

[Kla04] Hartmut Klauck. Quantum and approximate privacy. *Theory Comput. Syst.*, 37(1):221–246, 2004.

[KMSY14] Gillat Kol, Shay Moran, Amir Shpilka, and Amir Yehudayo. Direct sum fails for zero error average communication. In *Proceedings of the 5th conference on Innovations in theoretical computer science*, pages 517–522. ACM, 2014.

[KN97] Eyal Kushilevitz and Noam Nisan. *Communication complexity*. Cambridge University Press, Cambridge, 1997.

[KR13] Gillat Kol and Ran Raz. Interactive channel capacity. In *STOC '13: Proceedings of the 45th annual ACM symposium on Symposium on theory of computing*, pages 715–724, 2013.

[KS92] Bala Kalyanasundaram and Georg Schnitger. The probabilistic communication complexity of set intersection. *SIAM Journal on Discrete Mathematics*, 5(4):545–557, November 1992.

[Kus92] Eyal Kushilevitz. Privacy and communication complexity. *SIAM J. Discrete Math.*, 5(2):273–284, 1992.

[KW88] Mauricio Karchmer and Avi Wigderson. Monotone circuits for connectivity require superlogarithmic depth. In *STOC*, pages 539–550, 1988.

[LS] Troy Lee and Adi Shraibman. Lower bounds in communication complexity: A survey.

[MI11] Nan Ma and Prakash Ishwar. Some results on distributed source coding for interactive function computation. *IEEE Transactions on Information Theory*, 57(9), pages 6180–6195, 2011.

[PW10] Mihai Patrascu and Ryan Williams. On the possibility of faster sat algorithms. In Moses Charikar, editor, *SODA*, pages 1065–1075. SIAM, 2010.

[Raz92] Razborov. On the distributed complexity of disjointness. TCS: *Theoretical Computer Science*, 106, 1992.

[Raz98] Ran Raz. A parallel repetition theorem. *SIAM Journal on Computing*, 27(3):763–803, June 1998. Prelim version in STOC '95.

[Raz08] Alexander Razborov. A simple proof of Bazzi's theorem. Technical Report TR08-081, ECCC: Electronic Colloquium on Computational Complexity, 2008.

[Sch96] Leonard J. Schulman. Coding for interactive communication. *IEEE Transactions on Information Theory*, 42(6):1745–1756, 1996.

[Sha48] Claude E. Shannon. A mathematical theory of communication. *Bell System Technical Journal*, 27, 1948. Monograph B-1598.

[TVVW15] Himanshu Tyagi, Shaileshh Venkatakrishnan, Pramod Viswanath, and Shun Watanabe. Information complexity density and simulation of protocols. *arXiv preprint arXiv:1504.05666*, 2015.

[Wac90] Juraj Waczulk. Area time squared and area complexity of vlsi computations is strongly unclosed under union and intersection. In Jrgen Dassow and Jozef Kelemen, editors, *Aspects and Prospects of Theoretical Computer Science, volume 464 of Lecture Notes in Computer Science*, pages 278–287. Springer Berlin Heidelberg, 1990.

[Yao79] Andrew Chi-Chih Yao. Some complexity questions related to distributive computing. In *STOC*, pages 209–213, 1979.

[Yao82] Andrew Chi-Chih Yao. Theory and applications of trapdoor functions (extended abstract). In *FOCS*, pages 80–91. IEEE, 1982.

Something Old, Something New, Something Borrowed, and Something Proved

S. Kudekar
Qualcomm Research, New Jersey, USA

S. Kumar
Texas A&M University, College Station, USA

M. Mondelli and R. Urbanke
School of Computer and Communication Sciences, EPFL, Switzerland

H. D. Pfister
Duke University, USA

E. Şaşoğlu
UC Berkeley

Abstract–What do you get when you combine classical algebraic codes, EXIT functions from iterative coding, and the fact that monotone symmetric Boolean functions have sharp thresholds? Capacity!

I. Something Old: A Class of Algebraic Codes

Reed–Muller (RM) codes are among the oldest codes in existence. They were introduced by Muller [1] in the mid-fifties and soon thereafter Reed [2] published a decoding algorithm based on majority-logic that was well-suited to the computing resources available at the time. Due to their many desirable properties they are also among the most widely studied codes and classical books on coding theory typically dedicate a whole chapter to their study [3].

It is probably fair to say that, in the last twenty years, the study of RM codes has slowed and other types of codes have taken center stage. However, despite this slowdown, there was still a steady stream of publications dedicated to RM codes. To name only a single author, we note that Ilya Dumer published many papers on RM codes during this time and made notable progress on their efficient decoding (e.g., see [4]).

In recent years there has been renewed interest in RM codes, partly due to the invention of the capacity-achieving polar codes [5], which are closely related to RM codes. In particular, RM and polar codes are both derived from the same square matrix: the binary Hadamard matrix. The difference lies in which rows of the Hadamard matrix are chosen to be in the generator matrix of the code. For RM codes one picks the rows of largest Hamming weight, whereas for polar codes the choice is dictated by the reliability of each row, when decoded in a predetermined order with a successive-cancellation decoder.

Performance comparisons between polar and RM codes were carried out in [6], [7]. Simulation and analytic results suggest that RM codes do not perform well under either successive-cancellation or iterative decoding, but they do outperform polar codes under maximum a posteriori (MAP) decoding [5], [8]. In fact, numerical simulations suggest something even stronger; namely, that it is possible to construct a family of codes of fixed rate and block length that interpolates between the polar code and the RM code such that the error probability under MAP decoding decreases monotonically as the code tends towards the RM code, see Figure 1 and [9].

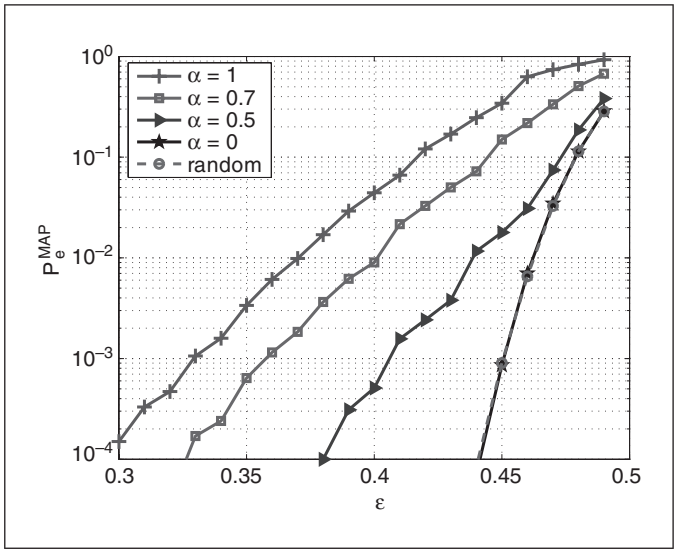


Fig. 1 Block error probability P_e^{MAP} under MAP decoding for the transmission of codes from the interpolating family over the BEC(ε). The code employed for transmission corresponds to the polar code for α = 1 and to the RM code for α = 0. Note that P_e^{MAP} is a decreasing function of α and, in addition, the error performance of the RM code is comparable to that of random codes.

Coupled with the fact that polar codes achieve capacity under successive decoding, these empirical observations raise the following question:

Do RM codes achieve capacity under MAP decoding?

We do not know exactly when or by whom this question was first considered. When RM codes were introduced in the mid-fifties, the question of finding capacity-achieving codes was probably not high on the agenda. Rather one was interested in finding codes and coding schemes that showed solid coding gains at practical complexities. However, the situation has changed significantly in the last twenty years with the introduction of turbo codes and the development of LDPC codes.

The rest is contemporary history. Soon after describing polar codes in 2008, Arıkan proposed this question as an interesting research challenge. During the recent program on Information Theory at the Simons Institute, see http://simons.berkeley.edu/programs/inftheory2015, this problem was posted as one of the open challenges for the program by Emmanuel Abbe. Indeed, just prior to this, Abbe, together with his co-authors Amir Shpilka and Avi Wigderson had made some progress on this question [10]. They showed that RM codes were indeed capacity-achieving under MAP decoding when transmission takes place over the binary erasure channel (BEC) and the rates converge to either 0 or 1. Further, they showed that the answer was also affirmative for transmission over the binary symmetric channel (BSC) when the rate converges to 0 and that these codes are "not too bad" for rates approaching 1.

II. Something New: RM Codes Achieve Capacity on the BEC for any Rate

As it turns out, this question has an affirmative answer for the BEC and any fixed code rate $R \in (0,1)$ [11], [12].

Up until perhaps twenty years ago, a result that only concerned the BEC would not have been taken very seriously. Afterall, the BEC seems very *special*. For example, MAP decoding of linear codes for the BEC can be done in cubic time whereas, for general channels, no polynomial algorithm is known. Nevertheless, over the years the coding community has come to realize the importance of the BEC. Almost everything we learned about iterative decoding was discovered first for the BEC, and then based on this knowledge, extended later to general channels. The BEC now provides an opportunity to crack the easiest case of a difficult problem and, hopefully, provide insights that will be useful for the general case.

Let us state the main result a bit more precisely. Consider a sequence of RM(r_n, n) codes of increasing n and rate R_n converging to R, $0 < R < 1$. For any $0 \le \varepsilon < 1-R$ and any $\delta > 0$ there exists an n_0 such that for all $n > n_0$ the block error probability of RM(r_n, n) over BEC(ε) is bounded above by δ under MAP decoding.

III. Something Borrowed: Three Ingredients

Perhaps more interesting than the result itself is what it relies on. A priori one would assume that such a result should be based on the very specific structure of RM codes. In fact, very little is needed as concerns the code itself. The proof relies on the following three ingredients:

A. RM codes are doubly transitive.

B. EXIT functions satisfy the area theorem.

C. Symmetric monotone sets have sharp thresholds.

As a preview, only the first ingredient relates to the code and it simply says that the code is highly symmetric. Perhaps the surprising ingredient is the second one. EXIT functions are one of the most frequently used notions when analyzing *iterative* coding systems. It is therefore a priori not clear why they would play any role when considering classical algebraic codes. The third ingredient is a staple of theoretical computer science, but has so far only appeared in very few publications dealing with coding theory.

Before describing in more detail each of these ingredients, we need to introduce some notation. Let RM(*r, n*) denote the Reed–Muller (RM) code of *order r* and *block length* $N = 2^n$ [3]. This is a linear code with dimension $K = \sum_{i=0}^{r} \binom{n}{i}$, rate $R = K/N$, and minimum distance $d = 2^{n-r}$. Its generator matrix consists of all rows with weight at least 2^{n-r} of the Hadamard matrix $\left(\begin{smallmatrix}1&0\\1&1\end{smallmatrix}\right)^{\otimes n}$, where $\otimes$ denotes the Kronecker product. Let $[N] = \{1,\dots,N\}$ denote the index set of codeword bits. For $i \in [N]$, let x_i denote the ith component of a vector x, and let $x_{\sim i}$ denote the vector containing all components *except* x_i. For $x, y \in \{0,1\}^N$, we write $x \preceq y$ if y dominates x componentwise, i.e. if $x_i \le y_i$ for all $i \in [N]$.

Let BEC(ε) denote the binary erasure channel with erasure probability ε. Recall that this channel has *capacity* $1-\varepsilon$ bits/channel use. In what follows, we will fix a rate R for a sequence of RM codes and show that the bit error probability of the code sequence vanishes for all BECs with capacity strictly larger than R, i.e., erasure probability strictly smaller than $1-R$.

A. RM Codes Are Doubly Transitive

The only property of RM codes that we will exploit is the fact that these codes exhibit a high degree of symmetry, and in particular, that they are invariant under a 2-transitive group of permutations on the coordinates of the code [3], [13], [14].

This means that for any $a, b, c, d \in [N]$ with $a \neq b$ and $c \neq d$, there exists a permutation $\pi : [N] \to [N]$ such that

(i) $\pi(a) = c$, $\pi(b) = d$, and

(ii) *RM(r, n)* is closed under the permutation of its codeword bits according to π. That is,

$$(x_1,\dots,x_N) \in RM(r,n) \iff (x_{\pi(1)},\dots,x_{\pi(N)}) \in RM(r,n).$$

B. EXIT Functions Satisfy the Area Theorem

We will be interested in MAP decoding of the ith codebit x_i from observations $y_{\sim i}$, that is, all channel outputs except y_i. The error probability of the ith such decoder for transmission over a BEC(ε) is called the ith *EXIT function* [15, Lemma 3.74], which we denote by $h_i(\varepsilon)$.

More formally, let $C[N,K]$ be a binary linear code of rate $R = K/N$ and let X be chosen with uniform probability from $C[N,K]$. Let Y denote the result of transmitting X over a BEC(ε). The EXIT function $h_i(\varepsilon)$ associated with the ith bit of C is defined as

$$h_i(\varepsilon) = H(X_i \,|\, Y_{\sim i}).$$

Furthermore, let $\hat{x}^{\mathrm{MAP}}(y_{\sim i})$ denote the MAP estimator of the ith code bit given the observation $y_{\sim i}$. Then,

$$h_i(\varepsilon) = \mathbf{P}(\hat{x}^{\mathrm{MAP}}(Y_{\sim i}) = ?).$$

At this point, a natural question arises: why should we consider this suboptimal decoder (we do not even use the whole output vector!) and EXIT functions instead of the optimal block-MAP

decoder? The answer is in the well-known *area theorem* [15]—[18]. Consider the *average* EXIT function $h(\varepsilon)=\frac{1}{N}\sum_{i=0}^{N-1}h_i(\varepsilon)$. Then,

$$\int_0^{\varepsilon} h(x)\,\mathrm{d}x=\frac{1}{N}H(X\,|\,Y),$$

i.e., the area below the average EXIT function equals the conditional entropy of the codeword X given the observation Y at the receiver. In particular,

$$\int_0^1 h(x)\,\mathrm{d}x=R=\frac{K}{N}.$$

Recall that the decoding of each bit relies only on $N-1$ received bits. Hence, we will denote each erasure pattern by a binary vector of length $N-1$, where a 1 denotes an erasure and a 0 denotes a non-erasure. Given a binary linear code C, we wish to study the properties of Ω_i, the set of all the erasure patterns that cause a decoding failure for bit i.

More formally, let Ω_i be the set that consists of all $\omega\in\{0,1\}^{N-1}$ for which there exists $c\in C$ such that $c_i=1$ and $c_{\sim i}\preceq\omega$. It is not hard to check that this definition is in fact what we want. That is, given an erasure pattern $\omega\in\{0,1\}^{N-1}$, the ith bit-MAP decoder fails if and only if $\omega\in\Omega_i$. Consequently, if we define $\mu_\varepsilon(\cdot)$ as the measure on $\{0,1\}^{N-1}$ that puts weight $\varepsilon^j(1-\varepsilon)^{N-1-j}$ on a point of Hamming weight j, then

$$h_i(\varepsilon)=\mu_\varepsilon(\Omega_i).$$

Thus, Ω_i "encodes" the EXIT function of the ith position.

As the title of the next section suggests, the set Ω_i is monotone and symmetric.

- **Monotonicity:** if $\omega\in\Omega_i$ and $\omega\preceq\omega'$, then $\omega'\in\Omega_i$.
- **Symmetry:** if $C[N,K]$ is a 2-transitive binary linear code, then Ω_i is invariant under a 1-transitive group of permutations for any $i\in[N]$. Following [19], we say that Ω_i is symmetric.

A consequence of the symmetry of Ω_i is that all EXIT functions of a 2-transitive code are identical. That is, $h_i(\varepsilon)=h_j(\varepsilon)$ for all $i,j\in[N]$, or in other words, $h_i(\varepsilon)$ is independent of i.

C. Symmetric Monotone Sets Have Sharp Thresholds

The main ingredient for the proof was observed by Friedgut and Kalai [19] based on the breakthrough result in [20]. The result is well-summarized by the title of this section and the precise statement is as follows. Let $\Omega\in\{0,1\}^N$ be a symmetric monotone set. If $\mu_{\underline{\varepsilon}}(\Omega)>\delta$, then $\mu_{\overline{\varepsilon}}(\Omega)>1-\delta$ for $\overline{\varepsilon}=\underline{\varepsilon}+c\log(1/2\delta)/\log(N)$, where c is an absolute constant. In other words, the measure $\mu_\varepsilon(\Omega)$ transitions from δ to $1-\delta$ in a window of size $O(1/\log(N))$.

We note that Tillich and Zémor derived a related theorem in [21] to show that *every* sequence of linear codes of increasing Hamming distance has a sharp threshold under block-MAP decoding for transmission over the BEC and the BSC. As far as we know, this was the first application of the idea of sharp thresholds to coding theory. However, even though the result by Tillich and Zémor tells us that the threshold exists and it is (very) sharp, it does not tell us *where* the threshold is located. This is where the area theorem will come in handy.

IV. Something Proved: The Proof

It remains to see how all these ingredients fit together.

Consider a sequence of codes RM(r_n,n) with rates converging to R. That is, the nth code in the sequence has a rate $R_n\le R+\delta_n$, where $\delta_n\to 0$ as $n\to\infty$.

By symmetry, $h_i(\varepsilon)$ is independent of i, and, thus, it is equal to the average EXIT function $h(\varepsilon)$. Therefore, by the area theorem we have

$$\int_0^1 h_i(\varepsilon)\,\mathrm{d}\varepsilon=R_n\le R+\delta_n.$$

Consider the set Ω_i that encodes $h_i(\varepsilon)$. Recall that Ω_i is monotone and symmetric. Therefore, from the sharp threshold result we have that if $h_i(\overline{\varepsilon})=1-\delta$, then $h_i(\underline{\varepsilon})\le\delta$ for $\overline{\varepsilon}=\underline{\varepsilon}+c\log(1/2\delta)/\log(N-1)$, where c is an absolute constant.

Since $h_i(\varepsilon)$ is increasing and it is equal to the probability of error of the estimator $\hat{x}^{\mathrm{MAP}}(y_{\sim i})$, the error probability of the ith bit-MAP decoder is upper bounded by δ for all $i\in[N]$ and $\varepsilon\le\underline{\varepsilon}$.

In order to conclude the proof, it suffices to show that $\underline{\varepsilon}$ is close to $1-R$. Note that by definition of $\overline{\varepsilon}$, the area under $h_i(\varepsilon)$ is at least equal to

$$(1-\overline{\varepsilon})(1-\delta)\ge 1-\overline{\varepsilon}-\delta=1-\underline{\varepsilon}-c\frac{\log\left(\frac{1}{2\delta}\right)}{\log(N-1)}-\delta.$$

On the other hand, this area is at most equal to $R+\delta_n$. Combining these two inequalities we obtain

$$\underline{\varepsilon}\ge 1-R-\delta-\delta_n-c\frac{\log\left(\frac{1}{2\delta}\right)}{\log(N-1)}. \tag{1}$$

We see that $\underline{\varepsilon}$ can be made arbitrarily close to $1-R$ by picking δ sufficiently small and N sufficiently large. In other words, the bit error probability can be made arbitrarily small at rates arbitrarily close to $1-R$.

V. Something More: Extensions and Questions

The proof outline above explains how one can get a vanishing bit error probability. In order to prove that the block error probability is also small for rates below the Shannon threshold, it is possible to exploit symmetries beyond 2-transitivity within the framework of Bourgain and Kalai [22] and obtain a stronger version of the sharp threshold result. If one insists on using the sharp threshold result by Friedgut and Kalai, it is still possible to prove that also the block error probability tends to zero by carefully looking at the weight distribution of RM codes.

How about other 2-transitive codes? As already pointed out, the only property we use of RM codes is that they are 2-transitive. Hence, the foregoing argument proves that any family of 2-transitive codes is capacity achieving over the BEC under bit-MAP decoding. This includes, for example, the class of extended BCH codes ([3, Chapter 8.5, Theorem 16]).

How about general channels? We are cautiously optimistic. Note that it suffices to prove that RM codes achieve capacity for the BSC since (up to a small factor) the BSC is the worst channel, see [23, pp. 87–89]. Most of the ingredients that we used here for the BEC have a straighforward generalization (e.g., GEXIT functions

replace EXIT functions) or need no generalization (2-transitivity). However, it is currently unclear if the GEXIT function can be encoded in terms of a monotone function. Thus, it is possible that some new techniques will be required to prove sharp thresholds in the general case.

How about low-complexity decoding? One of the main motivations for studying RM codes is their superior empirical performance (over the BEC) compared with the capacity-achieving polar codes. By far the most important practical question is whether this promised performance can be harnessed at low complexities.

Let us end on a philosophical note. What tools do we have to show that a sequence of codes achieves capacity? The most classical approach is to create an ensemble of codes and then to analyze some version of a typicality decoder. If the ensemble has pair-wise independent codewords, then this leads to capacity-achieving codes. A related technique is to look directly at the weight distribution. If this weight distribution is "sufficiently close" to the weight distribution of a random ensemble, then again we are in business. An entirely different approach is used for iterative codes. Here, the idea is to explicitly write down the evolution of the decoding process when the block length tends to infinity (this is called density evolution). By finding a sequence of codes such that density evolution predicts asymptotically error-free transmission arbitrarily close to capacity, we are able to succeed. Finally, there are polar codes. The proof that these codes achieve capacity is "baked" into the construction itself.

Our results suggest that "symmetry" is another property of codes that ensures good performance.

Acknowledgements

We thank the Simons Institute for the Theory of Computing, UC Berkeley, for hosting many of us during the program on Information Theory, and for providing a fruitful work environment. Further, we gratefully acknowledge discussions with Tom Richardson and Hamed Hassani.

References

[1] D. E. Muller, "Application of boolean algebra to switching circuit design and to error detection," *IRE Trans. Electronic Computers*, vol. EC-3, no. 3, pp. 6–12, 1954.

[2] I. Reed, "A class of multiple-error-correcting codes and the decoding scheme," *IRE Trans. Electronic Computers,* vol. 4, no. 4, pp. 38–49, 1954.

[3] F. J. MacWilliams and N. J. A. Sloane, *Theory of Error-Correcting Codes.* NorthHolland, 1977.

[4] I. Dumer, "Recursive decoding and its performance for low-rate Reed-Muller codes," *IEEE Trans. Inf. Theory*, vol. 50, no. 5, pp. 811–823, May 2004.

[5] E. Arikan, "Channel polarization: A method for constructing capacity-achieving codes for symmetric binary-input memoryless channels," *IEEE Trans. Inf. Theory*, vol. 55, no. 7, pp. 3051–3073, July 2009.

[6] E. Arıkan, "A survey of Reed-Muller codes from polar coding perspective," in *Proc. IEEE Inf. Theory Workshop (ITW),* Jan. 2010, pp. 1–5.

[7] ——, "A performance comparison of polar codes and Reed-Muller codes," *IEEE Commun. Lett*., vol. 12, no. 6, pp. 447–449, June 2008.

[8] N. Hussami, S. B. Korada, and R. Urbanke, "Performance of polar codes for channel and source coding," in *Proc. IEEE Int. Symp. on Inf. Theory (ISIT)*, July 2009, pp. 1488–1492.

[9] M. Mondelli, S. H. Hassani, and R. Urbanke, "From polar to Reed-Muller codes: a technique to improve the finite-length performance," *IEEE Trans. Commun*., vol. 62, no. 9, pp. 3084–3091, Sept. 2014.

[10] E. Abbe, A. Shpilka, and A. Wigderson, "Reed-Muller codes for random erasures and errors," in *STOC*, 2015.

[11] S. Kumar and H. Pfister, "Reed-Muller codes achieve capacity on erasure channels," May 2015, [Online]. Available: http://arxiv.org/abs/1505.05123.

[12] S. Kudekar, M. Mondelli, E. Sasoglu, and R. Urbanke, "Reed-Muller codes achieve capacity on the binary erasure channel under MAP decoding," May 2015, [Online]. Available: http://arxiv.org/abs/1505.05831.

[13] T. Kasami, L. Shu, and W. Peterson, "New generalizations of the Reed-Muller codes–I: Primitive codes," *IEEE Trans. Inf. Theory*, vol. 14, no. 2, pp. 189–199, Mar. 1968.

[14] T. Berger and P. Charpin, "The automorphism group of generalized Reed-Muller codes," *Discrete Mathematics*, vol. 117, pp. 1–17, 1993.

[15] T. Richardson and R. Urbanke, *Modern Coding Theory*. New York, NY, USA: Cambridge University Press, 2008.

[16] A. Ashikhmin, G. Kramer, and S. ten Brink, "Code rate and the area under extrinsic information transfer curves," in *Proc. IEEE Int. Symp. on Inf. Theory (ISIT)*, 2002, p. 115.

[17] ——, "Extrinsic information transfer functions: model and erasure channel properties," *IEEE Trans. Inf. Theory*, vol. 50, no. 11, pp. 2657–2673, Nov. 2004.

[18] C. Méasson, A. Montanari, and R. Urbanke, "Maxwell's construction: the hidden bridge between maximum-likelihood and iterative decoding," *IEEE Trans. Inf. Theory*, vol. 54, no. 12, pp. 5277 – 5307, Dec. 2008.

[19] E. Friedgut and G. Kalai, "Every monotone graph property has a sharp threshold," *Proc. Amer. Math. Soc.,* vol. 124, pp. 2993–3002, 1996.

[20] J. Kahn, G. Kalai, and N. Linial, "The influence of variables on boolean functions," in *Proc. IEEE Symp. on the Found. of Comp. Sci.,* Oct 1988, pp. 68–80.

[21] J.-P. Tillich and G. Zémor, "Discrete isoperimetric inequalities and the probability of a decoding error," *Combinatorics, Probability and Computing*, vol. 9, pp. 465–479, 2000. [Online]. Available: http://journals.cambridge.org/article_ S0963548300004466

[22] J. Bourgain and G. Kalai, "Influences of variables and threshold intervals under group symmetries," *Geometric & Functional Analysis,* vol. 7, no. 3, pp. 438–461, 1997.

[23] E. Şaşoğlu, "Polar coding theorems for discrete systems," Ph.D. dissertation, EPFL, 2011.

Fourier-Motzkin Elimination Software for Information Theoretic Inequalities

Ido B. Gattegno, Ziv Goldfeld, and Haim H. Permuter
Ben-Gurion University of the Negev

I. Abstract

We provide open-source software implemented in MATLAB, that performs Fourier-Motzkin elimination (FME) and removes constraints that are redundant due to Shannon-type inequalities (STIs). The FME is often used in information theoretic contexts to simplify rate regions, e.g., by eliminating auxiliary rates. Occasionally, however, the procedure becomes cumbersome, which makes an error-free hand-written derivation an elusive task. Some computer software have circumvented this difficulty by exploiting an automated FME process. However, the outputs of such software often include constraints that are inactive due to information theoretic properties. By incorporating the notion of STIs (a class of information inequalities provable via a computer program), our algorithm removes such redundant constraints based on non-negativity properties, chain-rules and probability mass function factorization. This newsletter first illustrates the program's abilities, and then reviews the contribution of STIs to the identification of redundant constraints.

II. The Software

The Fourier-Motzkin elimination for information theory (FME-IT) program is implemented in MATLAB and available, with a graphic user interface (GUI), at http://www.ee.bgu.ac.il/~fmeit/. The Fourier-Motzkin elimination (FME) procedure [1] eliminates variables from a linear constraints system to produce an equivalent system that does not contain those variables. The equivalence is in the sense that the solutions of both systems over the remaining variables are the same. To illustrate the abilities of the FME-IT algorithm, we consider the Han-Kobayashi (HK) inner bound on the capacity region of the interference channel [2] (here we use the formulation from [3, Theorem 6.4]). The HK coding scheme insures reliability if certain inequalities that involve the partial rates R_{10}, R_{11}, R_{20} and R_{22}, where

$$R_{jj} = R_j - R_{j0},\ j = 1,2, \tag{1}$$

are satisfied. To simplify the region, the rates R_{jj} are eliminated by inserting (1) into the rate bounds and adding the constraints

$$R_{j0} \le R_j,\ j = 1,2. \tag{2}$$

The inputs and output of the FME-IT program are illustrated in Fig. 1. The resulting inequalities of the HK coding scheme are fed into the textbox labeled as 'Inequalities'. The non-negativity of all the terms involved is accounted for by checking the box in the upper-right-hand corner. The terms designated for elimination and the target terms (that the program isolates in the final output) are also specified. The joint probability mass function (PMF) is used to extract statistical relations between random variables. The relations are described by means of equalities between entropies. For instance, in the HK coding scheme, the joint PMF factors as

$$P_{Q,U_1,U_2,X_1,X_2,Y_1,Y_2} = P_Q P_{X_1,U_1|Q} P_{X_2,U_2|Q} P_{Y_1,Y_2|X_1,X_2}, \tag{3}$$

and implies that $(X_2,U_2) - Q - (X_1,U_1)$ and $(Y_1, Y_2) - (X_1, X_2) - (Q, U_1,U_2)$ form Markov chains. These relations are captured by the following equalities:

$$H(X_2,U_2\,|\,Q) = H(X_2,U_2\,|\,Q,U_1,X_1) \tag{4a}$$

$$H(Y_1,Y_2\,|\,X_1,X_2) = H(Y_1,Y_2\,|\,Q,U_1,U_2,X_1,X_2). \tag{4b}$$

The output of the program is the simplified system from which redundant inequalities are removed. Note that although the first and the third inequalities are redundant [4, Theorem 2], they are not captured by the algorithm. This is since their redundancy relies on the HK inner bound being a union of polytops over a domain of joint PMFs, while the FME-IT program only removes constraints that are redundant for every fixed PMF. An automation of the FME for information theoretic purposes was previously provided in [5]. However, unlike the FME-IT algorithm, the implementation in [5] cannot identify redundancies that are implied by information theoretic properties.

III. Theoretical Background

A. Preliminaries

We use the following notation. Calligraphic letters denote discrete sets, e.g., χ. The empty set is denoted by ϕ, while $\mathcal{N}_n \triangleq \{1,2,\ldots,n\}$ is a set of indices. Lowercase letters, e.g. x, represent variables. A column vector of n variables $(x_1,\ldots,x_n)^\top$ is denoted by $\mathbf{x}_{\mathcal{N}_n}$, where $\mathbf{x}^\top$ denoted the transpose of $\mathbf{x}$. A substring of $\mathbf{x}_{\mathcal{N}_n}$ is denoted by $\mathbf{x}_\alpha = (x_i \in \Omega | i \in \alpha, \phi \neq \alpha \subseteq \mathcal{N}_n)$, e.g., $\mathbf{x}_{\{1,2\}} = (x_1,x_2)^\top$. Whenever the dimensions are clear from the context, the subscript is omitted. Non-italic capital letters, such as A, denote matrices. Vector inequalities, e.g., $\mathbf{v} \ge \mathbf{0}$, are in the componentwise sense. Random variables are denoted by uppercase letters, e.g., X, and similar conventions apply for random vectors.

B. Redundant Inequalities

Some of the inequalities generated by the FME may be redundant. Redundancies may be implied either by other inequalities or by information theoretic properties. To account for the latter, we combine the notion of Shannon-type inequalities (STIs) with a method that identifies redundancies by solving a linear programming (LP) problem.

1) *Identifying Redundancies via Linear Programming:* Let $\mathrm{A}\mathbf{x} \ge \mathbf{b}$ be a system of linear inequalities. To test whether the i-th inequality is redundant, define

- $\mathrm{A}^{(i)}$ - a matrix obtained by removing the i-th row of A;
- $\mathbf{b}^{(i)}$ - a vector obtained by removing the i-th entry of b;
- $\mathbf{a}_i^\top$ - the i-th row of A;
- b_i - the i-th entry of b.

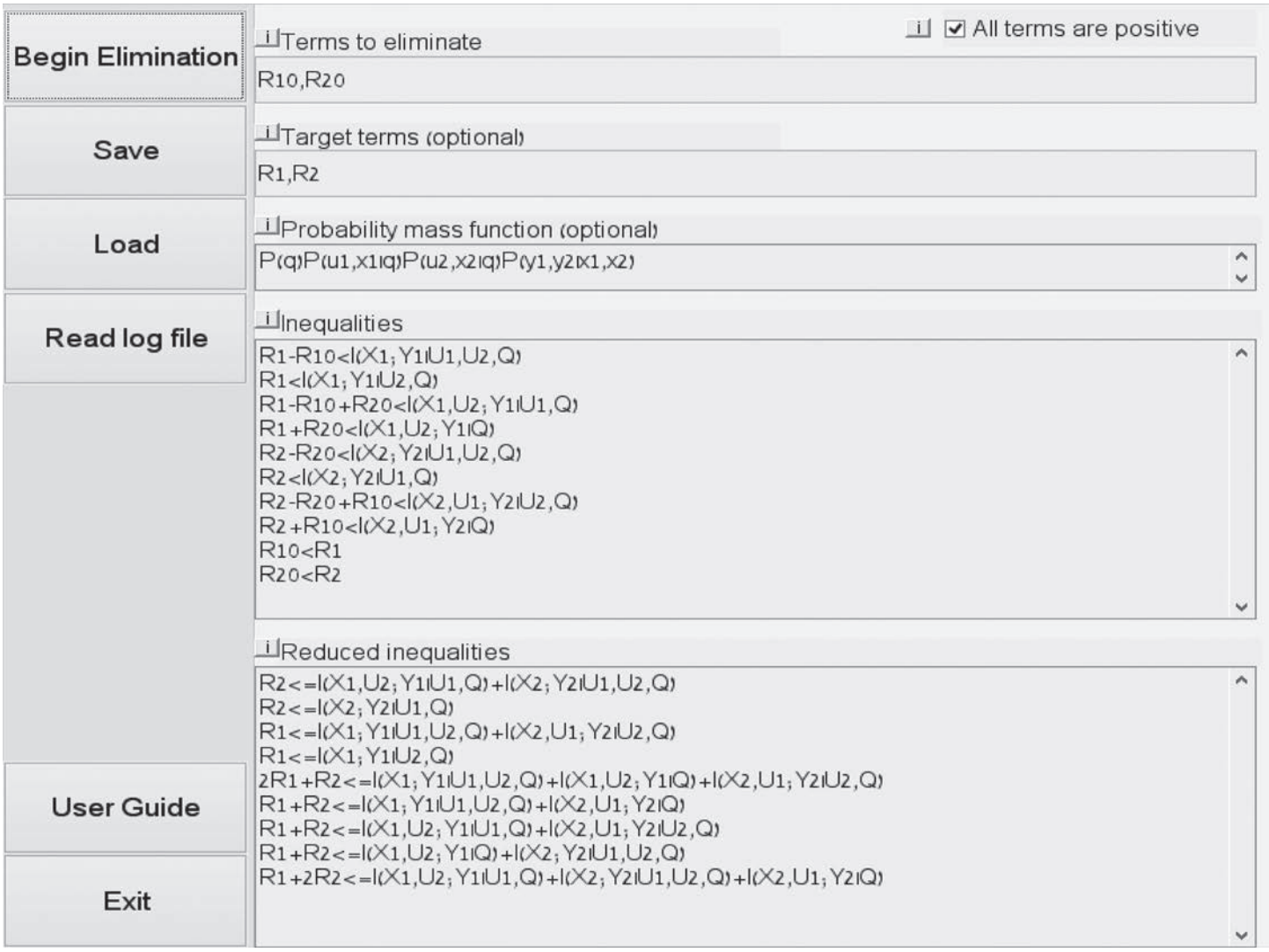


Fig. 1 FME-IT input and output - HK inner bound.

The following lemma states a sufficient and necessary condition for redundancy.

Lemma 1 (Redundancy identification) *The i-th linear constraint in a system* $\mathrm{A}\mathbf{x} \geq \mathbf{b}$ *is redundant if and only if*

$$\rho_i^* = \min_{\mathrm{A}^{(i)}\mathbf{x} \geq \mathbf{b}^{(i)}} \mathbf{a}_i^\top \mathbf{x} \tag{5}$$

satisfies $\rho_i^* \geq b_i$.

Lemma 1 lets one determine whether a certain inequality is implied by the remaining inequalities in the system by solving a LP problem. When combined with the notion of STIs, the lemma can also be used to identify redundancies due to information theoretic properties.

2) *Shannon-Type Inequalities:* In [6], Yeung characterized a subset of information inequalities named STIs, that are provable using the ITIP computer program [7] (see also [8]).

Given a random vector $\mathbf{X}_{\mathcal{N}_n}$ that takes values in $\chi_1 \times \ldots \times \chi_n$, define $\mathbf{h}_\ell \triangleq \left(H(\mathbf{X}_\alpha) \,|\, \phi \neq \alpha \subseteq \mathcal{N}_n\right)$[1]. The entries of $\mathbf{h}_\ell$ are *labels* that correspond to the joint entropies of all substrings of $\mathbf{X}_{\mathcal{N}_n}$. Every linear combination of Shannon's information measures is uniquely representable as $\mathbf{b}^\top \mathbf{h}_\ell$, where b is a vector of coefficients. This representation is called the *canonical form*. Fixing the PMF of $\mathbf{X}_{\mathcal{N}_n}$ to p, $\mathbf{h}_\ell(p) \in \mathbb{R}^{2^n-1}$ denotes the evaluation of $\mathbf{h}_\ell$ with respect to p.

We represent a linear information inequality as $\mathbf{f}^\top \mathbf{h}_\ell \geq 0$, where f is a vector of coefficients, and say that it *always holds* if it holds for every PMF. Formally, if

$$\min_{p \in \mathcal{P}} \mathbf{f}^\top \mathbf{h}(p) = 0, \tag{6}$$

where $\mathcal{P}$ is the set of all PMFs on $\mathbf{X}_{\mathcal{N}_n}$, then $\mathbf{f}^\top \mathbf{h}_\ell \geq 0$ always holds.

Since the minimization problem in (6) is intractable, Yeung suggested a simple affine space that contains the set where the canonical vectors take values. This space is described by all basic inequalities, which are non-negativity inequalities on all involved entropy and mutual information terms. The description is further simplified by introducing a minimal set of information inequalities, referred to as *elemental inequalities*.

[1]We order the elements of $\mathbf{h}_\ell$ lexicographically.

Definition 1 (Elemental inequality) *The set of elemental inequalities is given by:*

$$H(X_i \,|\, \mathbf{X}_{\mathcal{N}_n \setminus \{i\}}) \geq 0 \tag{7a}$$

$$I(X_i; X_j \,|\, \mathbf{X}_{\mathcal{K}}) \geq 0, \tag{7b}$$

where $i, j \in \mathcal{N}_n, i \neq j, \mathcal{K} \subseteq \mathcal{N}_n \setminus \{i, j\}$.

The left-hand side of every elemental inequality is a linear combination of the entries of $\mathbf{h}_\ell$. Therefore, the entire set can be described in matrix form as

$$\mathrm{G}\mathbf{h}_\ell \geq \mathbf{0}, \tag{8}$$

where G is a matrix whose rows are coefficients. Consequently, the cone

$$\Gamma_n = \left\{ \mathbf{h} \in \mathbb{R}^{2^n - 1} \,\middle|\, \mathrm{G}\mathbf{h} \geq \mathbf{0} \right\}, \tag{9}$$

contains the region where $\mathbf{h}_\ell(p)$ take values. The converse, however, does not hold in general.

Based on Γ_n, one may prove that an information inequality always holds by replacing the convoluted minimization problem from (6) with a LP problem. To state this result, we describe the probabilistic relations that stem from the factorization of the underlying PMF by means of linear equalities between entropies (such as in (3)) as

$$\mathrm{Q}\mathbf{h}_\ell = \mathbf{0}, \tag{10}$$

where Q is a matrix of coefficients.

Theorem 1 (Constrained STIs [6, Theorem 14.4]) *Let* $\mathbf{b}^\top \mathbf{h}_\ell \geq 0$ *be an information inequality, and let*

$$\rho^* = \min_{\substack{\mathbf{h}: \\ \mathrm{G}\mathbf{h} \geq \mathbf{0} \\ \mathrm{Q}\mathbf{h} = \mathbf{0}}} \mathbf{b}^\top \mathbf{h}. \tag{11}$$

If $\rho^* = 0$, *then* $\mathbf{b}^\top \mathbf{h}_\ell \geq 0$ *holds for all PMFs for which* $\mathrm{Q}\mathbf{h}_\ell = \mathbf{0}$, *and is called a constrained STI.*

IV. The Software Algorithm

The algorithm is executed in three stages. In the first stage, the input system of linear inequalities is transformed into matrix form. Assume the input system contains L variables. Denote by $\mathbf{r}_0$ the L-dimensional vector whose entries are the variables of the system. The input inequalities are represented as

$$\mathrm{A}_0 \mathbf{r}_0 + \mathrm{B}_0 \mathbf{h}_\ell \geq \mathbf{c}_0, \tag{12}$$

where $\mathbf{c}_0$ is a vector of constants and $\mathbf{h}_\ell$ is the vector of joint entropies as defined in Subsection III-B2. The rows of the matrices A_0 and B_0 hold the coefficients of the rates and the information measures, respectively, in each inequality. We rewrite (12) as

$$\mathrm{A}_1 \mathbf{x}_1 \geq \mathbf{c}_0, \tag{13a}$$

where

$$\mathrm{A}_1 \triangleq [\mathrm{A}_0 | \, \mathrm{B}_0] \tag{13b}$$

$$\mathbf{x}_1 \triangleq (\mathbf{r}_0^\top \, \mathbf{h}_\ell^\top)^\top. \tag{13c}$$

Henceforth, the elements of $\mathbf{h}_\ell$ are also treated as variables.

The second stage executes FME. Suppose we aim to eliminate the first $L_0 < L$ variables in the original $\mathbf{r}_0$. To do so, we run the FME on the first L_0 elements of $\mathbf{x}_1$ (see (13c)) and obtain the system

$$\mathrm{A}\mathbf{x} \geq \mathbf{c}, \tag{14}$$

where x is the reduced version of $\mathbf{x}_1$ after the elimination. The matrix A and the vector c are determined by the FME procedure.

The third stage identifies and removes redundancies. Let

$$\tilde{\mathrm{G}} \triangleq [0 \,|\, \mathrm{G}], \tag{15}$$

where G is the matrix from (8), and

$$\widetilde{\mathrm{A}} \triangleq \begin{bmatrix} \mathrm{A} \\ \widetilde{\mathrm{G}} \end{bmatrix} \tag{16a}$$

$$\tilde{\mathbf{c}} \triangleq \left(\mathbf{c}^\top \mathbf{0}^\top \right)^\top. \tag{16b}$$

Further, to account for constraints that are induced by the underlying PMF factorization, set

$$\tilde{\mathrm{Q}} \triangleq [0 \,|\, \mathrm{Q}], \tag{17}$$

where Q is the matrix from (10). Applying Lemma 1 (redundancy identification)[2] on each of the rows of

$$\tilde{\mathrm{A}}\mathbf{x} \geq \tilde{\mathbf{c}} \tag{18a}$$

under the constraint

$$\tilde{\mathrm{Q}}\mathbf{x} = \mathbf{0}, \tag{18b}$$

while relying on the machinery of Theorem 1, removes the redundant inequalities and results in the reduced system.

References

[1] A. Schrijver, *Theory of linear and integer programming*. John Wiley & Sons, 1998.

[2] Te Sun, Han and Kobayashi, Kingo, "A new achievable rate region for the interference channel," *IEEE Trans. Inf. Theory*, vol. 27, no. 1, pp. 49–60, Jan. 1981.

[3] El Gamal, Abbas and Kim, Young-Han, *Network information theory*. Cambridge University Press, 2011.

[4] H.-F. Chong, M. Motani, H. K. Garg, and H. E. Gamal, "On the Han-Kobayashi Region for the Interference Channel," *IEEE Trans. Inf. Theory*, vol. 54, no. 7, pp. 3188–3195, July 2008.

[2] We use an extended version of Lemma 1 that accounts also for equality constraints [9, Theorem 2.1].

[5] Joffrey Villard, "GUI for automatic Fourier-Motzkin elimination," http://www.joffrey-villard.fr/fmg?lang=en.

[6] R. W. Yeung, *Information theory and network coding*. Springer Science & Business Media, 2008.

[7] R. W. Yeung and Y.-O. Yan, "Information theoretic inequality prover (ITIP)," http://user-www.ie.cuhk.edu.hk/~ITIP/.

[8] Rethnakaran Pulikkoonattu, Etienne Perron and Suhas Diggavi, "X Information Theoretic Inequalities Prover," http://xitip.epfl.ch/.

[9] S. Jibrin and D. Stover, "Identifying redundant linear constraints in systems of linear matrix inequality constraints," *Journal of Interdisciplinary Mathematics*, vol. 10, no. 5, pp. 601–617, May 2007.

President's Column *continued from page 1*

of Error for Classical and Classical-Quantum Channels." The 2015 IT Society Paper Award was also announced; the award winning paper is titled "A Family of Optimal Locally Recoverable Codes" by Itzhak Tamo and Alexander Barg. The inaugural James L. Massey Research and Teaching Award for Young Scholars went to Young-Han Kim. The 2015 IT Society Aaron D. Wyner Distinguished Service Award went to Han Vinck. And the 2015 Shannon Award, announced at ISIT 2014, was presented to Robert Calderbank. The 2015 Wolf Student Paper Awards were announced later in the week; the recipients were Tarun Jog for the paper "On the Geometry of Convex Typical Sets," Marco Mondelli for the paper "Unified Scaling of Polar Codes: Error Exponent, Scaling Exponent, Moderate Deviations, and Error Floors," and Yihong Wu and Pengkun Yang for their paper "Optimal Entropy Estimation on Large Alphabets via best Polynomial Approximation."

The ISIT 2015 banquet ended with the announcement of the 2016 Shannon Award. The 2016 Shannon Lecturer will be Alexander Semenovich Holevo. Professor Holevo was chosen for our community's highest honor for his contributions to the field of quantum information theory. Over forty years ago, Holevo initiated the study of capacities for quantum channels. Very recently, he and his co-authors have settled a decades-old conjecture resolving the capacities of quantum Gaussian channels.

Looking ahead, we are moving forward on a number of plans to celebrate Shannon's 100th birthday. You can read updates on these plans in the Centenary section on Claude Shannon's Wikipedia page (https://en.wikipedia.org/wiki/Claude_Shannon#Shannon_Centenary). Bell Labs will develop an exhibit on Shannon's time there. Many universities around the world have signed on to hold "Shannon Day" programs—celebrating the Shannon centenary through public outreach events targeted to the general population and in particular to young people. These include Technische Universität Berlin, University of South Australia (UniSA), UNICAMP (Universidade Estadual de Campinas), University of Toronto, Chinese University of Hong Kong, Cairo University, Telecom ParisTech, National Technical University of Athens, Indian Institute of Science, Indian Institute of Technology Bombay, Nanyang Technological University, University of Maryland, University of Illinois at Chicago, Ecole Polytechnique Federale de Lausanne, The Pennsylvania State University (Penn State), University of California Los Angeles, Massachusetts Institute of Technology, and University of Illinois at Urbana-Champaign. The organizers would love to sign on more locations. Please see their request for participation elsewhere in this issue.

As noted earlier, the Information Theory Society is also working to create a documentary about Shannon's life and work. The Board of Governors allocated seed funding for this project at their meeting in June, and we are working to raise the remainder of the funds through science funding agencies, foundations, companies, and individuals. Several proposals are currently under review, but further funds will be required. I would love to hear from companies, foundations, and individuals interested in helping with this important and historic project.

As always, I want to thank all of the Society's many volunteers; the Society simply wouldn't exist without you. If you are not currently an active participant in the society, I strongly encourage you to get involved; I am happy to help you find a way to engage that matches your interests and availability. The vibrance of our field and community depend both on technical contributions and on the time, energy, and ideas of our members. I welcome your questions, comments, and suggestions. Please contact me at effros@caltech.edu

The Historian's Column

Anthony Ephremides

Having just returned from our latest Symposium in Hong Kong I was reflecting on the presentations I attended and was attempting to compare them with those of past years; especially with those of long, long ago. This comparison included Shannon's lectures, keynote presentations, papers by established researchers, and papers by students. My comparison did not focus on the content but rather on the presentation style and form of delivery. Fully aware that "mature" (in years) people are often (and justly) accused of romanticizing about the past, I tried to be objective and "normalize" my observations and reactions by taking into account how things have changed in general in the world.

Here are my conclusions. First, and foremost, the technology for preparing talks (which has vastly improved from the days of hand-written viewgraphs for overhead projectors, or, worse yet, hand-written presentations on the blackboard, and yes there were even some of those) has not improved the efficacy and quality of the delivery. Animation, zooming, multiple fonts, multimedia, and other wonderful features of today's methods have not succeeded in improving the delivery of the message in the talks. Of course there are many exceptions but, on average, the unintended consequence of the use of powerful media is the cluttering of the message. The temptation to squeeze more material and "information" on each slide, which has been amplified by the improved capabilities of the tools, has led to frequent excesses that disconnect the speaker from the audience.

Second, the amount of preparation by most speakers has clearly declined. Rehearsing and memorizing a talk is of course a disastrous practice but, by the same token, casual reliance on improvisation ability can be equally disastrous. Little attention seems to be given to the possibility that the audience may include those who are not thoroughly familiar with highly specialized aspects of the presentation content. As a result, again, speaker and audiences can be disconnected.

Third, the organization of most presentations seems to be not carefully thought out. In fact, a pervasive practice that especially the younger members of our community seem to be embracing is the one in which a table of contents is presented which could apply to almost ANY subject and reads like this. Introduction, Past Work, Model, Analysis, Results, Simulations, Conclusions (the latter often being just a summary of the talk rather than any substantive conclusion). Such a blueprint may provide some comfort and reduction of effort but does little to spark interest and engage the listener.

Finally, last, but not least, many presentations seem to be conveyed by robots rather than by eloquent, inspired and inspiring speakers. Perhaps this is setting the bar too high but in the IT Society we only have high bars. A presentation at the ISIT (or anywhere, for that matter) should not be just an attempt to "read" the slides (often with the speaker facing the screen for the duration of the talk). It should be a real attempt to motivate and engage the audience, cultivate interest in the presented work, and explain to as many listeners as possible the essence and the importance of the reported work.

Was it different in years past? To be sure, not much was different. There were always abuses of time and length, clumsiness in the preparation and delivery, unskillful organization, and the like. What was different was the understanding that presenting a paper implied the acceptance of substantial responsibility. The effort that went into it was evident and, in most cases, resulted in a better, clearer, and more effective talk. Yes, there was Rudi Ahlswede who would place his viewgraphs on one-another on the overhead projector and would proceed to write on them and scratch out things with markers or even with his fingers as he turned some of them at a 45-degree angle. But then there was Tom Cover who would place truly poorly prepared viewgraphs (at least with the standards of today's technology) on the projector and then make them "bloom" with information as he went on to explain and illustrate rather than "read" what was on them. There was that (un-named) ex-colleague of mine who would not turn his head even once to face the audience and who would go on for more than ten minutes beyond his allotted 20-minute slot until the session chair would approach him from behind and touch him on the shoulder (at which point he would turn back and look as if the werewolf had just appeared behind him and growled). But then there was Jim Massey who would talk about the seemingly simplest problem one could imagine and turn it to a fascinating story full of insights and excitement. There were dull and dry accounts of routine work but there were also inspirational and entertaining presentations that mixed the right amount of humor into the technical material.

Perhaps one of the culprits for the trend towards duller experiences in our symposia is the pressure that competition produces and the perceived need for more and more papers to be written and presented. I was glancing in the programs of ISITs from the '70's and '80's and could not find authors who had five or more papers in the program. Today it is rather routine to have multiple papers. Of course, some colleagues have many students and they simply try to have them all exposed and included in the Symposium program. However, it can lead also to embarrassing situations with the same person being a co-author of all the papers in the session (and also chairing the session!).

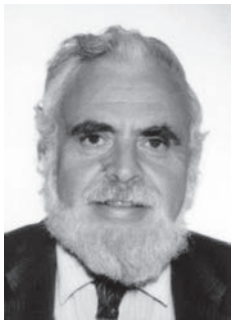
Perhaps I am being over-critical but I could not help feeling that we should adopt a slightly more relaxed attitude about this matter. We are all victims of "multi-tasking", busily running to fulfill multiple commitments (sometimes even in the Symposium itself and sometimes to other responsibilities elsewhere). One thing that was not available in the old days was today's ubiquitous connectivity. In one session I noticed that almost ALL "listeners" were glued to their laptops or smartphones while a hapless speaker was reciting the results of his work.

I need to close with a very insightful quote from Jim Massey. When he was program chair and someone asked him how many papers could he submit to the Symposium, could it be three papers, or four papers, he answered "why don't you just send us your best paper?" We cannot turn the clock back and things will continue to evolve and take their course. But an occasional mid-course correction by looking back can only be beneficial.

GOLOMB'S PUZZLE COLUMN™

Simple Theorems About Prime Numbers

Solomon W. Golomb



See which of these statements you can prove,

1) The sequence {3, 7, 11, 19, 23, 31, 43, …} of primes of the form $4n - 1$ is infinite.

2) The sequence {5, 11, 17, 23, 29, 41, 47, …} of primes of the form $6n - 1$ is infinite.

3) There are infintely many "twin primes" (consecutive odd numbers, both of which are prime) if and only if there are infinitely many positive integers n NOT of the form $6ab \pm a \pm b$, where a and b are positive integers and all combinations of the ± signs are allowed.

4) Let p_n denote the *nth* prime ($p_1 = 2$, $p_2 = 3$, *etc*) and let $\pi(x)$ be the number of prime numbers $\leq x_1$ (Thus $\pi(p_n) = n$.) Then every positive integer occurs exactly once, either in the sequence *a*) $n + \pi(n)$, or in the sequence *b*) $p_n + n - 1$, as n takes on all positive integer values.

5) The ratio $\frac{n}{\pi(n)}$ takes on every positive integer value > 1 at least once, as $n > 1$ runs through the positive integers.

From the Editor *continued from page 2*

off preparations for the Shannon Centenary to take place in 2016. You may have noticed the new logo on the front page of the newsletter! Please consider lending a hand.

Jasper Goseling, Tanya Ignatenko, Jos Weber, and Frans Willems have prepared a report on the 2015 European School of Information Theory (ESIT); Mahdi Cheraghchi, Salim El Rouayheb, and Emina Soljanin have prepared a report on the DIMACS Workshop on Coding-Theoretic Methods for Network Security; and Sid Jaggi has prepared a report on the Croucher Summer Course in Information Theory 2015 (CSCIT 2015). Finally, Edmund Yeh has prepared the Board of Governors meeting minutes from the ITA meeting in CA in February.

With sadness, we conclude this issue with tributes to two prominent members of our community that have recently passed away, Robert B. Ash (1935–2015) and Carlos R.P. Hartmann (1940–2015). Many thanks to Michael Pursley and to Yunghsiang S. Han and Pramod K. Varshney for preparing the tributes.

Please help make the newsletter as interesting and informative as possible by sharing 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, in 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 IT Society website, such as award announcements, calls for nominations and upcoming conferences, can be submitted at 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:

October 10, 2015 for the issue of December 2015.
January 10, 2016 for the issue of March 2016.

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.

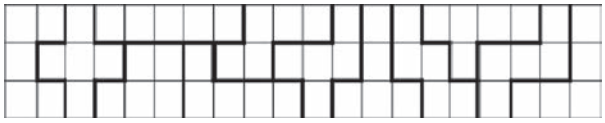
With best wishes,
Michael Langberg.

GOLOMB'S PUZZLE COLUMN™

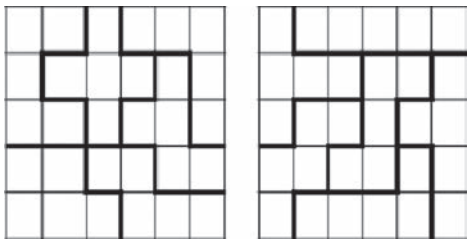
Pentominoes Challenges Solutions

Solomon W. Golomb

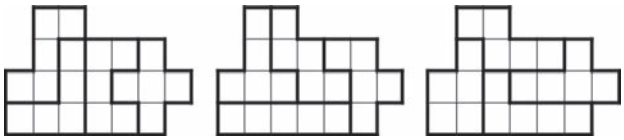
1)



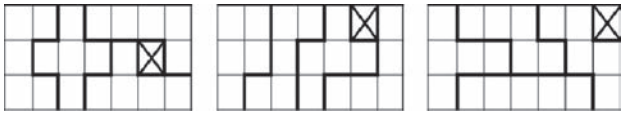
2)



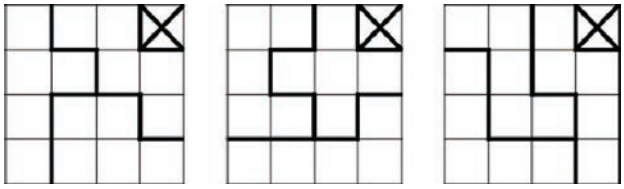
3)



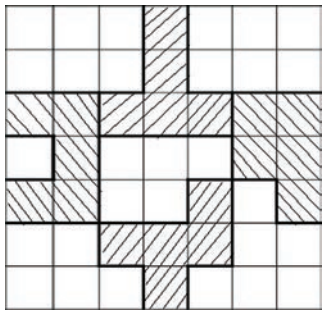
4)



5)

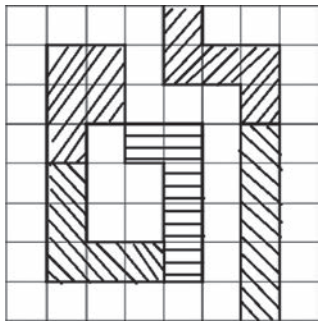


6)



Note that the five empty regions of five or six squares can hold no pentominoes other than the four already used.

7)



Note that the only pentominoes that will fit in any of the empty regions are the five that have already been used.

Solution 5 has the unused square in the same corner position in each 4 × 4 square. There are several other solutions. Only the I pentomino cannot appear in any solution, for obvious reasons.

The Students' Corner

Bernhard C. Geiger
On behalf of the IT Student Subcommittee

When I started my PhD in 2010, my advisor generously sent me to the Information Theory Workshop in Dublin to get to know the people and the field. It was not yet decided whether I would focus on IT in my studies, but this workshop made the decision clear. From the first day, I felt comfortable in this community, and I felt like I was being cared for, being valued and welcome, and being part of a large family. Probably one of the reasons why I felt so much at home was that I did not feel like I was being treated as "just a student", but rather as a peer—even when I was talking to Shannon awardees! Another reason was the fact that the IT society undertakes a lot of effort to make its students' life better. To name just a few, I mention the regular Schools of Information Theory, the student luncheons at workshops and conferences, and the tutorials and short courses targeted at students.

Many of these activities are (co-)organized by the IT Student Subcommittee (www.itsoc.org/people/committees/student), that is, by Deniz Gündüz, Osvaldo Simeone, Jonathan Scarlett, and myself. In order to fit our offers to your needs, we depend on your

input: What do you expect from the IT society in general, and from the Student Subcommittee in particular? If you have any ideas for events, virtual meetings, lecture series, or mailing lists, please let us know!

One of our most recent innovations is this students' column. To fill this column, we need your help. Have you recently read a good book or taken an online course on information theory that you would like to recommend to your colleagues? Would you like to tell us about an exciting event at a recent conference? Have you found a way out of struggling with research that could be helpful for others? Or can you give us any hints for the inevitable search for a good job in academia or industry? Finally, do you have a feeling that something is wrong in the way the IT society does things, something maybe that people who have been into "IT" for so long do not recognize anymore? Then let us know— tell us your thoughts, experiences, and wishes!

If you have anything to share, contributions to the column or suggestions for the IT Student Subcommittee, please send an e-mail to Parham Noorzad (parham@caltech.edu), a graduate student from Caltech, who will act as our "student editor".

From the field

IEEE Hong Kong Section Information Theory Chapter

The IEEE Hong Kong Section Information Theory Chapter is very honored to receive the 2015 IEEE Information Theory Society Chapter of the Year Award for contributions to Information Theory research and education. This is the second time that the Hong Kong IT Chapter has received this prestigious honor. The current Chapter Chairman is Chee Wei Tan. The Hong Kong IT Chapter continues the good traditions of organizing and supporting academic conferences and student-related activities that heavily involve chapter members working in collaboration with the local universities, the Institute of Network Coding (INC), the government research funding agency and the Croucher Foundation in Hong Kong.

Some of the notable highlights were student-centered international activities organized by Sidharth (Sid) Jaggi and Chandra Nair. The first one was the 2014 IT Society East Asian School in Information Theory with David Tse, Alon Orlitsky, Rüdiger Urbanke, Yasutada Oohama as school lecturers. This was the very first Asian School of IT. The second one was the 2015 Hong Kong Croucher Summer Course in Information Theory that took place right before ISIT 2015 and saw students from eleven different countries and regions learning from leading experts such as Emre Telatar, Pascal O. Vontobel, Navin Kashyap, and the 2015 Shannon Award recipient Robert Calderbank. All in all, the participating students were very enthusiastic with the valuable opportunities to interact closely with world-class researchers. We will continue with the momentum to engage students and young researchers in immersive activities and to nurture their interests in information theory.

At the 2015 IEEE Hong Kong-Taiwan Joint Workshop on Information Theory and Communications, we renewed old friendships with our Taiwanese colleagues and brought together more early-career scientists than previous years to exchange in the disciplines of information theory and communications. The keynote speaker at this workshop was Tracey Ho who was also our IT Society Distinguished Lecturer. Tracey spoke about "Real-world Network Coding" that brought together theoretical developments in network coding with real-world practical system implementation, based on her experience as the co-founder of two network coding-related start-up companies in the United States. These workshops allow professors, young scientists, graduate students and colleagues from Hong Kong and across the straits (and the greater Asia-Pacific) to come together to share their research findings and build collaborations and friendships.

We were also pleased to co-sponsor the IT Society's flagship conference, the 2015 IEEE International Symposium on Information Theory (ISIT), that was co-chaired by David Tse and Raymond Yeung. In fact, there were a number of firsts in the 2015 ISIT: this was the very first ISIT held in China. We had the first ISIT Banquet on a boat (Jumbo Kingdom at Aberdeen Harbor). This was the first public performance by Raymond, who was also the Founding Chapter Chairman of the Hong Kong IT Chapter, playing the harmonica and singing along with Toby Berger at the ISIT Award Luncheon. Hong Kong was truly fortunate to have a series of newly-attempted IT-related activities in 2015. Certainly, we will continue to foster long-term and closely-knitted collaborations between local and overseas researchers, and to attract more people to work in the areas of information theory and communications. In the near future, we plan to organize outreach activities to celebrate the Shannon›s Centennial and to get more people know about Shannon, his achievements and his legacy.

Shannon Centenary: We Need You!

The SHANNON CENTENARY, 2016, marks the life and influence of Claude Elwood Shannon on the hundredth anniversary of his birth on 30 April 1916. It is inspired in part by the Alan Turing Year [1]. Please help us to collect and prepare materials (photos, posters, games, Wikipedia entries, …) that we can make available to all the places that expressed interested in participating in the activities. To join us, please contact christina.fragouli@ucla.edu

Many thanks in advance!

Christina, Lav, Michelle, and Ruediger

Links

[1] https://en.wikipedia.org/wiki/Alan_Turing_Year

Report on the 2015 European School of Information Theory (ESIT)

Jasper Goseling, Tanya Ignatenko, Jos Weber, and Frans Willems

The 2015 European School of Information Theory was held in Zandvoort, The Netherlands, from April 20 to 24. Zandvoort is located close to Amsterdam on the North Sea coast. The school hosted 112 participants, including 89 young researchers, in particular PhD students and a number of PostDocs and MSc students. The school was organized according to the same format as previous schools in Tallinn, Estonia (2014), Ohrid, Macedonia (2013), and Antalya, Turkey (2012).

There were six 3-hour tutorials scheduled that were delivered by distinguished speakers. The students presented their own research during one of the three poster sessions. Moreover at ESIT 2015 there were three shorter lectures scheduled that were focusing on applications and entrepreneurial aspects of Information Theory.

The students participating in the school came from twenty different countries, mostly from Europe but also from Latin America, Africa, and the Middle East. The countries with the largest number of participants were Germany, France, Switzerland, and the Netherlands. Special guests at the school included Gerhard Kramer, representing the IEEE Information Theory Society, but also Han Vinck who invented the Information Theory School concept (in Europe) more than twenty years ago. Fredrik Brännström and Alexandre Graell I Amat, both from Chalmers University of Technology, who will organize the ESIT next year in Gothenburg, Sweden, also were guests in Zandvoort.

The school received generous support from the IEEE Information Theory Society and from the Netherlands Institute for Research on ICT (NIRICT). Additional support came from the CTIT, EIRICT, the Gauss Foundation, the Werkgemeenschap voor Informatie- en Communicatietheorie, and the IEEE Benelux Chapter on Information Theory. This support made it possible to provide fee waivers and travel grants to a number of student participants. EIT-ICT Labs supported the entrepreneurial presence.

Registration of the school opened on Sunday evening. Each student received a t-shirt with his/her poster on it. Monday morning started with a lecture by Young-Han Kim on Wireless Relay Networks. In the afternoon there was a first poster session. After that two entrepreneurial presentations were delivered, one by Frank Fitzek (Steinwurf, CodeOn) on network coding, and a second one by Geert-Jan Schrijen (Intrinsic-ID) on hardware-intrinsic security. In the evening there was a walking dinner scheduled at one of Zandvoort's beach clubs. Kees Schouhamer Immink (Turing Machines) gave a presentation there about managing (your own) intellectual property. On the second day, Tuesday, there was a lecture by Michael Langberg about Network Information Theory in the morning and in the afternoon Richard Durbin gave a tutorial lecture about Storage and Search of Genome Sequence Information. Wednesday morning it was Stephanie Wehner's turn to lecture. She gave an Introduction to Quantum Information Theory. In the afternoon the participants were taken on an excursion to the Keukenhof, to see the famous Dutch tulip gardens, and to socialize. The day ended with the official School Banquet, again in a beach club. On Thursday Imre Csiszár gave a tutorial on Information Theoretic Secrecy. The afternoon was filled with two poster sessions. Just like on Monday there was a lot of lively interaction when the students presented their own work. On Friday morning, Stephan ten Brink, who was delayed in traveling to Zandvoort by one day since Deutsche Bahn was subdued to strikes, gave the last tutorial lecture. Stephan lectured about Iterative Detection and Decoding in Communications.

After the event, many participants reported their satisfaction both with the organization and with the scientific contents. The team of organizers consisted of Jasper Goseling (University of Twente, chair), Jos Weber (Delft University of Technology), and Tanya Ignatenko and Frans Willems (both from Eindhoven University of Technology). The organizers acknowledge the assistance of the advisory board that included Gerhard Kramer and Vitaly Skachek.

The six tutorial lectures were videotaped. These videos and photographs taken during the school, together with the tutorial slides, can be found on the school's website http://www.itsoc.org/european-school-2015.

Preparations for ESIT 2016 in Sweden are in full swing. We are looking forward to next year's event.

DIMACS Workshop on Coding-Theoretic Methods for Network Security

Organizers:

Mahdi Cheraghchi, University of California, Berkeley
Salim El Rouayheb, Illinois Institute of Technology
Emina Soljanin, Bell Labs

A cross-discipline coding theory workshop was held at the Center for Discrete Mathematics and Theoretical Computer Science (DIMACS), Rutgers University, New Jersey, on April 1–3, 2015. The workshop brought together experts in coding theory, network coding, network security, and privacy, from the electrical engineering and computer science disciplines, along with experts from the industry. The goal was to discuss recent progress and identify open problems in security that arise in networks and distributed systems which could be effectively addressed by coding-theoretic techniques.

The workshop was motivated by the data explosion we witness in today's digital world which reinforces the concerns about security and privacy in networks. Coding-theoretic techniques, such as network coding and erasure coding for distributed storage, have been recently proposed and partially adopted in practice in order to reduce the cost incurred by data growth in networks in terms of bandwidth use, storage capacity, and energy consumption. Unfortunately, using such codes in networks creates novel security vulnerabilities e.g., pollution attacks and eavesdropping, which have not yet been adequately addressed. But, the distributed nature of networked systems does not only open new venues to attack. It also often imposes information-theoretic limitations on the adversary, making it possible to achieve provable and information-theoretic security without relying on computational assumptions of traditional cryptography. The workshop included talks that addressed recent progress in the literature on topics such as private information retrieval, differential privacy, distributed secret sharing, exposure-resilient and tamper-resilient coding

For more information and workshop slides, see http://dimacs.rutgers.edu/Workshops/SecureNetworking/announcement.html

The Croucher Summer Course in Information Theory 2015

Sidharth Jaggi

The Croucher Summer Course in Information Theory 2015 (CSCIT2015) was held in Hong Kong, 8–12 June, 2015, at the Chinese University of Hong Kong (CUHK). The Summer School was made possible by a very generous grant by the Croucher Foundation, "an independent private foundation dedicated to promoting the standard of the natural sciences, technology and medicine in Hong Kong". Due to the deliberate scheduling the week before the International Symposium on Information Theory (ISIT) 2015, turnout was high, with 68 attendees (almost all postgraduate students or postdoctoral scholars, with a few undergraduates and a couple of junior faculty) from 11 countries over four continents.

The weeklong program featured five tutorial-style talks, each by experts well-known for their contributions to the information theory and coding theory literature, each on consecutive mornings of CSCIT2015. Navin Kashyap from the Indian Institute of Science began the program on Monday with a comprehensive tutorial on Lattice Codes, and Vincent Tan gave a similarly in-depth chalk-talk on Tuesday with a talk on Second-order Asymptotics in Information Theory based on a monograph he recently authored on the subject. Wednesday saw CUHK's own local expert on coding theory give a intriguing talk on Factor Graph Transforms, showing connections between these "transforms to gauge transforms in physics and ... holographic transforms in theoretical computer science." Thursday saw one of the inventors of Polar Codes, Emre Telatar from the Ecole Polytechnique Fédérale de Lausanne, give a masterful whiteboard exposition on the design and analysis of these codes from first principles, and the denouement on Friday was delivered by the 2015 Claude E. Shannon lecturer, Robert Calderbank, giving a talk entitled "The Art of Measurement", in which he seamlessly wove together themes from classical and quantum error-correction, machine learning and information theory, all as a relaxed prelude to his Shannon lecture at ISIT the next week.

Supplementing the technical program by experts in the morning were sessions in the afternoons enabling participants to present their own results and discuss their research interests. On Monday and Tuesday afternoons each about 35 participants had a chance to give a short spotlight talk describing their research interests, followed by a long poster session enabling the other participants to have discussions on topics of mutual interest. Votes for "best posters" were solicited from both the participants and speakers, and four "lucky speakers", Simona Poilinca (Jacobs University Bremen), Guido Carlo Ferrante (Singapore University of Technology and Design (SUTD)), Jae Oh Woo (Yale), and Deepesh Data (Tata Institute of Fundamental Research), were selected to present long-form talks of their work on Thursday afternoon. Thursday afternoon also saw an "Information Theory Speed Dating" session designed to help break the cross-cultural ice and get participants who might not have otherwise interacted with each other spend a few minutes talking freely about life, the universe, and information theory. This then broke up into a spontaneous open problem session instigated and mediated by a participant, Swanand Kadhe (Texas A&M University).

All the speakers gave generously of their time, participating in academic and social sessions, freely dispensing advice about both research and life in general—there was a panel discussion entitled "Information Theory: A personal perspective" as a final session on Friday afternoon.

Complementing the academic schedule, there were also multiple opportunities for participants to interact with each other socially. There were nightly outings to parts of Hong Kong (Victoria Peak, Mong kok market, and Tsim Sha Tsui harbour). There was also a half-day boat-ride/hike/dinner excursion to Lamma island on Wednesday afternoon. A Facebook page allowed students to post photographs and interact online, and a complementary Piazza forum allowed for posting of academic questions/discussions.

Feedback from the participants was enthusiastically positive, with comments along the lines of "Extremely well organized. The choice of speakers and the topics were perfect. The social events were an added bonus.", and "It was very well organized, and useful for my PhD studies."

The primary organizer of CSCIT2015 was Sidharth Jaggi (CUHK), and the Co-Director was Gerhard Kramer (Technical University of Munich). Details are viewable at www.ie.cuhk.edu.hk/Croucher-summer-course-in-IT-2015/

IEEE Information Theory Society Board of Governors Meeting Minutes

The Marine Room, La Jolla, CA, 02.01.2015, 1 PM–5 PM Pacific Time

Edmund Yeh

Present: Michelle Effros, Ruediger Urbanke, Abbas El Gamal, Urbashi Mitra, Vijay Kumar, Vincent Poor, Jeff Andrews, Wei Yu, Aylin Yener, Matthieu Bloch, Edmund Yeh, Emanuele Viterbo, Michael Honig, Alex Vardy, Andrew Barron, Elza Erkip, Emina Soljanin, Tracey Ho, Nick Laneman, Dave Forney, Anand Sarwate, Frank Kschischang (via Skype), Gerhard Kramer (via Skype).

The meeting was called to order at 1 PM Pacific Time by Information Theory Society (ITSoc) President, Michelle Effros.

1) **Motion:** Vote to approve the minutes from the GlobalMeet BoG meeting (9/20/2014). Motion was passed.

2) **Motion:** Vote to approve the meeting agenda. Motion was passed.

3) Michelle presented the President's Report. Michelle welcomed the 2015 class of BoG Members: Helmut Bölcskei, Stephen Hanly, Ubli Mitra, Vince Poor, Aylin Yener, and Wei Yu, as well as the new officers: Rudiger Urbanke (Second Vice President), Daniela Tuninetti (Treasurer), Michael Langberg (Newsletter Editor). Michelle expressed thanks to Abbas El Gamal for his service as President, Muriel Medard for her service as Senior Past President, Aylin Yener for her service as Treasurer, Tara Javidi for her service as Newsletter Editor, Matthieu Bloch for his service as Online Committee Chair, as well as continuing officers, committee members, and members of the board.

   Congratulations were given to ITSoc members who have recently won IEEE Awards and Medals. These include Imre Csiszár (Hamming Medal), Richard Baraniuk (Mulligan Education Medal), Simon Litsyn (Johnson Information Storage Systems Award), and Andrea Goldsmith (Armstrong Achievement Award). IT Society Members who became IEEE Fellows in the class of 2015 are: Jean Armstrong, Gerhard Bauch, Kristine Bell, Daniel Bliss, Christian Cachin, Ning Cai, Biao Chen, Merouane Debbah, Pingzhe Fan, Nihar Jindal, Young-Han Kim, David Love, Gianluca Mazzini, Krishna Narayanan, Aylin Yener, and Wei Zhang. Finally, the prestigious National Medal of Science has been awarded to Tom Kailath.

   Michelle gave an update on the position of the ITSoc Administrator. This position was approved by the BoG in Fall 2014, approved and posted by the IEEE in winter 2014/2015. IEEE has been concerned with the quality of the received applications for the position. IEEE is currently looking to create a full-time position by combining the ITSoc position with a position sponsored by the IEEE or by another society.

   Michelle reported on the State of the Society. Currently, Society finances are sound with room for new initiatives. The Transactions continues its tradition of excellence. Conferences are on track for 2015–2017, while the venue for ISIT 2018 remains to be determined. ITSoc membership grew by 4% in 2014. The ITSoc was awarded the 2014 IEEE Professional Development Award, which recognizes the Society's exemplary educational, mentoring, and member support services (e.g., mentor network, WITHITS, Student Committee, Schools, etc.)

   Abbas noted that he received the IEEE Professional Development Award on behalf of the Society. The award will be passed on to the next President.

   In terms of priorities for the coming year, Michelle noted that the ITSoc does a good job of fostering communication among its members, but doesn't do as well at communicating beyond the Society. To remedy this, outreach and education activities should extend beyond the IT community. The Shannon Centennial (April 2016) is a great opportunity to start these activities. Other possible activities include the following. A sub-committee of the Conference Committee is investigating the possibility of joint workshops with other communities. The Newsletter Editor is considering curating a series of articles by authors outside our community on topics with potential for mutual exploration. An ad hoc committee is being formed which will team up with science shows, blogs, authors, or the local press to highlight the past, present, and future of information theory. The Committee will also prepare materials for Shannon Days around the world, and educational materials for kids, teachers, and the broader public. In these outreach activities, the WITHITS, Student, and Outreach Sub-committees will also play important roles.

   A discussion followed. Given the influence of Shannon's master's thesis on computing, it was suggested that Shannon Centennial activities be connected to the Computer Society. It was also suggested that the Boole Bicentennial held in Cork, Ireland, be connected with the Shannon Centennial. It was noted that there have recently been a number of movies focused on scientific and technological figures (e.g. Nash, Turing, Hawking). Perhaps it's time for a well-made movie on Shannon. It was pointed out that the IEEE has a media and publicity arm which can professionally produce movies. The Khan Academy seems to have produced some very accessible videos on information theory. Another possibility is to use crowd-sourcing to produce videos. Finally, science museums may be contacted to advertise Shannon-related activities.

4) Aylin Yener presented the (Former) Treasurer's Report. Aylin first discussed the 2014 budget, for which the actual numbers and bottom line will be available late February/

early March 2015. Due to the 2013 surplus, the Society has $55k from the 50% rule. Support for the three new schools (i.e. Hong Kong at $20k, India at $10k and Australia at $15k) were included as our three initiatives in 2014. A note to the new Treasurer: initiatives can be up to three years. Aylin suggests that support for the 2015 Hong Kong and India Schools be included as initiatives. Aylin moved to the 2015 budget. The budget was finalized in Sept 2014. The projected surplus is $125k. Support for the 2015 North American, European, East Asian, and Indian Schools were all approved (totaling $66.5k). The Distinguished Lecturer (DL) program is healthy but can grow further. Currently, travel expenses of $2k are allowed for each DL visit. New initiatives are needed for 2015. Aylin concluded that the Society budget is in good shape. The financial outlook for 2014 and 2015 looks strong. Conference closings are on schedule up to now, but need to be watched closely. Reimbursements have all been finished.

In the ensuing discussion, it was suggested that the Society should spend as much as it can. One way to improve Society finances for the long term is to have new conferences, and to co-sponsor new conferences.

5) Gerhard Kramer presented the Nominations and Appointments (N&A) Committee Report. Gerhard reviewed the composition of the N&A Committee, the External Nominations Committee, the Fellows Committee, and the Awards Committee, as well as the Shannon, Wyner, Cover, and Massey Award Committees.

   Gerhard then discussed the Online Committee, of which Matthieu Bloch has served as Chair since 2011. The N&A Committee appoints Anand Sarwate, who has served on the Online Committee since 2007, as the new Online Committee Chair.

   Motion: Vote to approve the appointment of Anand Sarwate as the Online Committee Chair. Motion was passed.

6) Matthieu Bloch presented the Online Committee Report. Matthieu began by mentioning that hosting on Pareja and web.com has been officially terminated. A complete backup of the server has been carried out. Part of the former hosting budget for web.com will be reused for itsoc.org. Matthieu reported that SixFeetUp has had a new project manager since fall 2014, with a smooth ongoing transition. The Master Service Agreement is in place for 2015. SixFeetUp rates have increased from $150/hour to $165/hour.

   Matthieu anticipates a 6–8 months transition period with Anand. During this period, the list of the Online Committee's role and tasks will be drafted. The documentation of new features and the media resources project will be finished. In terms of social media, an experimental Facebook page has been set up at https://www.facebook.com/pages/IEEEInformation-Theory-Society/339934289488983. Further experimentation will be carried out on the page before public advertisement. An IEEE.tv test channel is now available at https://ieeetv.ieee.org/player/html/viewer?channel=information-theory. The Committee is finalizing the re-encoding of all media resources. Videos will be linked into itsoc.org for easier navigation.

   A discussion followed. It was suggested all IT conferences be hosted on the ITSoc website. Such a measure may require a statement of support from the BoG. It was pointed out that the ITSoc website could be scaled better (e.g. website should automatically be scaled for mobile devices). It was suggested that this project may become a $10k initiative.

7) Aylin Yener presented the Schools Subcommittee report. The main item was the proposal for the 2016 European School of Information Theory in Gothenburg, Sweden. Giuseppe Durisi presented the School proposal. The proposed location for the School is Chalmers University of Technology located in central Gothenburg. The organizers are Fredrik Brannstrom, Giuseppe Durisi, and Alexandre Graell i Amat. Gerhard Kramer will serve as advisor. The School will take place April 4-8, 2016, on campus. The planned program includes 6 invited tutorial lectures, poster presentations, and a research visit to Ericsson. Topics include finite block lengths, fiber optics, distributed storage, compressive sensing, wireless networks, and graphical models. Confirmed lecturers include Gerhard Kramer and Henry Pfister. The target attendance is 100 participants (PhD students and postdocs). The organizers ask for ITSoc financial support of $20,000. This amount will be used to cover rent of rooms, tutorial speakers (partly), and lunches.

   A discussion followed. It was suggested that ITSoc members be offered a significantly lower registration fee. It was also suggested that Schools try to obtain more support from industry. Finally, it was pointed out that Schools should be combined with membership drives. School registration should try to get participants to sign up for membership.

   Motion: To approve funding at $20k for the 2016 European School of Information Theory in Gothenburg, Sweden. Motion was passed.

8) Frank Kschischang presented the Editor-in-Chief (EiC) Report. Frank expressed thanks to the support of the Executive Editorial Board members, the Peer Review Support Specialist, the Senior Editor, and the Information Director. He reviewed the Associate Editor retirements since July 2014. Giuseppe Durisi, the former Publications Editor, retired in August 2014. The Publications Editor role is now terminated, as the only task in the post-Pareja era is paper-scheduling, which requires approximately 10 minutes per month using IEEE's POPP (Publishing Operations Production Portal) tool. This task is now performed by the EiC.

   Frank reviewed the Editorial Board status as of February 2015. The Board currently consists of 41 Associate Editors (AEs). Some further expansion of the Editorial Board (to about 50) is planned. Particular needs exist in compressive sensing, complexity and cryptography, quantum information theory, and statistics.

   Frank then presented some statistics. The number of papers submitted to the Transactions has declined slightly over the last two years. The page budget for the Transactions in 2014 was 8500 pages. The actual page count was 8074. This yields a surplus of $34k in publication costs. Frank presented the

acceptance and rejection rates during 2014, in overall terms and by editorial area. The fast rejection rate (decision taking fewer than 30 days) is about 12%. Excluding decisions made within 30 days, the median time to first decision is 195 days (the overall median is 170 days). The first decision is reached within one year in 87% of cases. Outliers among Associate Editors are a concern. Frank and Lisa Jess are monitoring this, and sending reminders when appropriate. Some aggressive action (re-assignment of papers) was taken in July 2014 in one case.

A discussion followed. It was noted that there is still a sense that the decision time for the Transactions is too long. Frank indicated that the Board would quickly flag papers which are delayed. It was suggested that the Board try to identify which factors are most important in causing editorial delays. It was asked what the average load for an AE is (30 papers a year). It was then suggested that the Board should aim for roughly 2 papers per month per AE. By that measure, the current load may be too large.

9) Ruediger Urbanke presented the Membership Committee Report. The main items are the Outreach and Student Subcommittee Reports, presented by Joerg Kliewer. Joerg first presented the Outreach Subcommittee Report. Joerg thanked Elza Erkip and Daniela Tuninetti, who are leaving the committee. Bobak Nazer is continuing, while Tara Javidi is joining as a new member. It is proposed that Aaron Wagner and Joerg Kliewer serve as co-chairs of the Outreach Subcommittee.

Motion: To approve the appointments of Aaron Wagner and Joerg Kliewer as co-chairs of the Outreach Subcommittee of the Membership Committee. Motion was passed.

Joerg continued to report the recent activities of the Outreach Subcommittee. At ISIT 2014, the Subcommittee organized the panel discussion "How to Survive Tenure Track" with panelists Salman Avestimehr, Rob Calderbank, Natasha Devroye, and Pulkit Grover. Approximately 50 people attended. The panel was followed by the traditional ISIT mentoring get-together reception. Joerg gave an update on the Mentoring Program. Currently, there are about 31 mentoring pairs. Recent interviews indicate the success of the program. For 2015, a panel discussion on "101 Reasons to Study IT" has been organized for ITA with the Student Subcommittee. Panelists include Emina Soljanin, Andrea Montanari, and Venkatash Saligrama. There will also be an event for ISIT. The $3k budget for 2015 will be sufficient for the planned activities. For the long term, an advertising video, perhaps based on a revamp of the UCSD Shannon video, is being planned.

In the discussion which followed, it was recommended the the Subcommittee return with a more formal proposal on the advertising video. The proposal is a good candidate for an initiative.

Joerg moved to report the activites of the Student Subcommittee. The faculty coordinators for the Subcommittee are Deniz Gunduz and Osvaldo Simeone. At ITA 2014, a panel discussion (co-organized with the Outreach Committee) on "Landing Your Dream Job" was held at Tony Roma's. Panelists included Giuseppe Caire, Bertrand Hochwald, Muriel Medard, and Joseph Soriaga. Lunch was served and the event had very high attendance. At CISS 2014, a roundtable discussion on current research topics with moderators and pizza also had very high attendance. At ISIT 2014, lunch with the Shannon awardee was hosted by Osvaldo Simeone. The interview is available at: http://media.itsoc.org/isit2014/JanosKornerInterview.mp4. Expenses for the ITA 2014, CISS 2014 and ISIT 2014 events are already in the budget. For 2015, one goal is to extend membership to students and postdocs with the aim of enhancing diversity and establishing a presence in Asia and Latin America. The ITA panel, CISS roundtable discussion, and the ISIT Meet the Shannon Awardee event will be continued. The Subcommittee budget for 2015 is $10k.

10) Elza Erkip presented the Conference Committee Report. New members of the committee are Albert Guillen i Fabregas, Ubli Mitra, and Daniela Tuninetti (ex-officio). Retiring members are Lars Rasmussen and Aylin Yener (ex-officio).

Elza gave updates on upcoming ISITs. First, for ISIT 2015 in Hong Kong (Tse, Yeung), finances are in good shape, with a $60k loan from IEEE. Sponsorship and the venue have been finalized. Plenary speakers and tutorials have been confirmed. Submissions are now closed. The conference received 953 submitted papers, which will be handled by 153 TPC members. Semi-plenary sessions will be held at the conference. For ISIT 2016 (Guillen i Fabregas, Martinez, Verdu), the venue, banquet venue, and PCO have been finalized. For ISIT 2017 in Aachen (Kramer, Mathar), the dates June 25–30 have been fixed. An initial budget as well as potential sponsors have been determined. For ISIT 2018, there is strong interest from a team in Colorado (Mahesh Varanasi, Rockey Luo, Ali Pezeshki). The team is currently examining venue options and quotes. Other possibilities for 2018–2019 include Helsinki in 2018 (Vitaly Skacheck) and Paris in 2019 (Pablo Piantanida).

A discussion followed on ISIT 2018. It was suggested that having ISIT at a non-urban location can lead a memorable experience (e.g. Whistler, Canada for ISIT 1995). Colorado in the summer can be refreshing. On the other hand, some concerns were expressed regarding the high elevation in Colorado, and its effects on the health of attendees. It was suggested that the organizers closely examine the accessibility of venues in terms of travel times from major airports. Ali Pezeshki mentioned that the team will be visiting potential venues over the summer.

Elza next discussed the schedule for ISIT approvals. The Conference Committee recommends that approvals for ISITs be decided only during the annual BoG meeting during ISIT. Reasons for this include (1) larger BoG participation at the ISIT BoG meetings, (2) ease of attendance by the proposers, (3) ease of scheduling competing proposals. For ITWs, it is recommended that proposals be evaluated as they arrive. Since there are multiple ITWs during a year, this allows the BoG to act quickly on topics and venues.

A discussion followed. It was pointed out that approving ISITs only at the ISIT BoG meetings can lead to excessive delay if proposals are not ready to be presented then. It was decided that there should not be an official motion regarding this proposal. Rather, the proposal can serve as a guideline for the BoG.

Elza continued with an update on the upcoming ITWs. For ITW 2015 in Jerusalem, decisions on papers have been sent and the program is in place. There will be a panel chaired by Tony Ephremides. Workshop registration is now open. The contract has been delayed due to a lack of response from the IEEE. For ITW 2015 in Korea, the budget has been approved via email.

Elza continued with the proposal to hold ITW 2017 in Kaohsiung, Taiwan during Nov 5–8, 2017. The venue will be the KEC Kaohsiung Exhibition Center. The proposed General Co-Chairs are Po-Ning Chen, Gerhard Kramer, and Chih-Peng Li. The proposed Technical Program Co-Chairs are Hsiao-feng Lu, Stefan Moser, and Chih-Chun Wang. Workshop themes include information theory for content distribution, information theory and biology, coding for memories, and information theory and quantum communication. Hotel accommodation options, registration fees, a preliminary budget, a preliminary program, and preliminary deadlines were presented. A budget surplus of about 10% is expected. The conference committee recommends BoG approval of the ITW 2017 proposal.

In the brief discussion which followed, it was suggested that due to the low cost, the workshop could take place over 5 days rather than 3 days. This would allow for fewer parallel sessions. It was also pointed out that in the past, there would be one large ITW (with parallel sessions) and one single-track ITW per year.

Motion: To approve Kaohsiung, Taiwan, as the location for ITW 2017. Motion was passed.

Next, Elza mentioned that the Conference Committee has formed a new subcommittee to explore joint workshops to increase ties with other communities. The members of the subcommittee are Jeff Andrews, Michelle Effros (ex-officio), Elza Erkip, Ubli Mitra, and Alon Orlitsky.

Elza mentioned a new journal *IEEE Transactions on Molecular, Biological, and Multi-Scale Communications*, for which Ubli Mitra serves as Editor-in-Chief. Information on the journal can be found at https://www.ieee.org/membership-catalog/productdetail/showProductDetailPage.html?product=PER475-ELE.

Next, WiOpt 2015 has requested technical co-sponsorship from ITSoc. ITSoc has provided technical co- sponsorship since 2006. The Conference committee recommends BoG approval of this request.

Motion: To approve technical co-sponsorship for WiOpt 2015. Motion was passed.

Elza discussed the financial implications of technical co-sponsorship (TCS). Starting December 31, 2015, IEEE will charge $1000 per conference and $15 per paper for TCS. This cost can be borne either by ITSoc or by the co-sponsored conference. Currently, ITSoc pays for TCS as overhead, but it is not clear how this overhead is computed. Another option is for ITSoc to offer financial co-sponsorship in return for a small percentage of the conference revenue. The cost and revenue for the Society under this option are not clear.

In the brief discussion which followed, it was suggested that financial co-sponsorship may be beneficial for the Society due to the additional revenue gained. It remains unclear, however, how favorable conferences would be to financial co-sponsorship.

The meeting was adjourned at 4:30 PM Pacific Time.

In Memoriam, Robert B. Ash (1935–2015)

Michael Pursley

Robert Ash was taking his usual walk in Urbana, Illinois, on April 14, when he was struck in a crosswalk by a motorist and sustained injuries from which he died a few hours later. Bob was an excellent teacher and an extremely prolific writer. His scholarly publications came early and often.

Bob was born on May 20, 1935, in New York City. By age 26, he had received the Ph.D. degree from Columbia University and published his first coauthored book [1]. Bob's well-known book on information theory [2] was published when he was only 30 years old. By his 40th birthday, he had published five more books [3]–[7]. In all, Bob is the author or coauthor of nearly 20 books and sets of lecture notes, including [8]–[15]. Of all his publications, Bob was most proud of the books that he made available for free at his web site [16].

While he was an undergraduate student at Columbia, Bob met Carol Schwartz. Within a little more than a year, they decided to marry. Bob was not yet 21 years old, and according to New York state law he could marry only with his mother's permission. Fortunately, she gave it, and Bob and Carol were married on January 29, 1956. The newlyweds completed their undergraduate studies in May of that year. Bob received a B.S. degree in electrical engineering from Columbia and Carol received a B.A. degree in mathematics from Hunter College. Little did they know that 33 years later they would be coauthors of two books in mathematics.

Bob continued his studies at Columbia and was awarded M.S. and Ph.D. degrees in 1957 and 1960, respectively, both in electrical engineering. He was an Instructor during 1958–1960 and an Assistant Professor during 1960–1962. Among Bob's Ph.D. students at Columbia were Aaron Wyner, Eli Brookner, and Will Gersch.

In 1962, Bob and Carol Ash headed west. Bob was a Visiting Assistant Professor at the University of California, Berkeley, and Carol pursued graduate studies in mathematics and earned her M.A. degree from Berkeley in 1963. During the year at Berkeley, Bob was recruited by Mac Van Valkenburg for a faculty position at the University of Illinois at Urbana-Champaign. He served as an Associate Professor in EE at Illinois during 1963-68, he held a joint appointment between EE and the Department of Mathematics during 1965–68, and he became full time in math in 1968. He was promoted to Professor in 1971.

Anyone who has read Bob's book on information theory appreciates his thorough treatment of Markov information sources. In his review of the book, Jim Massey referred to the chapter on information sources as "a compilation of material on Markov information sources superior to any other known to this reviewer. The book would be worth having for this chapter alone." About the book as a whole, Massey said "this is a very scholarly treatise which will generously reward the reader for his time spent in its mastery."

It may surprise many readers to learn that Bob did not begin his career in information theory. Most of his early research was in circuit and system theory, as evidenced by his doctoral dissertation, "The Application of Linear Graph Theory to System Analysis," his first book [1], and his first journal articles [17]–[20]. In the early 1960s, Bob's interests shifted to information theory and coding, resulting in his book and such journal articles as [21]–[24]. The 1963 paper by Wyner and Ash [21] is considered to be one of the fundamental early contributions to the theory of what are now called convolutional codes. Included in the article are bounds on the smallest guard space required to correct all error bursts of a given maximum length.

Bob's 1965 article [24] provided one of the first examples of a channel model for which the strong converse fails. According to John Kieffer, one of Bob's Ph.D. students at Illinois, "the article was a partial inspiration for my own paper in the January 2007 *IEEE Transactions on Information Theory* in which I computed the ε-capacity for a class of averaged channels, including the one that Bob had analyzed. The problem in general remains unsolved as far as I know." The 1965 article relies heavily on the work of Jacob Wolfowitz, who was destined to join Bob at Illinois five years later.

One entry in the partial list of Bob's publications is quite distinct from the others in many respects. *The Calculus Tutoring Book* [8] is a mathematics book published by an engineering organization, it was written primarily by Carol Ash, and its diagrams are freehand line drawings. There is a carefully selected collection of examples and problems with solutions (the solutions alone occupy 106 pages), and the book's many hand-drawn illustrations make it a warm and inviting alternative to the usual calculus textbooks.

Over the years, I have benefited tremendously from Bob's books. During the time that I was at Illinois, I recommended that our graduate students take as many as possible of Bob's advanced courses in real analysis, measure theory, measure-theoretic probability theory, and random processes. Wayne Stark and Jim Lehnert were among the graduate students who followed that advice, and both rated Bob as a truly outstanding instructor. Wayne remarked, "Bob was a superb teacher, meticulously working out proofs, pointing out the potential pitfalls in proofs, and often adding humor as he lectured."

I can do no better than to close with the following remarks by John Kieffer: "Bob was a great advisor. He is the reason I work in information theory. He told me once that he wanted to be remembered as an expositor. He succeeded in that quite well."

Partial List of Publications by Robert B. Ash

[1] B. Friedland, O. Wing, and R. Ash, *Principles of Linear Networks*, McGraw-Hill, New York, 1961.

[2] R. B. Ash, *Information Theory*, Wiley, New York, 1965 (reprinted with corrections, Dover, New York, 1990).

[3] R. B. Ash, *Basic Probability Theory*, Wiley, New York, 1970.

[4] R. B. Ash, *Complex Variables*, Academic Press, New York, 1971 (2nd ed. with W. P. Novinger, Dover, Mineola, NY, 2004).

[5] R. B. Ash, *Real Analysis and Probability*, Academic Press, New York, 1972.

[6] R. B. Ash, *Measure, Integration, and Functional Analysis*, Academic Press, New York, 1972.

[7] R. B. Ash and M. F. Gardner, *Topics in Stochastic Processes*, Academic Press, New York, 1975.

[8] C. Ash and R. B. Ash, *The Calculus Tutoring Book*, IEEE Press, Piscataway, NJ, 1986.

[9] R. J. McEliece, R. B. Ash, and C. Ash, *Introduction to Discrete Mathematics*, Random House, New York, 1989.

[10] R. B. Ash, *Real Variables with Basic Metric Space Topology*, IEEE Press, Piscataway, NJ, 1993 (revised edition, Dover, Mineola, NY, 2009).

[11] R. B. Ash, *A Primer of Abstract Mathematics*, Mathematical Association of America, Washington, DC, 1998.

[12] R. B. Ash, *Probability and Measure Theory*, 2nd Ed., with contributions by C. Doleans-Dade, Academic Press, San Diego, 2000.

[13] R. B. Ash, *Basic Abstract Algebra*, Dover, Mineola, NY, 2007.

[14] R. B. Ash, *A Course in Algebraic Number Theory*, Dover, Mineola, NY, 2010.

[15] R. B. Ash, *Statistical Inference: A Concise Course*, Dover, Mineola, NY, 2011.

[16] R. B. Ash, *Books on Line*, http://www.math.uiuc.edu/~r-ash/

[17] R. B. Ash and W. H. Kim, "On realizability of a circuit matrix," *IRE Transactions on Circuit Theory*, vol. 6, no. 2, pp. 219–223, June 1959.

[18] D. E. Rosenheim and R. B. Ash, "Increasing reliability by the use of redundant machines," *IRE Transactions on Electronic Computers*, vol. EC-8, no. 2, pp. 125–130, June 1959.

[19] R. B. Ash, "Topology and the solution of linear systems," *Journal of the Franklin Institute*, pp. 453–463, December 1959.

[20] R. Ash, W. H. Kim, and G. M. Kranc, "A general flow graph technique for the solution of multiloop sampled systems," *Transactions of the ASME, Journal of Basic Engineering*, pp. 360–366, June 1960.

[21] A. D. Wyner and R. B. Ash, "Analysis of recurrent codes," *IEEE Transactions on Information Theory*, vol. 9, no. 3, pp. 143–156, July 1963.

[22] R. B. Ash "Capacity and error bounds for a time-continuous Gaussian channel," *Information and Control*, vol. 6, pp. 14–27, 1963.

[23] R. B. Ash "Further discussion of a time-continuous Gaussian channel," *Information and Control*, vol. 7, pp. 78–83, 1964.

[24] R. B. Ash, "A simple example of a channel for which the strong converse fails," *IEEE Transactions on Information Theory*, vol. 11, no. 3, pp. 456–457, July 1965.

In Memoriam, Carlos R.P. Hartmann (1940–2015)

Yunghsiang S. Han and Pramod K. Varshney

Dr. Carlos R.P. Hartmann, 75, was involved in a freak accident on April 18, 2015 in which he sustained severe injuries. He could not recover from them and died at University Hospital in Syracuse, NY on April 21, 2015. Carlos, a Professor at Syracuse University, was a true scholar, enthusiastic teacher, and a dedicated administrator.

Carlos received his bachelor's and master's degrees from the Instituto Technologico de Aeronautica in Sao Paulo, Brazil, and a Ph.D. from the University of Illinois at Urbana-Champaign under Dr. Robert T. Chien. He joined the faculty of Syracuse University in 1970, where he remained until his death. He became the Director of the former School of Computer and Information Science (CIS) in 1992, and oversaw the merger of the School of CIS with the former Department of Electrical and Computer Engineering in 1996. He then served as department chair of the newly formed Department of Electrical Engineering and Computer Science until 2011. He was a Fellow of the IEEE and served as Associate Editor of the IEEE Transactions on Information Theory.

Carlos was known for his innovative research in information and coding theory. In 1972, he and Kenneth K. Tzeng discovered a generalization of the BCH bound that came to be called the Hartmann-Tzeng bound. In 1976, he and Luther D. Rudolph proposed a new optimal symbol-by-symbol decoding algorithm for linear block codes that remains to this day one of the best symbol-by-symbol decoding algorithms. In 1982, he and Pramod K. Varshney along with other colleagues published an information theoretic approach for the design of decision trees that had a great impact on pattern recognition applications. In 1984, Carlos and Lev B. Levitin presented a new minimum distance decoding algorithm for linear block codes, thus addressing a very difficult problem. The now-famous algorithm is known as the zero-neighbors algorithm. In 1993, he and his Ph. D. student, Yunghsiang S. Han, developed a sequential-type algorithm based on Algorithm A* from artificial intelligence. At the time, this algorithm drew a lot of attention since it was the most efficient maximum-likelihood decoding algorithm for binary linear block codes. A list of some of his important publications follows.

Partial List of Publications by Carlos R. P. Hartmann

[1] C. R. P. Hartmann, K. K. Tzeng, and R. T. Chien, "Some Results on the Minimum Distance Structure of Cyclic Codes," *IEEE Transactions on Information Theory*, pp. 402–409, May 1972.

[2] C. R. P. Hartmann and K. K. Tzeng, "Generalizations of the BCH Bound," *Information and Control*, pp. 489–498, June 1972.

[3] L. D. Rudolph and C. R. P. Hartmann, "Decoding by Sequential Code Reduction," *IEEE Transactions on Information Theory*, pp. 549–555, July 1973.

[4] C. R. P. Hartmann and L. D. Rudolph, "An Optimum Symbol-by-Symbol Decoding Rule for Linear Codes," *IEEE Transactions on Information Theory*, pp. 514–517, September 1976.

[5] C. R. P. Hartmann, L. D. Rudolph, and K. G. Mehrotra, "Asymptotic Performance of Optimum Bit-by-Bit Decoding for the White Gaussian Channel," *IEEE Transactions on Information Theory*, pp. 520–522, July 1977.

[6] L. D. Rudolph, C. R. P. Hartmann, T.-Y. Hwang, and N. Duc, "Algebraic Analog Decoding of Linear Binary Codes," *IEEE Transactions on Information Theory*, pp. 430–440, July 1979.

[7] C. R. P. Hartmann, P. K. Varshney, K. G. Mehrotra, and C. Gerberich, "Application of Information Theory to the Construction of Efficient Decision Trees," *IEEE Transactions on Information Theory*, pp. 565–577, July 1982.

[8] L. B. Levitin and C. R. P. Hartmann, "A New Approach to the General Minimum Distance Decoding Problem: The Zero-Neighbours Algorithm," *IEEE Transactions on Information Theory*, pp. 378–384, May 1985.

[9] J. Gao, L. D. Rudolph, and C. R. P. Hartmann, "Iteratively Maximum Likelihood Decodable Spherical Codes and a Method for Their Construction," *IEEE Transactions on Information Theory*, pp. 480–485, May 1988.

[10] Y. S. Han, C. R. P. Hartmann, and C-C. Chen, "Efficient Priority-First Search Maximum-Likelihood Soft-Decision Decoding of Linear Block Codes," *IEEE Transactions on Information Theory*, pp. 1514–1523, September, 1993.

[11] Y. S. Han, and C. R. P. Hartmann, "The Zero-Guards Algorithm for General Minimum Distance Decoding Problem," *IEEE Transactions on Information Theory*, pp. 1655–1658, September, 1997.

[12] Y. S. Han, C. R. P. Hartmann, and K. G. Mehrotra, "Decoding Linear Block Codes Using a Priority-First Search: Performance Analysis and Suboptimal Version," *IEEE Transactions on Information Theory*, pp. 1233–1246, May, 1998.

CALL FOR PAPERS

FOUNDATIONS & APPLICATIONS OF SCIENCE OF INFORMATION

Special Issue of *Proceedings of IEEE*

Special Issue Editors: Thomas Courtade (University of California, Berkeley), Ananth Grama (Purdue University), Michael Mahoney (University of California, Berkeley), and Tsachy Weissman (Stanford University).

Authors are invited to submit manuscripts presenting recent advances in the core foundations of the *Science of Information* and its applications to diverse fields, including Economics, Life Sciences, Communication Systems, and Data Analytics. Topics of interest span theoretical foundations (modeling and analysis), algorithms, as well as application studies.

Scope of the Issue The issue covers the following topics: (i) Core foundations of science of information; (ii) Applications to large-scale data handling (compression, sampling, analytics on data summaries); (iii) Emerging communications systems (including cyber-physical systems); (iv) Applications in life sciences; (v) Applications in social sciences and economics; and (vi) Formal approaches to data analytics. Other topics closely related to science of information will also be considered.

What/ Where to Submit: Submitted manuscripts may not exceed ten (10) single-spaced double-column pages using 10-point size font on 8.5x11 inch pages (IEEE conference style), including figures, tables, and references. Submissions should be made through ScholarOne Manuscripts (`https://mc.manuscriptcentral.com/pieee`). For most information on the special issue, and detailed submission information, please visit the Center for Science of Information web site at `http://soihub.org`.

Review of Manuscripts and Important Dates All submitted manuscripts will be peer reviewed for scope, correctness, and significance.
Receipt of Full Papers: August 31, 2015
Notification of Review Decisions and Revisions: Dec 15, 2015
Submission of Revised Manuscripts: Feb 28, 2016

Questions and Queries. Please direct all questions and queries to Bob Brown at bobbrown@purdue.edu

Center for Science of Information
NSF Science and Technology Center

Workshop Organizers

Rafael F. Schaefer
H. Vincent Poor
Holger Boche

TPC Members

Mario Goldenbaum
Eduard A. Jorswieck
Kittipong Kittichokechai
O. Ozan Koyluoglu
Gerhard Kramer
Lifeng Lai
Yingbin Liang
Pin-Hsun Lin
Derrick Wing Kwan Ng
Tobias J. Oechtering
Walid Saad
Aydin Sezgin
Andrew Thangaraj
Xiangyun Zhou

2015 IEEE CNS 2nd Workshop on Physical-layer Methods for Wireless Security Workshop

The **2nd Workshop on Physical-layer Methods for Wireless Security** will take place during CNS 2015 in Florence, Italy, Sep 28-30, 2015. Previously unpublished contributions in wireless security based on physical-layer methods are solicited, including (but not limited to):

- Secrecy capacity of wireless channels
- Secure communication under adversarial attacks
- Practical code design for physical layer security
- Secure cross-layer design techniques
- Secure communication with an uncertain physical layer
- Information theoretic approaches for authentication
- Jamming-assisted secure wireless transmission
- Cooperative secure communications
- Secret key generation and agreement
- Secret key capacity of wireless channels
- Practical and implementation issues

The workshop features two keynotes given by world leading researchers in the field:

- Matthieu Bloch
- Eduard Jorswieck

Submitted papers should be of sufficient length and detail for review by experts in the field. Papers should be submitted for review through EDAS. Final papers will be limited to 6 pages in length in the standard IEEE conference paper format. Accepted papers will be published in IEEE Xplore.

Key dates

Paper submission deadline	**July 10, 2015 (extended)**
Acceptance notification	August 3, 2015
Camera-ready version due	August 10, 2015
Workshop date	September 30, 2015

For more information, please contact the workshop organizers

Rafael F. Schaefer, H. Vincent Poor
Princeton University
Princeton, NJ, USA
{rafaelfs,poor}@princeton.edu

Holger Boche
Technische Universität München
Munich, Germany
boche@tum.de

FIFTY-THIRD ANNUAL ALLERTON CONFERENCE ON COMMUNICATION, CONTROL, AND COMPUTING

September 29 2015 – Opening Tutorials
September 30-October 2, 2015 – Conference Sessions

The Fifty-Third Annual Allerton Conference on Communication, Control, and Computing will kick off with two Opening Tutorials being held on Tuesday, September 29, 2015 at the Coordinated Science Laboratory. The Conference sessions will start on Wednesday, September 30, 2015 through Friday, October 2, 2015, at the Allerton Park and Conference Center. The Allerton House is located twenty-six miles southwest of the Urbana-Champaign campus of the University of Illinois in a wooded area on the Sangamon River. It is part of the fifteen-hundred acre Robert Allerton Park, a complex of natural and man-made beauty designated as a National natural landmark. Allerton Park has twenty miles of well-maintained trails and a living gallery of formal gardens, studded with sculptures collected from around the world.

Papers presenting original research are solicited in the areas of communication systems, communication and computer networks, detection and estimation theory, information theory, error control coding, source coding and data compression, network algorithms, control systems, robust and nonlinear control, adaptive control, optimization, dynamic games, multi-agent systems, large-scale systems, robotics and automation, manufacturing systems, discrete event systems, multivariable control, computer vision-based control, learning theory, cyber-physical systems, security and resilience in networks, VLSI architectures for communications and signal processing, and intelligent transportation systems.

PLENARY LECTURE: Professor **Martin Vetterli** of the School of Computer and Communication Sciences, Ecole Polytechnique Fédérale de Lausanne, will deliver this year's plenary lecture. It is scheduled for Friday, October 2, 2015 at the Allerton Park and Retreat Center.

OPENING TUTORIAL LECTURES: Professor **Andrea Montanari**, Stanford University, and Professor **Francis Bach**, Laboratoire d'Informatique de l'Ecole Normale Superieure, will both present a tutorial lecture on Tuesday, September 29, 2015 at the Coordinated Science Laboratory, University of Illinois at Urbana-Champaign.

INFORMATION FOR AUTHORS: Regular papers suitable for presentation in twenty minutes are solicited. Regular papers will be published in full (subject to a maximum length of eight 8.5" x 11" pages, in two column format) in the Conference Proceedings. Only papers that are actually presented at the conference and uploaded as final manuscripts can be included in the proceedings, which will be available after the conference on IEEE Xplore.

For reviewing purposes of papers, a title and a five to ten page extended abstract, including references and sufficient detail to permit careful reviewing, are required.

Manuscripts can be submitted during **June 15-July 6, 2015** with the submission deadline of July 6 being firm. Please follow the instructions at the Conference website: http://www.csl.uiuc.edu/allerton/**.**

Authors will be notified of acceptance via e-mail by August 7, 2015, at which time they will also be sent detailed instructions for the preparation of their papers for the Proceedings.

Final versions of papers to be presented at the conference are required to be submitted electronically by October 4, 2015 in order to appear in the Conference Proceedings and IEEE Xplore.

Conference Co-Chairs: Angelia Nedich and Minh Do
Email: *allerton-conf@illinois.edu* URL: www.csl.illinois.edu/allerton/

COORDINATED SCIENCE LABORATORY AND THE DEPARTMENT OF ELECTRICAL AND COMPUTER ENGINEERING

University of Illinois at Urbana-Champaign

CALL FOR PAPERS

2016 Australian Communications Theory Workshop (AusCTW'16)

Melbourne, Victoria
20 - 22 January 2016

Workshop Announcement

Monash University is pleased to host the 16th Australian Communications Theory Workshop. The workshop will bring together researchers and post-graduate students in physical layer communications and information theory for two and a half days of technical presentations, tutorials and networking. Past workshops have provided formal and informal environments to successfully foster collaborative research.

Invited Talks

Invited talks will be given by leading researchers and outstanding graduate students.

Peer Reviewed Contributed Papers

Papers presenting original and unpublished contributions are solicited (maximum length is 6 pages). All contributed papers will be subject to peer review. Topics of interest include, but are not limited to:

- coded modulation
- coding theory and practice
- communication systems
- channel modelling
- detection and estimation
- ultra-wide band communications
- OFDM & DMT processing techniques
- blind signal separation techniques
- information theory and statistics
- network coding
- compressed sensing
- iterative decoding algorithms
- multiuser detection
- cross-layer PHY-MAC-NET optimisation
- DSP for communications
- molecular, biological and multi-scale communications

We are pleased to announce technical co-sponsorship by the IEEE Information Theory Society ACT Section IT Chapter. All accepted papers are to be presented as posters during the conference. Accepted and appropriately presented papers will appear in full in the conference proceedings and will be submitted to IEEE*Xplore* for archival. Please see conference website (http://ausctw2016.eng.monash.edu/) for paper submission details.

Non-Peer Reviewed Contributions

To facilitate maximum participation, all attendees are invited to present a poster at the workshop for which only an abstract need be submitted. Abstracts are *not* subject to peer review and appear in the workshop *book of abstracts*. Please see conference website for abstract submission details.

2016 Australian Information Theory School

The 2016 Australian Information Theory School will be held at the same venue on 17-19 January 2015. Please see conference website for registration details (http://ausits2016.eng.monash.edu/).

Key Dates

Paper submission deadline:
Friday, October 16, 2015

Notification of decisions:
Friday, November 20, 2015

Camera-ready papers due:
Friday, December 18, 2015

Poster abstracts due:
Friday, December 18, 2015

Early registration closes:
Friday, January 8, 2015

MONASH University IEEE

Call for Papers

2016 International Zurich Seminar on Communications

March 2 – 4, 2016

The 2016 International Zurich Seminar on Communications will be held at the Hotel Zürichberg in Zurich, Switzerland, from Wednesday, March 2, through Friday, March 4, 2016.

High-quality original contributions of both applied and theoretical nature are solicited in the areas of:

Wireless Communications	Optical Communications
Information Theory	Fundamental Hardware Issues
Coding Theory and its Applications	Network Algorithms and Protocols
Detection and Estimation	Network Information Theory and Coding
MIMO Communications	Cryptography and Data Security

Invited speakers will account for roughly half the talks. In order to afford the opportunity to learn from and communicate with leading experts in areas beyond one's own specialty, no parallel sessions are anticipated. All papers should be presented with a wide audience in mind.

Papers will be reviewed on the basis of a manuscript (A4, not exceeding 5 pages) of sufficient detail to permit reasonable evaluation. Authors of accepted papers will be asked to produce a manuscript not exceeding 5 pages in A4 double column format that will be published in the Proceedings. Authors will be allowed twenty minutes for presentation.

The deadline for submission is **September 27, 2015**.

Additional information will be posted at

`http://www.izs.ethz.ch/`

We look forward to seeing you at IZS.

Amos Lapidoth and Stefan M. Moser, Co-Chairs.

PRINCETON

Call for Papers CISS 2016

50th Annual Conference on Information Sciences and Systems

March 16, 17, & 18, 2016

Princeton University - Department of Electrical Engineering

and Technical Co-sponsorship with

IEEE Information Theory Society

Authors are invited to submit previously unpublished papers describing theoretical advances, applications, and ideas in the fields of: information theory, coding theory, communication, networking, signal processing, image processing, systems and control, security and privacy, machine learning and statistical inference.

Electronic submissions of up to 6 pages (in Adobe PDF format) including 3-4 keywords must be submitted by **December 15, 2015**. Submissions should be of sufficient detail and length to permit careful reviewing. Authors will be notified of acceptance no later than **January 11, 2016**. Final manuscripts of accepted papers are to be submitted in PDF format no later than **January 25, 2016**. These are firm deadlines that will permit the distribution of Electronic Proceedings at the Conference. Accepted Papers will be allotted 20 minutes for presentation, and will be reproduced in full (up to six pages) in the conference proceedings. IEEE reserves the right to exclude a paper from post-conference distribution (e.g., removal from IEEE Xplore) if the paper is not presented at the conference.

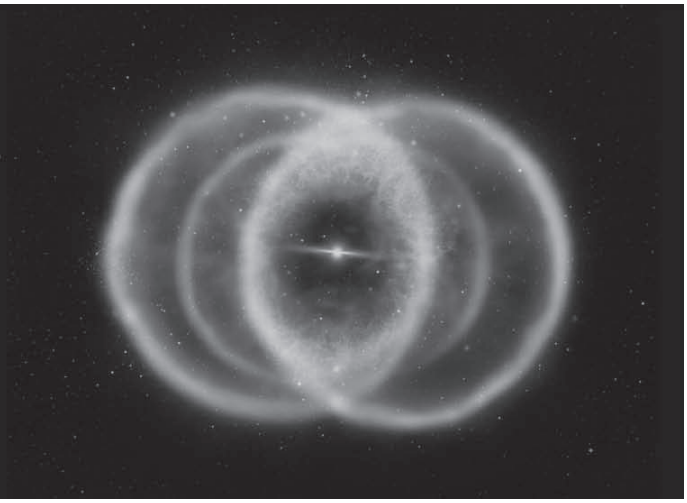
For more information visit us at: http://ee-ciss.princeton.edu/

CONFERENCE COORDINATOR	PROGRAM DIRECTORS	IMPORTANT DATES
Lisa Lewis Dept. of Electrical Engineering Princeton University Princeton, NJ 08544 Phone: (609) 258-6227 Email: CISS@princeton.edu	**Prof. Mung Chiang** **Prof. Peter Ramadge** Dept. of Electrical Engineering Princeton University Princeton, NJ 08544	**Submission deadline:** **December 15, 2015** **Notification of acceptance:** **January 11, 2016** **Final manuscript due:** **January 25, 2016**

Nexus of Information and Computation Theories

Institut Henri Poincaré
Spring 2016 Thematic Program
http://csnexus.info

January 25 - April 1, 2016
Paris, France



About the Program

Recently, a number of advances in the theory of computation have been made by using information-theoretic arguments. Conversely, some of the most exciting ongoing work in information theory has focused on problems with a computational component. The primary goal of this three-month IHP thematic program is to explore the rich interplay between information theory and the theory of computation, and ultimately create new connections and collaborations between both scientific communities.

- **Core of the Program:** eight weeks, split across four major themes (see below for details).
- **Central Workshop (February 29 - March 4):** broadly spanning the interface between CS and IT.
- **Tutorial Week (January 25 - 29) at CIRM (Marseille):** designed for students, but all are welcome.

Registration

Researchers and students who are considering attending any part of the program **must register on the website as soon as possible.** Registration is free but mandatory given the limited number of places. During the registration process, one can choose amongst the thematic weeks and/or the central workshop.

Program Organizers

Mark Braverman (Princeton)
Bobak Nazer (Boston University)
Anup Rao (University of Washington)
Aslan Tchamkerten (Telecom Paristech)

About IHP

The Henri Poincare Institute (IHP) is a research institute dedicated to mathematics and theoretical physics. Each quarter, the institute hosts a thematic program that brings together researchers from a particular discipline to foster the exchange of ideas.

ihp Institut Henri Poincaré

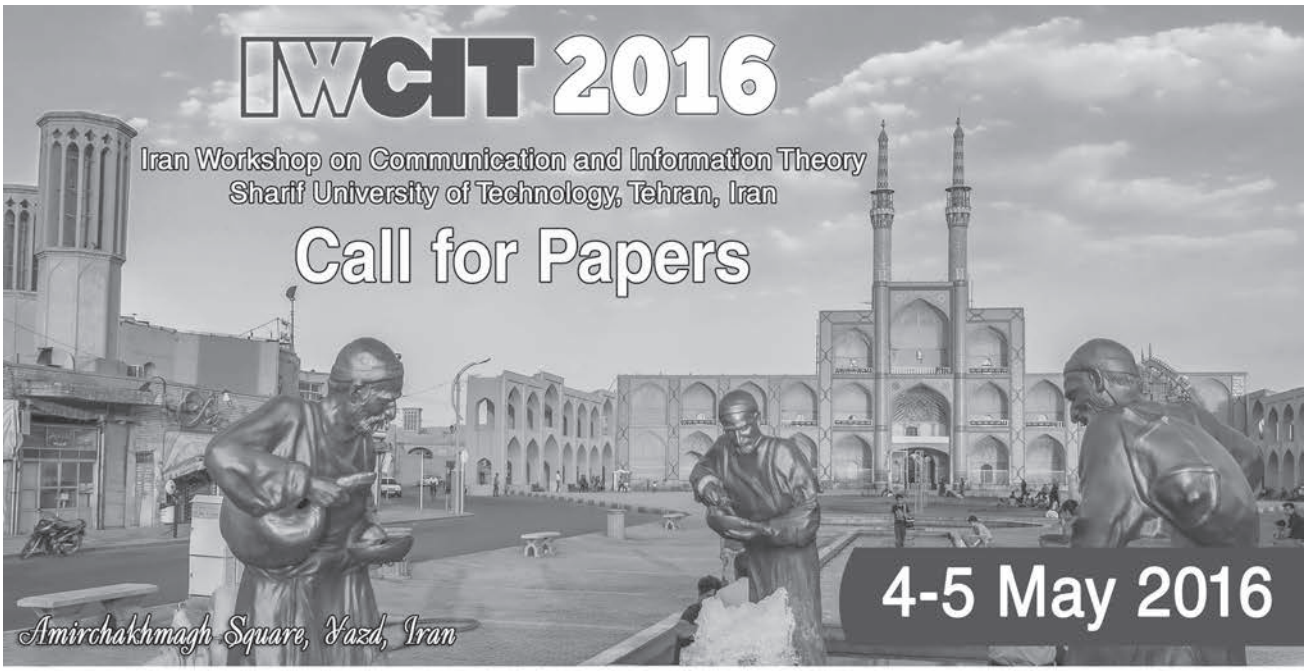
Theme Organizers

Distributed Computation (February 1 - 12)
Péter Gàcs (Boston Univeristy)
János Körner (Sapienza University of Rome)
Leonard Schulman (Caltech)

Fundamental Inequalities (February 15 - 26)
Kasper Green Larsen (Aarhus University)
Babak Hassibi (Caltech)
Iordanis Kerenidis (University Paris Diderot 7)
Raymond Yeung (Chinese University of Hong Kong)

Inference Problems (March 7 - 18)
Amit Chakrabarty (Dartmouth College)
Andrew McGregor (UMass Amherst)
Henry Pfister (Duke University)
Devavrat Shah (MIT)
David Woodruff (IBM)

Secrecy and Privacy (March 21 - April 1)
Prakash Narayan (University of Maryland)
Aaron Roth (University of Pennsylvania)
Anand Sarwate (Rutgers University)
Vinod Vaikuntanathan (MIT)
Salil Vadhan (Harvard University)



The fourth Iran Workshop on Communication and Information Theory will take place at Sharif University of Technology, on May 4th and May 5th 2016, 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, 2016
- Notification of Acceptance: March 15th, 2016
- Camera Ready Submission: April 15th, 2016

General Chairs:
- Aref, M. R.
Sharif University of Technology
- Sharafat, A. R.
Tarbiat Modares University

Technical Program Chair:
- Salehi, J. A.
Sharif University of Technology

Executive Chairs:
- Gohari, A.
Sharif University of Technology
- Seyfe, B.
Shahed University

Contact Us :
- Email:
info@iwcit.org
iwcit@sharif.ir
- Address:
Secretariat of IWCIT 2016 Room 503 Dept. of Electrical Engineering Sharif University of Techology Tehran, Iran
Tel : +98 21 66165910

IEEE IRAN SECTION

WWW . IWCIT . ORG

2016 IEEE International Symposium on Information Theory

Barcelona, Spain | July 10-15, 2016

Call for papers

The 2016 IEEE International Symposium on Information Theory will take place in Barcelona, Spain, from July 10 to 15, 2016. A lively city, known for its style, architecture, culture, gastronomy and nightlife, Barcelona is one of the top tourist destinations in Europe. 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
Pattern Recognition and Learning
Physical Layer Security
Quantum Information and Coding Theory
Sequences
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. 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 24, 2016, at 11:59 PM, Eastern Time (New York, USA). Acceptance notifications will be sent out by April 3, 2016.

We look forward to your participation in ISIT in the centennial year of Claude Shannon's birth.

General Co-Chairs
Albert Guillén i Fàbregas
Alfonso Martinez
Sergio Verdú

TPC Co-Chairs
Venkat Anantharam
Ioannis Kontoyiannis
Yossef Steinberg
Pascal Vontobel

Finance
Stefan Moser

Publications
Tobias Koch

http://www.isit2016.org/

Conference Calendar

DATE	CONFERENCE	LOCATION	WEB PAGE	DUE DATE
September 23–25, 2015	**Mathematical Tools of Information-Theoretic Security Workshop.**	Huawei Mathematical and Algorithmic Sciences Lab, Paris, France.	http://www.laneas.com/events/itsec-workshop2015	—
September 29–October 2, 2015.	**53rd Annual Allerton Conference on Communication, Control, and Computing.**	Allerton Retreat Center, Monticello, Illinois, USA.	http://allerton.csl.illinois.edu	Passed
September 30, 2015.	**2nd Workshop on Physical-Layer Methods for Wireless Security—IEEE CNS Conference.**	Florence, Italy.	http://www.princeton.edu/~rafaelfs/CNS2015/	Passed
October 11–15, 2015	**IEEE Information Theory Workshop (ITW 2015).**	Jeju Island, Korea	http://www.itw2015.org	Passed
October 18–20, 2015	**56th Annual IEEE Symposium on Foundations of Computer Science (FOCS 2015).**	Berkeley, California, USA.	http://www.cs.cmu.edu/~venkatg/FOCS-2015-cfp.html	Passed
December 6–10, 2015	**IEEE GLOBECOM.**	San Diego, California, USA	http://globecom2015.ieee-globecom.org	Passed
December 14–16, 2015	**IEEE Global Conference on Signal and Information Processing (GlobalSIP).**	Orlando, Florida, USA	http://2015.ieeeglobalsip.org	Passed
January 20–22, 2016	**Australian Communications Theory Workshop (AusCTW).**	Melbourne, Australia	http://www.ausctw.org.au	October 16, 2015
January 25–April 1, 2016	**IHP Thematic Program on the Nexus of Information and Computation Theories.**	Paris, France	http://csnexus.info	—
March 2–4, 2016	**2016 International Zurich Seminar on Communications.**	Zurich, Switzerland	http://www.izs.ethz.ch	September 27, 2015
March 16–18, 2016	**50th Annual Conference on Information Sciences and Systems.**	Princeton University	http://ee-ciss.princeton.edu	December 15, 2015
May 4–5, 2016	**4rd Iran Workshop on Communication and Information Theory (IWCIT).**	Sharif University of Technology, Tehran, Iran.	http://www.iwcit.org	January 11, 2016
July 10–15, 2016	**2016 IEEE International Symposium on Information Theory.**	Barcelona, Spain	http://www.isit2016.org	January 24, 2016

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