IEEE Information Theory Society Newsletter

Vol. 67, No. 1, March 2017 EDITOR: Michael Langberg, Ph.D. ISSN 1059-2362

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

President's Column

Rüdiger Urbanke

As I type this column with my little hands one thing is clear: If anything, this world needs more jokes ... but at the right places! In this respect, my perhaps biggest challenge will be to follow the lead of our previous president.

The Shannon Centenary presented a great opportunity to introduce Information Theory to a broad audience. I would like to thank the many volunteers who organized events all around the globe. The list of events is impressive: http://www.itsoc.org/resources/Shannon-Centenary.

I am also happy to report that the preparations to shoot major portions of the Shannon Documentary are frentically under way. Mark Levinson and his crew are about to start filming at Shannon's house in Massachusetts. With the help of Claude's family, Mark has managed to collect many of Shannon's old ``toys'' and is recreating his famous play room. The master himself will be played by John Hutton https://www.youtube.com/watch?v=JrAtV5a5aT4 Although much of the shooting will be done soon, editing a documentary is a long process. But I am hoping that at ITA 2018 we will be able to enjoy bits and bites—the movie premiere and unlimited popcorn, and most importantly for an IT premiere, a green carpet!

The parties are mostly over, but our work is not done. Like any society we have to keep reinventing ourselves to stay relevant. Our crown jewel, the Transactions on Information Theory has been losing clicks and impact factor over the years. There is no reason to panic. The IT Transactions is still one of the most prestigious IEEE journals and we could not wish for better Editors-in-Chief. We continue to publish only top articles—extreme vetting at its finest! Some of the developments are natural consequences of how thoroughly our society has embraced open access models. It is likely that many people download our papers from arXiv rather than Xplore. This of course takes a toll on our click rate but it also represents an opportunity for our Society to broaden our reach. And we have been so successful technically that communications is increasingly becoming a commodity. Both of these developments are in principle positive points and reasons to celebrate!

But it is a good reminder that we cannot tread still and that we have to continue to reach out and take advantage of new opportunities. ITA is a great example of how we can branch out and connect to other areas. The many Information Theory Schools that take place now on several continents annually and typically have a broad range of topics also play a crucial role. And a quick look at NIPS program shows that our members are already contributing significantly to machine learning. We should continue to support anything that accelerates and reinforces this process. Here is another thing I personally would like to see: More "work" and interaction during workshops and more willingness to experiment with different formats.

It is important in this context to recall that Jeff Andrews and Elza Erkip are heading a BoG ad-hoc committee exploring the creation of a new publication connecting information theory to other topics and communities. Two concrete proposals are on the table. One is a Magazine, which would replace the Newsletter, be archival, and contain more tutorial and vision articles on new topics with an emphasis on emerging new topics and applications of information theory. The other is a Special Topics journal, which would consist solely of special issues around focused topics, each special issue led by a unique team of guest editors. The goals would be (i) to provide a venue for faster publication, (ii) gain exposure for emerging topics in IT, and (iii) relieve some of the pressure on Trans IT, by also publishing special issues on

(continued on page 20)

From the Editor

Michael Langberg

Dear colleagues,

Our spring issue opens with Rüdiger Urbanke's first column as the IT society president. Please join me in warmly welcoming Rüdiger and in wishing him and our community a fruitful and prosperous year. We continue with several exciting announcements of recent award winners from our community, a list of recent elevations of members of our community to the grade of IEEE fellow, and a list of new elected members to the IT Society Board of Governors. Congratulations to all! We are all honored as a community.

This issue includes an intriguing survey article, "Reflection and Summary of the paper: The Capacity Region of the Two-Receiver Gaussian Vector Broadcast Channel with Private and Common Messages", by this years (co-)winners of the IT Society Paper Award, Yanlin Geng and Chandra Nair, which outlines an elegant and very useful technique for proving the optimality of Gaussian distributions from the single-letterization property of the functionals involved. Many thanks to the authors for their significant efforts in preparing this excellent contribution.

The issue continues with a number of regular columns and reports including Tony Ephremides's Historian's column; our ``Students' Corner" column presenting two essays, by Cheuk Ting Li and Nir Weinberger, reflecting on this years IEEE Jack Keil Wolf ISIT Student Paper Award; the column ``From the field" by Hiroshi Kamabe, on the IEEE Information Theory Society Japanese Chapter; a report on the "Munich Workshop on Information Theory of Optical Fiber (MIO 2016)" by Tobias Fehenberger, Javier García, René Essiambre, and Gerhard Kramer; a report by Deniz Gündüz, and Jossy Sayir on the ``2016 Information Theory Workshop" that took place at Cambridge, UK; a report on the ``UCSD Shannon Centenary Celebration" by Paul Siegel; a report on the Shannon Centenary Workshop in Armenia "From Information Age to Big Data Era", by Ashot N. Harutyunyan, Davit A. Sahakyan, and A.J. Han Vinck; a report on the "2016 IEEE Shannon Centennial Workshop on Communications and Information Theory (SCWCIT 2016)", by Chinmoy Saha, that took place in Thiruvananthapuram, Kerala, India; minutes from the IEEE Information Theory Society Board of Governors meeting this fall in Chicago; and a list of recent articles published in the IEEE Transactions on Information Theory and in Problems of Information Transmission.

With sadness, we conclude this column with a tribute to Paul Calvin Shields and to Hans Witsenhausen, two prominent and active members of our community, who passed away recently.

continued on page 4

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

Congratulations to the members of our community that have recently received the most prestigious awards of the IEEE and to those that have been recently elevated to the grade of IEEE Fellow!

We are all honored as a community!

IEEE Simon Ramo Medal: John Baras

The IEEE Simon Ramo Medal is awarded for exceptional achievement in systems engineering and systems science, sponsored by *Northrop Grumman Corporation*, to **JOHN BARAS** (LFIEEE)—Professor, University of Maryland, College Park, Maryland, USA. *For exceptional contributions to the conception and commercialization of internet- over-satellite systems, and for leadership in model-based engineering, systems science, and engineering research*.

IEEE Medal of Honor: Kornelis (Kees) A. Schouhamer Immink.

The IEEE Medal of Honor is awarded for an exceptional contribution or an extraordinary career in IEEE fields of interest, sponsored by the *IEEE Foundation*, to **KORNELIS (KEES) A. SCHOUHAMER IMMINK** (LFIEEE)—President, Turing Machines Inc., Rotterdam, The Netherlands. *For pioneering contributions to video, audio, and data recording technology, including compact disc, DVD, and Blu-ray*.

IEEE Alexander Graham Bell Medal: H. Vincent Poor

The IEEE Alexander Graham Bell Medal is awarded for exceptional contributions to communications and networking sciences and engineering, sponsored by *Nokia Bell Labs,* to **H. VINCENT POOR** (FIEEE)—Michael Henry Strater University Professor of Electrical Engineering, Princeton University, Princeton, NJ USA. *For fundamental contributions to signal processing and its application to digital communications.*

IEEE Koji Kobayashi Computers And Communications Award: Kannan Ramchandran

The IEEE Koji Kobayashi computers and communications award recognizes outstanding contributions to the integration of computers and communications—sponsored by NEC Corporation—to **KANNAN RAMCHANDRAN** (FIEEE)—Professor, University of California, Berkeley, Berkeley, California, USA. *For pioneering contributions to the theory and practice of distributed source and storage coding*.

IEEE Richard W. Hamming Medal: Shlomo Shamai

The IEEE Richard W. Hamming Medal is awarded for exceptional contributions to information sciences, systems, and technology, sponsored by *Qualcomm, Inc.*, to **SHLOMO SHAMAI** (FIEEE)—Professor, Technion-Israel Institute of Technology, Haifa, Israel. *For fundamental contributions to information theory and wireless communications*.

IEEE Jack S. Kilby Signal Processing Medal: Martin Vetterli

The IEEE Jack S. Kilby Signal Processing Medal is awarded for outstanding achievements in signal processing, sponsored by *Texas Instruments, Inc*., to **MARTIN VETTERLI** (FIEEE)—Professor, EPFL, Lausanne, Switzerland. *For fundamental contributions to advanced sampling, signal representations, and multirate and multiresolution signal processing*.

2017 Newly Elevated Fellows

Raviraj Adve
University of Toronto, Toronto, ON, Canada
for development of signal processing techniques for airborne radar

Alexei Ashikhmin
Bell Labs – Alcatel-Lucent New Providence, NJ, USA
for contributions to information theory and communication theory

Huaiyu Dai
North Carolina State University Raleigh, NC, USA
for contributions to MIMO communications and wireless security

Xinzhou Dong
Tsinghua University, China Beijing, China
for contributions to traveling wave-based transmission line protection and fault location

James Fowler
Mississippi State University Mississippi State, MS, USA
for contributions to lossy source coding and dimensionality reduction of multidimensional data

Michael Gastpar
Ecole Polytechnique Federale de Lausanne Lausanne, Switzerland
for contributions to network information theory

Stephen Hanly
Macquarie University Sydney, NSW, Australia
for contributions to capacity analysis and optimization of wireless communication networks

Masahito Hayashi
Nagoya University Nagoya, Japan

for contributions to Shannon theory, information-theoretic security, and quantum information theory

Amir Khandani
University of Waterloo Waterloo, ON, Canada
for contributions to resource allocation and interference management in network information theory

Witold Krzymien
University of Alberta Edmonton, AB, Canada
for contributions to radio resource management for cellular systems and networks

Teng-joon Lim
National University of Singapore, Singapore
for contributions to statistical signal processing in wireless communications

Xiaojun Lin
Purdue University West Lafayette, IN, USA
for contributions to scheduling and control of wireless networks

Board of Governors: New Members

Congratulations to the new members of the IT Society Board of Governors (a full list of members can be found on the ITSoc website).

Alexandros G. Dimakis
UT Austin

Andrew R Barron
Yale University

Christina Fragouli
University of California, Los Angeles

Gregory Wornell
Massachusetts Institute of Technology

Michele A Wigger
Telecom ParisTech

Tara Javidi
University of California, San Diego

From the Editor

continued from page 2

Full obituaries can be found at http://adobecreekfuneralhome.com/obituaries?2/paul?calvin?shields/870/ and http://www.ams.org/news/in-memory/in-memory respectively. Thanks to Robert Gray and Dave Neuhoff for bringing these announcements forward.

Continuing our remembrance and honoring of Sol Golomb, an extraordinary scholar and long time newsletter contributor, the third collection of Sol's earlier newsletter puzzle columns appear in this issue. This third collection includes solutions to the first collection of puzzles published in the September 2016 issue of the newsletter.

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

Announcements, news, and events intended for both the printed newsletter and the website, such as award announcements, calls for nominations, and upcoming conferences, can be submitted at the IT Society website http://www.itsoc.org. Articles and columns can be e-mailed to me at mikel@buffalo.edu with a subject line that includes the words "IT newsletter."

The next few deadlines are:

April 10, 2017 for the issue of June 2017.

July 10, 2017 for the issue of Sep. 2017.

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

I look forward to hearing your suggestions and contributions.

With best wishes,
Michael Langberg
mikel@buffalo.edu

Reflection and Summary of the Paper: The Capacity Region of the Two-Receiver Gaussian Vector Broadcast Channel with Private and Common Messages

Yanlin Geng, Chandra Nair

Abstract. The aim of this write-up is to introduce the readers to a general framework of ideas that are used in the paper and also place it in a related mathematical context. The basic contribution of the paper was to develop a set of tools and ideas that can be used to establish optimality of Gaussian distributions.

Background

For several optimization problems involving information measures in the presence of additive Gaussian noise that occur in many channel-coding and source-coding settings, the optimality of Gaussian distributions has been established over the years. The general technique for establishing the optimality of Gaussian distributions involved:

- Standard optimization techniques such as using Lagrange multipliers. This is applied for instance in maximizing differential entropy subject to a covariance constraint. Sometimes though this is also presented, in disguise, as an argument using the non-negativity of relative entropy.
- Entropy power inequality either in its naive form or ideas from its proof: a calculus of variations approach, by establishing the monotonicity of the function involved along the *Stam's path*.

The technique we employ in this paper is to derive the optimality of Gaussians as a natural consequence of the single-letterization property of the functionals involved. In the functional analysis literature such results do exist for parameters that tensorize (same concept as single-letterization) such as hypercontractive inequalities or Brascamp-Lieb inequalities. That Gaussians are extremal in the sense of providing the best constants for these inequalities are non-trivial results. The various approaches to prove the optimality of Gaussians include rearrangement inequalities [4, 5], ideas from optimal transport [2], heat flow [3], rotational invariance [12], among others. The approach presented in this paper works for these general body of problems as well, shares some similarities with the previous mentioned techniques[1], but is also different in interesting ways.

Before we get into why the single-letterizations arguments that we ubiquitously employ in information theory may directly lead to extremality of Gaussian distributions, we wish to state the following characterization of Gaussians.

Theorem 1 (Skitovic-Darmois characterization of Gaussian distributions, Theorem 1 in [11]). *Let $\mathbf{X}_1, .., \mathbf{X}_n$ be n mutually independent t-dimensional random column vectors, and let $A_1, .., A_n$ and $B_1, ..., B_n$ be non-singular $t \times t$ matrices. If $\sum_{i=1}^n A_i \mathbf{X}_i$ is independent of $\sum_{i=1}^n B_i \mathbf{X}_i$, then the $\mathbf{X}_i$ are normally distributed.*

Single-letter functionals that are sub-additive

The focus is on single-letter expressions (functionals of probability distributions) that are sub-additive (or tensorize). Further, we will only consider functionals arising from some channel-coding problems in this write-up.

The first example we will consider is the classical point-to-point communication model. Given a channel $W(y\,|\,x)$, we know that the maximum achievable rate is $\max_{p(x)} I(X; Y)$. Given two channels $W_1(y_1\,|\,x_1)$ and $W_2(y_2\,|\,x_2)$, define the product channel $W(y_1, y_2\,|\,x_1, x_2) := W_1(y_1\,|\,x_1)$ $W_2(y_2\,|\,x_2)$. Let $(X_1, X_2) \sim p(x_1, x_2)$; then observe that

$$\begin{aligned} I_W(X_1, X_2; Y_1, Y_2) &= I_{W_1}(X_1; Y_1) + I_{W_2}(X_2; Y_2) - I(Y_1; Y_2) \\ &\leq I_{W_1}(X_1; Y_1) + I_{W_2}(X_2; Y_2). \end{aligned} \tag{1}$$

Note that we used the chain-rule of mutual information and that $Y_1 \to X_1 \to X_2 \to Y_2$ is Markov (standard arguments) to obtain the equality in (1). For a fixed channel $I(X; Y)$ is a function of the input distribution, say denoted by $F_W(\mu_X)$. Hence the above inequality can be expressed alternatively as:

$$F_{W_1 \otimes W_2}(\mu_{X_1, X_2}) \leq F_{W_1}(\mu_{X_1}) + F_{W_2}(\mu_{X_2}). \tag{2}$$

The above inequality can be considered as the sub-additive property of mutual information over product channels.

Remark 1. If one has a single-letter expression for the capacity region for a discrete memoryless (multi-user) channel $W(y\,|\,x)$; then by grouping together two consecutive units of time slots and evaluating the same region for the new channel $W \otimes W$, one must not be able to increase the achievability region. As most natural capacity regions are convex (by a time-sharing argument), by looking at appropriate supporting hyperplanes to the region, one can state the above reasoning as:

$$\max_{\mu_{X_1, X_2}} M_{W \otimes W}(\mu_{X_1, X_2}) = 2 \max_{\mu_X} M_W(\mu_X), \tag{3}$$

for some appropriately defined $M_W(\mu_X)$, capturing the maximum value in some direction for a capacity region. For instance, for the capacity region of the multiple access channel, $W(y\,|\,x_a, x_b)$, the maximum achievable value of $\lambda R_1 + R_2$ for $\lambda \geq 1$ is given by

$$\max_{\mu_{x_a, x_b}} \{\lambda I(X_a; Y\,|\,X_b) + I(X_b; Y)\}.$$

Here $\lambda I(X_a; Y\,|\,X_b) + I(X_b; Y)$ can be considered as a function of the input (here input space is a pair of independent distributions) M_W (μ_X).

[1] The authors became aware of these connections after the publication of the paper. However the technique introduced is also substantially different from the mentioned techniques and is motivated directly by the previously developed information-theoretic reasonings. Indeed a lot of the manipulations used here is mimicking the ideas in [9], though that paper works exclusively in the discrete setting.

What has been curious to the authors and some of their collaborators is that almost all the proofs of capacity regions for generic settings; rather than establishing (3), (the proofs) end up establishing the stronger sub-additivity statement in the sense of (2).

Here is another functional that is considered in the article. Consider a broadcast channel $W(y, z \mid x)$. For $\lambda > 1$, define:

$$S_W^\lambda(\mu_X) := C_X[I(X;Y) - \lambda I(X;Z)] = \sup_{\mu_{U|X}} I(X;Y|U) - \lambda I(X;Z|U).$$

Here C_X denotes the upper concave envelope of the function $I(X;Y) - \lambda I(X;Z)$, viewed as a function over the probability distributions on X. (See [17] for how these envelopes come naturally in optimization problems involving auxiliary random variables.) Routine manipulations yield that for $(X_1, X_2) \sim \mu_{x_1,X_2}$, passing through a product broadcast channel $W_1(y_1, z_1 \mid x_1) \otimes W_2(y_2, z_2 \mid x_2)$; for any $\mu_{u \mid X_1, X_2}$

$$\begin{aligned} I(X_1,X_2;Y_1,Y_2|U) - \lambda I(X_1,X_2;Z_1,Z_2|U) = I(X_1;Y_1|U,Y_2) \\ - \lambda I(X_1;Z_1|U,Y_2) + I(X_2;Y_2|U,Z_1) - \lambda I(X_2;Z_2|U,Z_1) \\ - (\lambda - 1) I(Z_1;Y_2|U), \end{aligned} \tag{4}$$

implying

$$S_{W_1 \otimes W_2}^\lambda(\mu_{X_1,X_2}) \le S_{W_1}^\lambda(\mu_{X_1}) + S_{W_2}^\lambda(\mu_{X_2}). \tag{5}$$

The following points are worth noting:

- The manipulations done here directly follow the manipulations for obtaining the UV-outer-bound [16] for the broadcast channel; which in turn mimic the arguments in [7] and [14].
- If we set Z = X (channel to be noiseless), then the sub-additivity in (4) is equivalent to the tensorization of hyper-contractivity ribbon at a particular limit (see [1]).

Optimality of Gaussians

The main technical contribution of this article is to establish the optimality of Gaussians by examining the proof of sub-additivity.

Example 1: Point-to-point setting:

To illustrate this technique, first let us consider the point-to-point channel setting where $Y = X + G$. Here $G \sim \mathcal{N}(0,1)$ is a Guassian noise which is independent of the transmit symbol X. We will employ the method to establish that Gaussian inputs are extremal (a well known result with many simpler proofs), in the sense that, subject to $E(X^2) \le P$, Gaussians maximize $I(X; Y)$.

Let $X \sim \mu_X^*$ be a maximizer[2]. Choose X_1 and X_2 to be independent and each distributed according to μ_X^*. When passed through independent channels with Gaussian noises G_1, G_2, let Y_1, Y_2 denote the respective outputs. Denote the additive Gaussian noise channel by W, and let $M = I_W(X_1; Y_1)$ denote the value of the optimization problem.

Let X_+ and X_- denote any pair of rotations of X_1, X_2 that are orthogonal to each other; for instance $X_+ = (X_1 + X_2)/\sqrt{2}$ and $X_- = (X_1 - X_2)/\sqrt{2}$. Similarly define for the outputs and noises: $Y_+ = (Y_1 + Y_2)/\sqrt{2}$ $Y_- = (Y_1 - Y_2)/\sqrt{2}$, $G_+ = (G_1 + G_2)/\sqrt{2}$ and $G_- = (G_1 - G_2)/\sqrt{2}$. Since G's are Gaussians, G_+ is independent of G_- and as the channel is additive the Markov chain $Y_+ \to X_+ \to X_- \to Y_-$ holds. Equation (1) yields

$$I_{W \otimes W}(X_+, X_-; Y_+, Y_-) = I_W(X_+; Y_+) + I_W(X_-; Y_-) - I(Y_+; Y_-). \tag{6}$$

On the other hand bijections preserve mutual information; hence

$$2M = I_{W \otimes W}(X_1, X_2; Y_1, Y_2) = I_{W \otimes W}(X_+, X_-; Y_+, Y_-).$$

Since both X_+ and X_- satisfy $E(X^2) \le P$, we have $I_W(X_+; Y_+)$, $I_W(X_-; Y_-) \le M$. Thus, for equation (6) to hold, we must have $M = I_W(X_+; Y_+) = I_W(X_-; Y_-)$; and $I(Y_+; Y_-) = 0$. One could use the former terms, use a central limit theorem argument to show that Gaussians are maximizers; but it turns out to be more useful (in other settings) to deduce it from $I(Y_+; Y_-) = 0$ as follows: $I(Y_+; Y_-) = 0$ implies $Y_+ = (Y_1 + Y_2)/\sqrt{2}$, $Y_{\_} = (Y_1 - Y_2)/\sqrt{2}$ are independent. Since noises G_+, G_- are independent and Gaussian, this implies that X_+, X_- are independent. By construction X_1 and X_2 are independent; hence, Theorem 1 immediately implies that X_1 and X_2 must be Gaussian. Note that this also shows that Gaussian is the unique maximizer.

Example 2: Maximizing $S_W^\lambda(\mu_X)$ subject to a covariance constraint:

Now, let us consider the second example of sub-additivity mentioned. Consider additive channels where $\mathbf{Y} = A\mathbf{X}_1 + \mathbf{G}_1$ and $\mathbf{Z} = B\mathbf{X}_2 + \mathbf{G}_2$, where A, B are invertible matrices and $\mathbf{G}_1$ and $\mathbf{G}_2$ are Gaussian noise vectors independent of A, B, say $\mathcal{N}(0, I)$.

By mimicking the steps in the previous example: i.e. starting with any maximizer $\mathbf{X} \sim \mu_{\mathbf{X}}^*$, taking two independent copies (of $(U, \mathbf{X})$ in this case), taking rotations of them, and passing them through $W \otimes W$; from (4), we would obtain that $I(\mathbf{Z}_+; \mathbf{Y}_- \mid U_1, U_2) = 0$, which would then imply that $I(\mathbf{X}_+; \mathbf{X}_- \mid U_1, U_2) = 0$. Again Theorem 1 immediately implies that, conditioned on U_1, U_2, $\mathbf{X}_1$ and $\mathbf{X}_2$ must be Gaussian, implying Gaussian extremality (as well as its uniqueness).

Remark 2. The following points are worth noting:

- The above argument already helps recover the capacity region of the vector Gaussian broadcast channel with private messages [18] by the following reasoning. The above argument shows is that Gaussian distributions exhaust the UV-outer-bound region (or the Korner-Marton-outer-bound region). On the other hand, dirty paper coding argument [6] shows that when (U, X) are jointly Gaussian and Y is a Gaussian corrupted version of X; one can identify a (Gaussian) random variable V such that $I(V; Y) - I(V; U) = I(X; Y|U)$. This trick allows one to use Marton's coding scheme to achieve any point in the UV-outer-bound, thus establishing the capacity region.
- By making use of the enhancement ideas used in the proof of the capacity region of the vector Gaussian broadcast channel

[2] The purpose of this short write-up is to give the readers some insights into the arguments. Hence we will sweep some technical arguments under the carpet, such as existence of maximizers (for those interested see [10] for the general body of ideas involved to show why these do exist) of $I(X; Y)$ subject to $E(X^2) \le P$. In general that these maximizers exist are merely exercises in analysis; the covariance constraint (or some other suitable constraint) provides tightness (hence subsequential convergence) and then a suitable argument that shows that limits can be interchanged between function value and the limiting distribution needs to be used. The specifics may depend on the particular problem at hand but the machinery is rather standard.

with private messages Liu and Viswanath [13] were able to show the above mentioned Gaussian extremality.

Application: Capacity region of the vector Gaussian broadcast channel with common and private messages. As an application of the developed technique we solve a problem that had been open earlier (open problem 9.3 in [8]). Again, in this article, we will only outline the steps of the proof and some intuition behind this proof. The basic idea is to show that the UVW-outer-bound [15] for the broadcast channel reduces to the Marton's achievable region. The key is to show that Gaussian random variables exhaust the region formed by the UVW-outer-bound. Once this is done, then a dirty paper coding argument will show these rates are contained inside Marton's achievable region completing the proof.

To identify the right functional that is sub-additive, from the UVW-outer-bound, we utilize the min-max approach developed in [9]. Mimicking the arguments of the outer bound we show that the following functional is sub-additive: Consider a broadcast channel $W(y, z \,|\, x)$. For $\vec{\lambda} = (\lambda_0, \lambda_1, \lambda_2)$, where $\lambda_i > 0$, $i = 0, 1, 2$, $\lambda_2 > \lambda_1$, $\alpha \in [0, 1]$ and $\bar{\alpha} := 1 - \alpha$, consider the following function of μ_X defined by

$$T_W^{\vec{\lambda},\alpha}(\mu_X) := C_X\Big[-\lambda_0 \alpha I(X;Y) + (\lambda_2 - \lambda_0 \bar{\alpha}) I(X;Z) + \lambda_1 S_W^{\frac{\lambda_2}{\lambda_1}}(\mu_X)\Big],$$

where $S_W^{\lambda}(\mu_X)$ is the function defined earlier. Using the discarded terms in the proof of the sub-additivity of the above functional, the developed technique yields that the maximum of the function subject to a covariance constraint is achieved by Gaussians.

Conclusion

The main observation of the paper is that the terms that one normally discards in the proof of the single-letterization in information theory, can be used to deduce that Gaussians are maximizers of the sub-additive (tensorizing) functionals. This is done by appealing to a characterization of Gaussians (Theorem 1).

References

[1] Venkat Anantharam, Amin Gohari, Sudeep Kamath, and Chandra Nair, *On hypercontractivity and a data processing inequality,* 2014 IEEE International Symposium on Information Theory (ISIT'2014) (Honolulu, USA), June 2014, pp. 3022–3026.

[2] Franck Barthe, *On a reverse form of the brascamp-lieb inequality,* Inventiones mathematicae **134** (1998), no. 2, 335–361.

[3] Jonathan Bennett, Anthony Carbery, Michael Christ, and Terence Tao, *The brascamp–lieb inequalities: finiteness, structure and extremals,* Geometric and Functional Analysis **17** (2008), no. 5, 1343–1415.

[4] Herm Jan Brascamp and Elliott H Lieb, *Best constants in young's inequality, its converse, and its generalization to more than three functions,* Advances in Mathematics **20** (1976), no. 2, 151–173.

[5] H. J. Brascamp, Elliott H Lieb, and J.M Luttinger, *A general rearrangement inequality for multiple integrals,* Journal of Functional Analysis **17** (1974), no. 2, 227–237.

[6] M. Costa, *Writing on dirty paper (corresp.),* Information Theory, IEEE Transactions on **29** (1983), no. 3, 439–441.

[7] A. El Gamal, *The capacity of a class of broadcast channels,* IEEE Trans. Info. Theory **IT-25** (March, 1979), 166–169.

[8] Abbas El Gamal and Young-Han Kim, *Network information theory,* Cambridge University Press, 2012.

[9] Y. Geng, A. Gohari, C. Nair, and Y. Yu, *On marton's inner bound and its optimality for classes of product broadcast channels,* Information Theory, IEEE Transactions on **60** (2014), no. 1, 22–41.

[10] Y. Geng and C. Nair, *The capacity region of the two-receiver gaussian vector broadcast channel with private and common messages,* Information Theory, IEEE Transactions on **60** (2014), no. 4, 2087–2104.

[11] S. G. Ghurye and Ingram Olkin, *A characterization of the multivariate normal distribution,* The Annals of Mathematical Statistics **33** (1962), no. 2, pp. 533–541 (English).

[12] Elliott H. Lieb, *Gaussian kernels have only gaussian maximizers,* Inventiones mathematicae **102** (1990), no. 1, 179–208.

[13] Tie Liu and P. Viswanath, *An extremal inequality motivated by multiterminal information-theoretic problems,* Information Theory, IEEE Transactions on **53** (2007), no. 5, 1839–1851.

[14] K. Marton, *A coding theorem for the discrete memoryless broadcast channel,* IEEE Trans. Info. Theory **IT-25** (May, 1979), 306–311.

[15] C. Nair, *A note on outer bounds for broadcast channel,* Presented at International Zurich Seminar (2010).

[16] C. Nair and A. El Gamal, *An outer bound to the capacity region of the broadcast channel,* IEEE Trans. Info. Theory **IT-53** (January, 2007), 350–355.

[17] Chandra Nair, *Upper concave envelopes and auxiliary random variables,* International Journal of Advances in Engineering Sciences and Applied Mathematics 5 (2013), no. 1, 12–20 (English).

[18] H. Weingarten, Y. Steinberg, and S. Shamai, *The capacity region of the gaussian multiple-input multiple-output broadcast channel,* Information Theory, IEEE Transactions on **52** (2006), no. 9, 3936–3964.

The Historian’s Column

Anthony Ephremides

Most (if not all) of us are employed in Academia, Industry, or Government. Some are entrepreneurs or self-employed and some are still students who contemplate these options as they approach graduation. More or less it has been so throughout our brief history. Perhaps the entrepreneur class has grown a little recently (although I still remember Oscar Lenneman, one of Fred Beutler’s students in the ’70’s, who became an Art dealer in New York as soon as he finished his studies).

A small (almost minute) segment of our community who are in academia choose (for at least a portion of their careers) to go to University administration. They become department heads, or deans, or, in rare cases, provosts, chancellors, and even presidents. One of my ex-colleagues, Nariman Farvardin went through all the ranks from chair to president. Michael Tanner was chancellor and Don Snyder was department chair for many years. And so was Lee Davisson (another ex-colleague). And of course Vince Poor was Dean of Engineering at Princeton until last summer. There were others of course both in the US and elsewhere in the world.

I have often speculated about the motives of those who choose the administrative route. Several times during my career I have been asked whether I was interested in an administrative position, especially department chair. My answer has always been that to be department head, one would have to be in the intersection of three classes of people. That is, one should be Able, Willing, and Acceptable. Unfortunately, I do not belong even to the union of these classes. So, for me it was a no-brainer. I am still obsessed by the belief that a department chair (or dean, or higher-up) will have to meet on a daily basis with people who have grievances, while at the same time lacking any real power to do much about them. Perhaps this is an exaggeration but it is not far from the truth. This belief of mine removed any desire to seek such a job. Hence, I have been unwilling. Furthermore, I have a rather short temper that might lead me to inappropriate reactions that might get me into trouble. Hence, I have been unable. And, finally, I have a habit of needling and, perhaps sometimes, offending people (including friends or enemies). Thus I have not been acceptable. The closest I came to assuming an administrative position has been when I became the founding co-director of the NASA-sponsored Center for the Commercial Development of Space (the legendary CCDS) at the University of Maryland with my colleague John Baras. The theme of the Center was Satellite and Hybrid Networks and I was much more fascinated with the technical side of the job that led to some significant advances in modifying the TCP protocol to make it suitable for links with long transmission delays. For this I was the co-recipient of a prestigious innovation award. Thus, I offloaded the directorship to John and was much happier ever since.

Nonetheless, some colleagues have had very successful administrative careers. Those who did were typically characterized by exceptional, so-called, “people-skills”. That is, they were able to interface with others with an uncanny ability to be “smooth”, persuasive, civil, and friendly. For example, Lee Davisson, who chaired my department from 1980 to 1985, and who had a trade-mark “poker” facial expression and demeanor, was able to completely conceal his emotions, if he chose to. A colleague would storm into his office with serious complaints (perhaps concerning salary, or space, or students, or staff, or other colleagues, or all of the above) and after thirty minutes of “tete-a-tete” discussion with him, would exit calm and with a smile but without having achieved any of his requests! Now, isn’t that exceptional? I never found out how he could do that! To be fair, occasionally, an administrator can make a great deal of difference. The right person at the right place at the right time can have a major impact on the development of his/her unit. For sure, both Lee and Nariman did have such an effect on my department. And, come to think of it, although I do know several lousy administrators, I cannot think of one in that category from the ranks of our Society. I guess this is because of the “magic” of Information Theory. Another aspect of one’s professional life concerns the fateful decision of retirement. Some people quit early while others literally “die” on the job. Unlike in most countries, the issue of mandatory retirement in the United States was settled by the Supreme Court in a ruling that mandatory retirement based on age constitutes “age discrimination”.

Increasingly, as my hair turns more white or thins out (or both), I am being asked whether I am retired. Note that the question is not whether I intend to retire but, rather, whether I am already retired. My answer, in an effort to be funny, is “Whoa! Retired? I am not even tired (ha-ha)”!

Seriously, though, this is a complex question. Clearly, if all cling to their job, and if they are blessed with good health, they “block” younger folks who are qualified to replace them. As a matter of practice, most academics do retire more or less “on-time”. Nonetheless, some do choose to stay on. And in several cases, those who stay continue to be productive, energetic, and useful, while some others barely meet the minimum requirements and become a burden to their units. So, what to do?

My personal view is that retirement should be handled just like promotion and tenure. If we are judged to be still contributing positively to our environments, that is, if we still teach effectively, if we mentor graduate students, and if we attract external funding for our research, then we should be allowed to stay on. If however we evolve into minimalists who abuse the generosity of the tenure system, perhaps we should be asked to retire. And to give the occasion a positive spin we could “dress-up” the decision by accompanying the retirement congratulations with the legendary golden watch!

Students' Corner: Reflections on ISIT Student Paper Awards

"The IEEE Jack Keil Wolf ISIT Student Paper Award is given to up to 3 outstanding papers for which a student is the principal author and presenter." For this issue, we asked winners and finalists of this award to write a short essay about their work and experiences leading up to their ISIT paper. The responses we received are published below.

The first essay is by Cheuk Ting Li, who is a graduate student at Stanford University. Cheuk Ting describes his work on the amount of common randomness required to generate a jointly continuous distribution. **C. T. Li and A. El Gamal, "Distributed simulation of continuous random variables**," in Proc. IEEE Int. Symp. Information Theory, 2016.

The second contribution is by Nir Weinberger, a graduate student at Technion. Nir shares his thoughts about the review process which proved very beneficial for his ISIT paper. **N. Weinberger and N. Merhav, "A Large Deviations Approach to Secure Lossy Compression**," in Proc. IEEE Int. Symp. Information Theory, 2016.

If you have any questions or comments, or would like to contribute to this column in the future, feel free to contact me at parham@caltech.edu

Parham Noorzad

Distributed Simulation of Random Variables—the Hard Part and the Easier Part

By Cheuk Ting Li (ctli@stanford.edu)

Two parties, Alice and Bob, share only common randomness W and wish to generate correlated random variables X and Y, respectively, with a prescribed joint distribution. What is the minimum average description length of W needed to accomplish this task? In other words, what is the minimum entropy H(W) needed such that X and Y are conditionally independent given W?

If X or Y are discrete and have finite entropies, then we can simply set W = X (or Y) and the average description length of W is finite. If X and Y are continuous (e.g., jointly Gaussian), however, it is not clear whether a finite average description length of W is possible, since H(X) and H(Y) would be infinite. Quite surprisingly, we showed that for log-concave distributions such as Gaussian, H(W) can be upper-bounded by I(X; Y) + 24. This is the main result of the paper "Distributed simulation of continuous random variables," that I coauthored with my advisor Prof. Abbas El Gamal. Much to my honor, this paper received the IEEE Jack Keil Wolf ISIT Student Paper Award at ISIT 2016.

I started working on the distributed simulation problem three years ago with Prof. El Gamal and Dr. Gowtham Kumar, another student of Prof. El Gamal who graduated in 2014 and is now at Google. I learned a lot from my advisor and Gowtham about how to explore a new problem setting, which is very different from studying an existing well-defined problem. The paper "Exact common information" that Gowtham presented at ISIT 2014 was focused on the case in which X and Y are discrete. It is clear that the exact common information rate is greater than or equal to the asymptotic common randomness rate needed for distributed simulation with vanishing total variation distance, known as Wyner's common information. We showed that equality holds for several examples, but were not able to show if it holds in general. Even the basic problem of computing the minimum of H(W) for small X and Y alphabet sizes is computationally very difficult due to a combinatorial explosion.

Given these difficulties, it appeared unthinkable to consider continuous X and Y. Not only we cannot efficiently compute the minimum of H(W), but we cannot even write a program that computes it. Although completely solving a problem can be much harder than establishing any noteworthy property about it, it is exactly the difficulty of the problem that makes any discovery intriguing. Merely proving finiteness of H(W) would already be surprising. When the puzzle pieces fit together and we were finally able to establish an upper bound in terms of mutual information for log-concave distributions, it was akin to discovering a treasure at the end of an arduous journey.

In Praise of Peer Review

By Nir Weinberger (nir.wein@gmail.com)

When I reminisce about the time period during which I worked with my Ph.D. advisor, Prof. Neri Merhav, on our paper on secure lossy compression, I recall that I did not doggedly work on this problem. Instead, I let it incubate at the back of my mind for a while and only started to actively work on it when I found the suitable tools.

The rate-distortion theorem for lossy compression is one of information theory's most basic results and is usually proved using some sort of a covering lemma. In its standard form, however, no special attention is paid to the exact structure of the quantization cells which are used for covering. This is certainly immaterial if one is just interested in minimizing the compression rate. By contrast, Ahlswede has proved a covering lemma for type classes, where each quantization cell is a (subset of a) permutation of the largest cell. This additional structure paves the way for solving problems where other properties of the code are also of interest, e.g., secrecy.

I actually learned about this lemma in the review process of a different paper. The associate editor pointed us to one of his papers, where he had elegantly used this lemma (thanks Prof. Jun Chen!). So it turned out that that review had implications beyond the scope of the actual paper it was addressed to.

Despite the fact that the review process was very beneficial in my case, many share the feeling that this process may in general be daunting for both authors and reviewers. On one side of the equation stand the authors, who put their mightiest efforts in solving an information-theoretic problem and eagerly wait for the outcome of the review. On the other side, reviewers have to devote their precious research time and expertise to read a paper which, in some cases, may be quite far from their own interests.

That being said, I think that more often than not, the review process is also very beneficial for the reviewers. In most of the reviews I have conducted, I had to delve into a topic somewhat different than my own research. I honestly believe that the gain of being more open minded to other people's work outweighs the immediate loss in time to carry my own research.

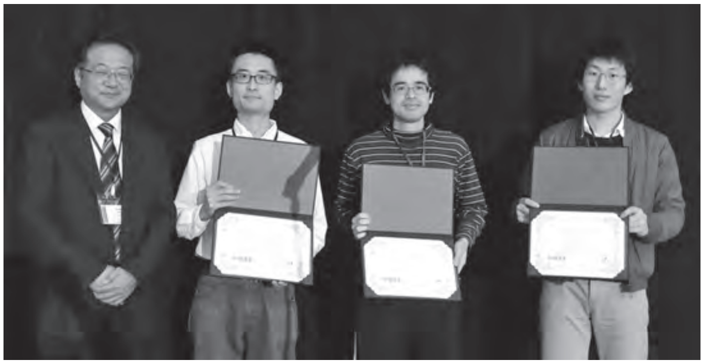
From the Field: IEEE Information Theory Society Japanese Chapter

Hiroshi Kamabe: Gifu University

The main activities of The IT Society Japan Chapter include co-sponsoring six workshops a year and SITA (Symposium on Information Theory and its Applications) once a year in collaboration with the IEICE (Institute of Electronics, Information and Communication Engineers) Research Society of Information Theory and its Applications. The details of the activities are as follows.

During the months of January, March, May, July, September and December, technical meetings on Information Theory are held generally. The events are jointly sponsored with Technical Committees on Signal Processing and Radio Communication Systems in January, with Technical Committees on Wide Band System and Information Security in March, and with Technical Committee on Enriched Multimedia in May. The technical meeting in September is held immediately after the Workshop for Error Correcting Code. The technical meeting that is held in December consists of four invited lectures for young researchers. None of the lectures undergo peer reviews.

SITA is co-hosted once a year in collaboration with the Research Society of Information Theory and its Applications, except in the year 2016. The topics discussed in this symposium include information theory, coding theory, and topics in related fields. None of these lectures are peer reviewed. This symposium has been held every year since 1978, and it is its 40th anniversary this year. There are more than a hundred presentations, three workshops and some special lectures conducted in this symposium. It is our tradition that this symposium is always held at a famous hot-spring area in Japan.



Young Researcher Best Paper Award in ISITA2016.

At SITA, we hold a general meeting of the Japan Chapter and report the activities conducted in the year to our members living in Japan.

ISITA (International Symposium on Information Theory and its Applications) is held once in every two years and awards are given to the outstanding publications that are published and presented by young members of our chapter living in Japan (Young Researcher Best Paper Award in ISITA). This symposium is always technically-sponsored with the IEEE IT Society.

Home page:
http://www.ieee-jp.org/section/tokyo/chapter/IT-12/

Report on the Munich Workshop on Information Theory of Optical Fiber (MIO 2016)

Organizers: Tobias Fehenberger, Javier García, René Essiambre, Gerhard Kramer

The Institute for Communications Engineering (LNT) at the Technical University of Munich (TUM) organized the 3rd Munich Workshop on Information Theory of Optical Fiber (MIO 2016) on December 5–6, 2016. The technical program included talks by leading researchers in the area of optical fiber communications. On Monday, December 5, the speakers were Andrew Ellis, Peter Andrekson, Ruben Luís, Nicolas Fontaine, Antonio Mecozzi, Darko

Group photo of MIO 2016 participants with Christmas concert musicians.

Discussion during the poster session.

Zibar, Sergei Turitsyn, Mariia Sorokina, and Mark Shtaif. On Tuesday, the speakers were Ronen Dar, Vahid Aref, Radan Slavik, and Maxim Kuschnerov. The talk topics included space-division multiplexing, optical and electronic signal processing, optical amplification, fiber nonlinearities, capacity calculations, and information theory. Doctoral candidates, postdocs, and scientists from several academic and industrial institutions presented posters. Around 80 persons attended the event.

The social program included lunches, coffee, snacks, and a Christmas Concert with trumpet and accordion with variations by Mozart. On Monday evening the attendees enjoyed a Bavarian winter dinner at the Löwenbräukeller on the Stiglmaierplatz in Munich.

Funding for the workshop was provided by the German Research Foundation (DFG) and the Alexander von Humboldt Foundation. The program, presentations, posters, theme song, and photos are available at the web address

http://www.lnt.ei.tum.de/en/events/munich-workshop-on-information-theory-of-optical-fiber-2016/

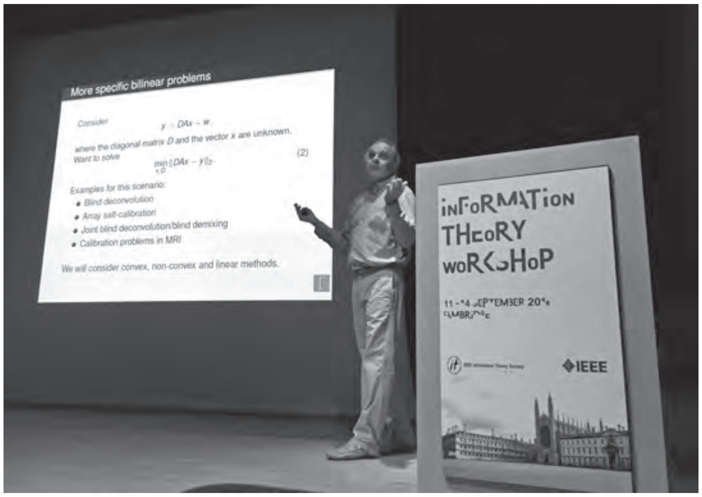
2016 Information Theory Workshop Cambridge, UK 11–15 September 2016

Deniz Gündüz, Jossy Sayir

The 2016 Information Theory Workshop was held in Cambridge, UK from 12th to 14th of September. It was the first major meeting of our society in the UK since the International Symposium on Information Theory (ISIT) held in Brighton in 1985, which is remembered as the last ISIT that Claude Shannon attended.

The workshop was chaired by Jossy Sayir, David MacKay and Deniz Gündüz. Tragically, David lost his battle against cancer a few months before the workshop. He was remembered in a special memorial session during the workshop.

The workshop brought together 173 information theorists from around the world to listen to three plenary talks and 113 paper presentations, which comprised a very exciting and stimulating technical program, put together by Helmut Bölcskei, Rob Calderbank, and Miguel Rodrigues. The plenary talks spanned diverse research problems in information theory and related areas. Yonina Eldar talked about theoretical limits of "Analog to Digital Compression", and how the theoretical results can be used to build a


More specific bilinear problems
Examples for this scenario:
Blind deconvolution
Array self-calibration
Joint blind deconvolution/blind demixing
Calibration problems in MRI
We will consider convex, non-convex and linear methods.
INFORMATION THEORY WORKSHOP
IEEE

Thomas Strohmer gave a plenary talk on bilinear programs in signal processing and communications.

more efficient ultrasound imaging technology. Andrew Blake talked about "Machines That Learn", exploring the differences and connections between probabilistic models and large-scale training networks in machine learning. Thomas Strohmer gave a very engaging talk on bilinear problems in signal processing and communications, and how they could help solve a murder mystery.

The organising committee included Iñaki Esnaola as the publications chair, Michèle Wigger as the publicity chair, Ramji Venkataramanan as the finance chair, and many volunteer students from the University of Cambridge, Imperial College London and the University of Sheffield.

The workshop was organised at Robinson College, which provided a whole package of accommodation and dining to the participants in the same location as the talks. This allowed a lot of extra time for discussions and catching up outside the usual conference schedule. The beautiful college grounds and the historic city of Cambridge provided a tranquil backdrop. The weather was unexpectedly cooperative: to the satisfaction of the workshop organisers, the umbrellas included in the welcome package were not needed. The social program included a welcome reception at Robinson College, a guided tour of Cambridge, and a chauffeured punting trip along the River Cam. The workshop banquet was held in the magnificent dining hall of Trinity College.

We hope it won't be another 31 years before information theorists return to the UK for a conference or workshop.

Shannon Centenary

UCSD Shannon Centenary Celebration October 10–11, 2016

Paul Siegel

UC San Diego celebrated the centennial anniversary of Claude Shannons birth with a program of events held on Monday-Tuesday, October 10–11, 2016 at the university's La Jolla campus. The Shannon Centenary Celebration featured three invited lectures, as well as a variety of informative posters, hands-on exhibits, and engaging video presentations that offered a glimpse into the world of Claude Shannon, the scientific discipline he created, and its sweeping applications. The Monday program also included morning and afternoon receptions, a buffet lunch, and a catered banquet in honor of the invited speakers.

The lectures were held in the auditorium at Atkinson Hall, home of the Qualcomm Institute, which is directed by the IT Society's Ramesh Rao. The talks were open to the public, and each drew an audience of 80–100 people, including students, faculty, and staff from across UCSD and the local community. There were even sightings of IT legends and UCSD benefactors, Andrew Viterbi and Irwin Jacobs. The exhibits in the Atkinson Hall theater included a display of robotic mice built by UCSD students for the IEEE Micromouse Competition, accompanied by the famous Bell Labs video of Shannon describing the competition's inspiration, his maze-navigating mouse, Perseus. Another exhibit described the Hamming code and displayed copies of *The Secret Code Menace*, a recently published fiction story, penned by UCSD faculty member Pamela Cosman, that teaches young adults about the concept of error-correction coding. There was also a poster with the full text of Shannon's *Rubric on Rubik Cubics*, along with an assortment of Rubik's cubes, information theory anagrams, and IT-inspired puzzles to entertain and challenge attendees. The nine informative and colorful posters commissioned by the IT Society in honor of the Shannon Centennial were also on display throughout the theater and Atkinson Hall foyer. Several large monitors and the theater's high-resolution video wall provided showings of slide presentations and videos about Shannon and information theory. The posters, puzzles, and videos, along with an album of photos from the event, can be found on the Shannon Centenary Celebration website at http://cmrr-star.ucsd.edu/claude-shannon/.

Alon Orlitsky, Ingrid Daubechies, and Robert Calderbank at the "Fallen Star" house (part of the UCSD Stuart Collection of outdoor art).

The distinguished speaker on Monday morning was Ingrid Daubechies, James B. Duke Professor of Mathematics and Electrical and Computer Engineering at Duke University, who delivered UCSD's 3rd Jack Keil Wolf Lecture in Information Theory and Applications. The lecture series, inaugurated in 2014, is named in honor of our beloved colleague Jack Wolf, a life-long member of the Information Theory Society, who served on the UC San Diego faculty from 1984 until 2011. Ingrid's presentation, *Reunited*, told the fascinating story behind the ongoing exhibition of the same name at the North Carolina Museum of Art, and the major role played by her Image Processing for Art Investigation (IPAI) group in bringing it to reality. The story begins with an artist's re-imagining of a missing panel from Francescuccio Ghissi's 14th century Italian alterpiece depicting the crucifixion of Jesus and scenes in the life of St. John the Evangelist. The eight extant panels, long separated and held in collections across the country, were reunited with the “reconstructed” panel to enable a display of the entire work for the first time in over a century. The visual mismatch between the faded originals and their freshly painted counterpart was overcome by the IPAI team through ingenious image processing techniques that digitally “aged” the new panel, allowing for a coherent presentation of the ancient masterpiece. Reversing the arrow of time, the IPAI researchers then virtually rejuvenated the old panels, providing the opportunity to view the alterpiece in its original glorious brilliance. The audience was captivated by Ingrid’s description of this successful partnership between the worlds of engineering and fine art; more information about the project can be found on the IPAI website at https://dukeipai.org/projects/ghissi.

On Monday afternoon, Robert Calderbank, Professor of Computer Science, Electrical Engineering, and Mathematics at Duke University and Director of its Information Initiative, presented UCSD’s 14th Annual Shannon Memorial Lecture. The Shannon Memorial Lectureship was established in 2003 to annually commemorate the accomplishments of Claude Shannon with a presentation by an outstanding information theorist. Rob, who received the IT Society’s Claude E. Shannon Award in 2015, was the 11th recipient of our Society’s highest honor to speak in the lecture series. Rob’s talk, *Remembering Shannon*, provided an insightful historical perspective on key developments—most notably, Shannon’s “mathematical theory of communication”—along the road from mechanical computing to the modern information age. The engaging narrative highlighted Rob’s technical versatility and his creative approach to connecting diverse aspects of mathematics, science, and engineering. The presentation slides are available on the Shannon Centenary Celebration website at http://cmrr-star.ucsd.edu/claude-shannon/.

The Shannon Memorial Lecture was followed by the announcement of the winner of the Shannon Graduate Fellowship. The purpose of this endowed fellowship, established by Jack Wolf in 2008, is to honor an outstanding graduate student at UCSD whose research is in the field of information theory. This year’s recipient, introduced by Young-Han Kim, was Joseph Connelly, a doctoral student of Ken Zeger, in recognition of his work in network coding.

The final invited lecture featured Dr. John E. Kelly III, IBM Senior Vice President, Cognitive Solutions and IBM Research, who spoke about *The New Era of Cognitive Computing*. His presentation conveyed the excitement that this new technology is generating, using recent applications of the IBM Watson platform to illustrate the growing number of scenarios in which cognitive computing is having an impact, from playing (and winning) *Jeopardy!* to diagnosing cancer to powering smart cities. The lecture was followed by a broad-ranging moderated discussion with Sandra Brown, Vice Chancellor for Research at UCSD.

Alon Orlitsky and Ingrid Daubechies.

The speakers were introduced by Alon Orlitsky (who shared photos of Ingrid at Burning Man!), Paul Siegel, and Vice Chancellor Sandra Brown, respectively.

The UCSD Shannon Centenary Celebration was organized by the Center for Memory and Recording Research (CMRR), the Information Theory and Applications Center, the Qualcomm Institute (QI), the Office of Research Affairs, and the Department of Electrical and Computer Engineering. Invaluable technical support was provided by CMRR staff members Iris Villanueva, Marina Robenko, and Gabby Tshamjyan, and by the QI Event Services team, led by Johnny Nguyen. Generous financial support came from the endowments of the JKW Lecture Series and the Shannon Memorial Lectureship, as well as from the IEEE Information Theory Society.

Shannon Centenary Workshop in Armenia “From Information Age to Big Data Era” October 3–5, 2016

Ashot N. Harutyunyan, Davit A. Sahakyan, and A.J. Han Vinck

For more information visit the workshop web: https://informationbigdata.wordpress.com/

On the occasion of the 100th anniversary of Claude E. Shannon Ashot N. Harutyunyan (VMware), Davit A. Sahakyan (Monitis) and A.J. Han Vinck (University of Duisburg-Essen) organized a workshop on Information Theory and Data Science. The workshop was hosted by VMware Armenia Training Center, from October 3 to 5, 2016 in Yerevan, Armenia.

The objective of the organizers was to initiate a conversation between the academia and industry, as well as engage students into modern and rapidly growing areas of research and technology innovation. They also aim at establishing a new track of cross-topic meetings of information theory and data science on a regular basis.

The 100th Shannon Centenary served as an occasion for a discussion forum on trends and opportunities connecting the Information Age to the modern era of Big Data, which started with a tremendous transformative impact on technologies, business, and our daily life. Intrinsically, the era of Big Data has been enabled by the preceding revolutionary Age of Information, when the science and technology of digital communications rapidly progressed and changed the reality we live in.

Speakers of the workshop with family members on panorama of Yerevan.

Several invited lectures were delivered by: Han Vinck on relations of information theory and big data; Gurgen Khachatrian (American University of Armenia) on security challenges in cloud computing; Mariam Haroutunian and Evgueni Haroutunian (Institute for Informatics and Automation Problems, Armenian National Academy of Sciences) on information theory research in Armenia; Yanling Chen (University of Duisburg-Essen) on secure communication in networked systems. Anahit Ghazaryan (School no. 21, Russian Ministry of Defense) lectured on biometrics and information theory. Her presentation summarized joint work with Vladimir Balakirsky who untimely passed away in 2013. Ashot N. Harutyunyan shared experiences in building an enterprise data analytics and relevant concepts from information theory.

Proceedings of the workshop can be downloaded from the event web: https://informationbigdata.wordpress.com/

2016 IEEE Shannon Centennial Workshop on Communications and Information Theory (SCWCIT 2016)

December 13–14, CDAC, Thiruvananthapuram, Kerala, India

Claude Elwood Shannon (April 30, 1916–February 24, 2001) was a renowned American mathematician, a genius electrical engineer, and an eloquent cryptographer. Due to his remarkable contribution in the field of information and communication technology, Shannon is considered as "the father of information theory." Shannon also contributed in many allied fields such as digital circuit design theory and cryptography.

The 2016 IEEE Shannon Centennial Workshop on Communications and Information Theory (SCWCIT 2016), during December 13–14, celebrated Shannon's 100th birthday at the Centre for Development of Advanced Computing (CDAC), Thiruvananthapuram, India. The workshop is sponsored by IEEE Information Theory Society and co-organized by the Indian Institute of Space Science and Technology, Center for Development of Advanced

(a)

(b)

Figure 1. (a) Wecome address by Dr.Chinmoy Saha, IIST and (b) Inauguration of the SCWCIT 2016 by Dr. V.K. Dadhwal, Director, IIST.

Figure 2. Speakers of SCWCIR delivering their lectures.

Computing, and IEEE Kerala Section (Antenna and Propagation society and Communications society).

The program was inaugurated by Dr. V.K. Dadhwal, Director, Indian Institute of Space Science and Technology, Trivandrum after the welcome address by Dr. Chinmoy Saha (Fig. 1). Dr. Vineeth B. S. (IIST) and Mr. Senthil Kumar (CDAC) were the organizing co-chairs for this workshop. The two day workshop featured Shannon centennial talks from eminent speakers such as Prof. Tapan K. Sarkar (Syracuse University, USA), Prof. Magdalena Salazar Palma (Carlos III University of Madrid, Spain), and Prof. Vikass Monebhurrun (CentraleSupelec, France), Prof. J. Y. Siddiqui (Institute of Radio Physics, Kolkata) and Birenjith P. S. (Govt. College of Engineering, Barton Hill). Prof. Tapan K. Sarkar (Fig 2(a)) delivered the first Shannon centennial lecture on "*Evolution of information theory from Maxwell to Shannon, Gabor, and Tuller from a physics perspective*" where the genesis and evolution of the field of information theory was highlighted great details. This was followed by a second Shannon centennial lecture by Prof. Magdalena Salazar Palma (Fig. 2(b)) on "*Simultaneous information and power transfer in wireless systems*" where theoretical and simulation analyses on information and power transfer possibilities, over the same wireless channel, by incorporating the transmitting and receiving antenna systems were thoroughly discussed. The last Shannon centennial lecture was delivered by Prof. Vikass Monebhurrun (Fig 2(c)) on "*How do we resolve uncertainty?*" which mainly focused on the application of polynomial chaos expansion method for the uncertainty quantification in numerical modeling using electromagnetic simulation tools. The first day of the workshop was concluded with a vibrant panel discussion on "*Information revolution in next decade: opportunities and challenges for India*" where current state-of-the-art of ICT was discussed along with its challenges in real-world implementations. The esteemed panelists for the topic were Mr. Sasi P. M. from CDAC, Prof. Raveendranathan from College of Engineering, Thiruvananthapuram, Dr. Deepak Mishra from IIST, and Dr. T. J. Aprem from Vikram Sarabhai Space Centre, Thiruvananthapuram. The panel was moderated by Dr. Chinmoy Saha, IIST.

Day-2 of SCWCIT 2016, December 14, started with a very interesting lecture by Prof. Jawad Y. Siddiqui from University of Calcutta on "*Remote diagnosis and patient monitoring in rural India—an IEEE AP-S SIGHT initiative*" where a conceptual method to diagnose and remotely monitor patients in rural India with the light of mobile communication technology was proposed. The talk was followed by another scintillating talk by Mr. Birenjith P. Sasidharan from Government Engineering College Bartonhill, Thiruvananthapuram on "*Distributed coding for storage*" where the concept of mutual information was highlighted. Apart from the technical talks, an undergraduate student poster presentation competition and a graduate student research discussion forum was also scheduled on Day-2. In the poster presentation competition, 10 student groups presented some of their early research results, and out of that, 3 best poster presenter groups were selected by the panel of judges. In a graduate research discussion forum, 7 research students presented some of their key research findings and also highlighted their future research directions. The two-day workshop, SCWCIT 2016, ended with a valedictory session where the three selected best poster presentation groups were awarded by the SCWCIT 2016 poster committee co-chairs. Moreover, all graduate research forum presenters were awarded mementoes by the SCWCIT 2016 workshop co-chairs. The closing ceremony was concluded by the vote of thanks by Dr. Vineeth B. S., the organizing committee co-chair of SCWCIT 2016.

The workshop was extremely successful in bringing together academicians, students, and engineering professionals in related fields to commemorate the contributions of Shannon through student poster presentations, and a student research discussion forum. Notably, the SCWCIT 2016 workshop was also covered by the leading news media of Southern India such as Indian Express, Madhyamayam, and Deepika.

Chinmoy Saha

Figure 3. (a) Talk by Prof, JY Siddiqui (b) A group-photo with the speakers and the organziers.

IEEE Information Theory Society Board of Governors Meeting

Location: Palmer House Hilton, Chicago, IL, USA
Date: 1 Oct 2016
Time: The meeting convened at 9:15am CDT (GMT-5); the meeting adjourned 2:15 CDT.
Meeting Chair: Alon Orlitsky
Minutes taken by: Stark Draper

Meeting Attendees: Jeff Andrews, Matthieu Bloch, Stark Draper, Michelle Effros, Abbas El Gamal*, Elza Erkip, Stephen Hanly*, Tracey Ho*, Frank Kschischang, Matt LaFleur#, Michael Langberg*, Pierre Moulin, David Neuhoff*, Krishna Narayanan, Alon Orlitsky, Anand Sarwate#, Emina Soljanin, Daniela Tuninetti, Rüdiger Urbanke, Aylin Yener, Wei Yu. (Remote attendees denoted by*, non-voting attendees by #.)

The IEEE Information Theory Society (ITSoc) President Alon Orlitsky called the meeting to order at 9:15am. Alon first summarized motions that were decided by email voting since the lastBoard of Governors (BoG) meeting:

1) The minutes of the July 2016 BoG meeting were approved.
2) It was decided that ISIT 2020 would be held in Los Angeles, California.
3) It was decided that ISIT 2021 would be held in Melbourne, Australia.
4) Rüdiger Urbanke was elected to serve as IEEE ITSoc President in 2017.
5) Elza Erkip was elected to serve as IEEE ITSoc First Vice-President in 2017.
6) Emina Soljanin was elected to serve as IEEE ITSoc Second Vice-President in 2017.
7) A motion was passed to send a message to the ITSoc membership regarding the proposedchanges to the IEEE Constitution that will be voted on in the fall 2016 IEEE election, anelection for which voting will close on 3 October 2016.

Alon next reviewed the meeting agenda.

Motion: A motion was made by Emina Soljanin to approve the agenda. The motion was seconded by Daniela Tuninetti. The motion was passed unanimously.

1) **President's Report:** Alon presented the President's report. Alon reported to the BoG that the state of society finances is solid. There are signifiant reserves. The 2016 ISIT was successful. There were 888 participants and 620 talks. Possibly this was the largest ISITever held outside the US. Current financial estimates for ISIT'16 (the books have yet to close) show 440K Euros income and a surplus of roughly 34K Euros. To date in 2016 about30 Shannon-tennials have been held with roughly 10 more scheduled by the end of the year.The BoG committed $55K (USD) to the Centennial. A balance remains, the use of which will be discussed later in this meeting. Alon thanked Shannon Centennial Committee Chairs Christina Frangouli and Rüdiger Urbanke and Committee Members Michelle Effros, Lav Varshney, Sergio Verdú for their efforts. Alon updated the BoG on the proposed IEEE amendment discussed in the last meeting. Over 40 of 50 technical societies and several past IEEE presidents have objected. Of the remaining ten societies one is supportive. Voting will close on 3 October. Alon previewed the updates that the BoG will receive in this meeting. Significant time has been set aside for forward-looking discussions. These includerethinking the organization of the Membership Committee, initiatives to found new journals,discussion of the Information Theory Paper Award, and other new initiatives for 2017. Alon reported the tentative scheduling and locations of BoG meetings in 2017: 12 February in San Diego (in connection with ITA), 25 June in Aachen (in conjunction with ISIT), and 30 September in Chicago (in conjunction with Allerton). Alon concluded his reports by thankingvolunteers who are concluding their terms of service. He thanked retiring BoG members Andrew Barron, Tracey Ho, Nick Laneman, Stephan Hanly, and Alex Vardy. He thanked retiring subcommittee chairs Osvaldo Simeone (Outreach) and Aylin Yener (Schools). He thanked retiring committee chair Nick Laneman (Massey), retiring Transactions Editor-in-Chief (EiC) Frank Kschischang, and retiring Senior Past President Abbas El Gamal. In conclusion, Alon welcomed the incoming Chair of the External Nominations Committee, David Neuhoff, and the incoming Second Vice President, Emina Soljanin.

2) **Treasurer's Report:** Treasurer Daniela Tuninetti presented her report on the state of the Society's finances. Daniela reviewed the budget for 2016 and the final forecast for 2017.

The budget for 2016 had a target surplus of $61K USD. However, the second-quarter forecast for 2016 forecasts a lower surplus due to reduced revenue from publications. Although there has been a decline in revenue from IEEE Xplore, in parallel, there has been a faster decline in publication expenses, due to lower Transactions page count and thus production costs incurred. The actual 2016 surplus will become more clear once the third-quarter 2016 forecast and actual surplus numbers from ISIT 2016 and ITW 2016 become available.

Given the 2015 operational surplus, the Society had up to $122K USD for 2016 new initiatives (according to the "50% rule"), of which the BoG scheduled $110K USD to spend on Shannon Centennial Events. The Shannon Centennial Committee has at present committed $55K USD and forecasts that it will not spend the full $110K USD amount.

Regarding the 2017 budget, the IEEE has almost approved the Society's proposed budget. The target surplus for 2017 is set to $11K USD. IEEE has also approved for inclusion in the 2017 budget a new initiative (according to IEEE's "3% rule") an expense of $105K USD to continue the set of broad outreach activities started with the Shannon Centennial Events in 2016.

Daniela raised a long-running BoG discussion of getting to a zero surplus, particularly in the context of funding new initiatives. Daniel recapped for the BoG the two IEEE rules that apply to funding new initiatives: the "50% Rule" and the "3% Rule". The "50% Rule" is as follows: if a society has a surplus of $X in a particular year it can spend $X/2 on new initiatives in the following year. The "3% Rule" is as follows: a society can spend up to 3% of its reserves in any given year on new initiatives. However, spending under the 3% Rule must first be approved by the IEEE and must be included in the budget. So, for instance, under the 3% Rule the IEEE has allowed the ITSoc to spend 2.5% of its reserves on new initiatives in 2017. This amounts to roughly $117k. Initiatives that this funding may be spent on will be discussed later in the meeting.

A discussion of the sources of ITSoc revenue followed. In contrast to most IEEE societies that rely on meetings to generate income, most ITSoc's revenues come from publications.As Daniela reported, income from publications, measured by clicks on IEEE Xplore, is decreasing. If this trend continues it may be a topic the BoG will have to consider.

3) **Transactions:** Transactions EiC Frank Kschischang presented a list of candidates to serve as associate editors.

> **Motion:** Frank made a motion to approve the list. The motion was seconded by Michelle Effros. The list was approved unanimously.

Frank next presented a proposal for a special issue of the Transactions to be dedicated to the memory of Solomon Golomb. The title would be "Shift Register Sequence in Memory of Solomon W. Golomb". The proposers, who would serve as the guest editors are Guang Gong, Tor Helleseth, and Vijay Kumar. This would be a 13th issue of the Transaction, to appear in 2018. There was a discussion of special issues generally, which have beencurtailed of late, the pros and cons of special issues, as well as the proposed scope and logistics of the issue. Frank will communicate the discussion points back to the proposers.

4) **Nominations and Appointments (N&A) Committee:** As his first order of business N&A Committee Chair Abbas El Gamal nominated Alexander Barg to serve as the next Executive Editor of the Transactions. The following motion was recommended by the N&A Committee and moved by Committee Chair Abbas El Gamal:

> **Motion:** "To appoint Alexander Barg as Executive Editor of the Transactions for the term extending from 1 January 2017 to 30 June 2018." The motion passed unanimously.

Abbas reviewed the new appointments to various committees: Fellows, Cover, Shannon, Wyner. Almost all committees are now fully staffed.

Abbas then discussed a proposal to move the Cover, Shannon, and Wyner appointmentcommittees to the task list of the Senior Past President to deal with at the end of their term. This has been the practice for the past two years. This was for information only.

5) **Conference Committee:** Elza Erkip presented the Conference Committee report on behalfof Committee Chair Emanuele Viterbo. Elza first reviewed the ISITs from 2016–2021. In Barcelona, the budget is not quite closed, but the current estimated surplus is 34K Euros.Detailed budgets for ISITs 2017–2019 were not available for the BoG to review at themeetings. Budget details will be shared with the BoG with approvals to be conducted online:

> **(Discussion and online motion)** ISIT 2017 in Aachen: 800 participants are expected and the base registration (IEEE + ITSoc membership + early) will be 620 Euros.
>
> **(Discussion and online motion)** ISIT 2018 in Vail: 850 participants are expected and the base registration (IEEE + ITSoc membership + early) will be $750 USD.
>
> **(Discussion and online motion)** ISIT 2019 in Paris: 800 participants are expected and the base registration (IEEE + ITSoc membership + early) will be 770 Euros.

The BoG inquired whether Paris would have a low-cost student housing option, e.g., in dorms. The BoG also requested that Aachen organizers be asked to ensure that there is astudent housing option (if one has not already been arranged). There was general consensus that, except in exceptional circumstances, any future ISIT should provide a dormitory housing option for students.

Organizers are targeting conference surpluses of approximately 10%. This engendered a discussion of the use of the surplus to fund other ongoing activities of the society such as long-term running schools.

The books of ITW Cambridge are currently closing, with a surplus of 5% expected. ITW Taiwan is on-track for 2017. Interest has been expressed in organizing an ITW for 2018, but discussions are at a very early stage. There appears to be a slow down in ITW proposals, and a discussion ensued of how the Conference Committee brings in ITW proposals. It may be the slowdown is negatively correlated with the arrival rate of ISIT proposals. It was also pointed out that ITWs are widely distributed geographically. Proposals of ITWs to be held closer to geographic clusters of ITSoc members would be welcome. The following motion was recommended by the Conference Committee, moved by Elza Erkip:

> **Motion:** "To approve technical co-sponsorship of the 15th Int. Symp. on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks (WiOpt 2017), to be held in Paris, France." The motion passed unanimously.

In conclusion, Elza reviewed Committee recommendations intended to reduce conference waste: reduced use of USB sticks to distribute proceedings (which, e.g., at ISIT'16 and ITW'16 were both made available online for the duration of the conference), conference bags, paper programs, and various printouts. This discussion engendered a wider discussion of standardization among ITSoc conferences.

6) **Membership Committee:** Membership Committee Chair Elza Erkip reviewed the makeup of the Committee and its duties, which includes selection of ITSoc distinguished lecturers. Elza reviewed proposed changes to the Distinguished Lecturer program to increase activity, to encourage chapters to contact lecturers, to encourage lecturers to help identify lecturing opportunities, and to improve the nominations process.

   Elza reviewed recent activities of the Student Subcommittee (e.g., meet the Shannon Lecturer at ISIT), the Outreach Subcommittee (e.g., ISIT round table mentoring event with 18 mentors and roughly 120 attendees), and the Women in Information Theory (WITHITS) Group (e.g., 'Samoan Circle' at ISIT and a lunch event at Allerton). The Outreach Subcommittee also runs the mentoring program and has been surveying current program participants for feedback.

7) **Online Committee:** Online Committee Chair Anand Sarwate reviewed the activities of the Committee. The main update is that the new website is active! Anand recently received a generic email from IEEE about complying with IEEE website standards (including branding and formatting). Anand will keep the BoG appraised of any future developments. The Committee's next steps include: integration of social media, upgrading the way news and announcements are emailed, archiving and consolidation of content, solicitation of contributed content including research tutorials, teaching, and other materials. The committee would appreciate receiving press releases for each ITSoc award so that it could post these to the website.

8) **External Nominations Committee:** Incoming Committee Chair David Neuhoff reviewed the membership and mandate of the committee and its current efforts. Focusing on awards and medals for which ITSoc members have been awarded in the past, there are four principal awards with mid-January deadlines, and six IEEE medals that have mid-June deadlines. The committee is soliciting nominations for these awards. There was discussion surrounding which awards the committee should solicit for and how the nominations process works. Dave emphasized that the job of the committee is to identify a candidate along with someone who could serve as nominator. Dave also reviewed some improvements that have been made in how the committee tracks nominations and awards made, with the aim of aiding current and future committees.

9) **Newsletter:** Newsletter Editor Michael Langberg reviewed the goals, logistics, and typical content of the Newsletter. There are technical contributions, mostly of a survey nature, which come from ITSoc and sister societies. A student column has been a new addition this year. Going forward the table of contents of each edition of the Transactions will be printed, as well as of Foundations and Trends in Communications and Information Theory, and, if possible, Problems of Information Transmission. The budget impact of this addition was discussed. It was suggested that each title in the online version of the Newsletter should link directly to the corresponding PDF on Xplore. Going forward workshop and conference organizers, as well as organizers of other activities that receive ITSoc financial support, will be required to submit reports to the Newsletter. Michael noted that the Newsletter's page count this year has been slightly higher than forecast. Therefore, the Newsletter may be slightly above budget. Michael also mentioned the passing of Solomon Golomb, who was a long-term contributor of puzzles to the Newsletter. A collection of his puzzles will be published over the next four issues. Michael is working with Alon, Daniela and Rudi to look into publishing all of Solomon Golomb's Newsletter puzzles as a stand-alone book.

10) **Shannon Documentary:** Writer and director of the Shannon documentary, Mark Levinson, called in to provide the BoG a status update. Mark talked about how exciting it is to bring to life a figure whose work has impacted us all, but who is not so well known. In the historical record there are no film interviews with Shannon, and there is very little footage of Shannon at all. On the other hand, transcripts exist of quite lengthy interviews. Mark characterized Shannon in these interviews as self-deprecating, sharp, playful, and funny. Mark's goal is to recreate what such an interview might have been like had Shannon conducted one on film. This "faux-interview" would anchor the film. Shannon's family has been supportive. His daughter sat down for a long interview and his son contributed as well. Mark's plan is to recreate the toy room in Shannon's house in Winchester, Massachusetts, a house that is still in the family. Mark has nearly finished scripting the faux-interview. He will circulate the script to a couple possible actors in next week. His goal is to shoot this central anchor of film by end of 2016. Following that, there will be documentary work. He is targeting to complete the film in late 2017. Mark's original target length was 50 minutes. This would have allowed the film to be shown in a one-hour television slot. However, the project is growing toward feature length, 70-80 minutes. The BoG asked Mark whether a feature length film could be edited to produce a short film also, of 15-20 minutes duration, for use in other venues.

11) **Pilot videos project:** Matthieu Bloch reported on a pilot project to produce educational videos. The initial objective is to create two videos showcasing successful applications of information theory: MIMO and network coding. The choice was made to focus initially on real-world technologies with the hope of engaging the general public. The target audience is a high school student, someone interested in technology but that doesn't (yet) have a deep technical background. Target venues include YouTube and social media outlets. Brit Cruise will be hired to create the first two videos. Brit Cruise has produced many videos for Khan Academy, including those on information theory. In contrast to the videos on information theory currently available Khan Academy, which focus on very basic topics, the content in question will highlight these more advanced applied topics. The budget for the initiative will derive from the balance of funds directed towards the Shannon Centennial. The current focus is the development of scripts. Matthieu encourages ITSoc members to volunteer to participate in this project.

12) **Online Instruction Initiative:** Suhas Diggavi reviewed for the BoG the goals of the Online Instructional Initiative. Currently a few committees are being arranged: steering (oversight), organizing (curate talks, maintain portal), finances (budgeting). A motion will be made later in the meeting to request $10K USD to initiate the creation of invited and curated content. The goal is to create, videotape, archive, and post online, 10 expository lectures.

13) **Schools Subcommittee:** Schools Subcommittee Chair Aylin Yener presented her report. The 2016 NASIT was held at Duke University in June 2016, had 99 student attendees, 5 lecturers, and social activities. The Joint Telematics Group/IEEE ITSoc Summer School was held at the Indian Institute of Science, Bangalore, in June/July 2016 had 121 attendees. The Indian School consisted of three short courses, each of 8 hours length, spread over 5 days.

    Aylin presented a proposal to hold the 2017 Latin American Week on Coding and Information in Brazil. This school will be three days long, will be held at University of Campinas (Unicamp), and will be held in (serial) conjunction with a three-day workshop. The School plus workshop are scheduled to run from 22 to 27 July, 2018. Expected attendance is 60 students, and speakers have mostly already been confirmed. Schools have been held in Brazil in the past, but have not been supported by ITSoc. The current hope is to hold a Latin American school every other year. While the request for funds is quite far in advance, at least in terms of the development of the ITSoc 2018 budget, the organizers are requesting ITSoc support early so it can serve as seed funding to attract other support. The BoG deferred discussion of the level of support till later in the meeting.

14) **Membership Committee Reorganization:** Elza Erkip discussed a possible reorganization of the Membership Committee. She summarized the Committee's duties: selection of the Chapter of the Year, appointment of distinguished lecturers, selection of the Padovani Awardee. The Committee has four subcommittees: (i) Schools, (ii) Student, (iii) Outreach, (iv) WITHITS. Between the Committee and the four subcommittees there are lots of volunteers. The first proposal is to move the Schools Subcommittee out of Membership, either to promote that subcommittee to committee level (due to its high level of activity) or to place it under the Conference Committee. The Committee and remaining subcommittees would then be reorganized to integrate all duties into a single structure. The Committee would continue to be headed by the Second Vice-President. Other members and their duties would include one liaison for chapters, two liaisons for WITHITS, two liaisons for student and outreach responsibilities, and two to three students and postdocs members. It was noted this is the only ITSoc committee on which students and postdocs can serve. Members' terms will be of two years' duration, and will be staggered. The exception will be the student and postdoc members whose terms will be of one year's duration. The Committee suggests to the BoG that it try out such a reorganization for one year and report back before formalizing into the bylaws. There was discussion of the roles and how the new committee structure would work, that a similar restructuring had been suggested in the past, and of the roles of the student and postdoc members. The responsibility for choosing the Padovani Lecturer might be shifted to the Schools Subcommittee. A decision on where the Schools Subcommittee would be placed in the organizational structure will be deferred until the proposed changes are tested for one year.

15) **New publications (JSTIIT & IT Magazine):** Jeff Andrews and Elza Erkip next picked up the discussions of new publications that they initiated at ISIT, respectively, of a special topics journal "Journal on Selected Topics in Information Theory" and of an "Information Theory Magazine".

    Jeff first discussed the Transactions in the context of the journals published by sister societies. ITSoc is unusual in having only a single journal. The core proposal is to have a new special topics journal with four to six issues each year, with a sub-to-pub time of under one year, and with a two-fold focus including both hot topics in core information theory and cross-cutting topics. First steps would include establishing a prestigious meta-Editorial board, pro-actively seeking out the first ten special issues, ensuring that at least half of the first ten issues are cross-cutting, and establishment of a culture of quality-over-quantity. Jeff reviewed various benefits to the ITSoc: technical, logistical, and financial.

    As Elza next outlined, the desire for an IT Magazine is driven by the question of how to reach out to the non information theory community. A magazine would provide the right venue for tutorial-style papers that could emphasize insights and potential uses of a line of research. It would blend traditional information theory areas with new ones. She noted that the magazines of sister societies such as Signal Processing (SP) or Communications (Comm) are well cited. Furthermore, much of the content now delivered through the Newsletter—the President's column, conference reports, a list of upcoming conferences—could rather be delivered through a magazine.

    There was a wide-ranging discussion of the examples of the SP and Comm magazines, the way they attract papers from industry, the way they standardize submission formats, the fact that the SP Society also has an electronic newsletter. The consensus was that all ITSoc publications need to maintain the example of extremely high quality publications that the Transactions sets. It was also discussed how a new publication could complement the Transactions, and if papers could be pushed from one to the other as appropriate. Finally, it was felt that the idea of a special topics journal being cross-cutting and fostering outreach to other communities should be very strongly emphasized from the get go, e.g., in the selection of those first ten issues. On the cautionary side, it was noted that ITSoc is about 1/6th or 1/10th the size of the SP and Comm Societies, and launching and maintaining one or two new publications would take significant effort. Finally, the idea of an IT Magazine was thought to have been raised some years back. The report generated at that point will be unearthed and its recommendations considered. An ad-hoc committee will be formed, headed by Jeff Andrews and Elza Erkip.

16) **Finances for new initiatives:** Daniela Tuninetti discussed some budgetary issues related to the pilot videos project and the online instructional initiative, discussed earlier in the meeting by Mathieu Bloch and Suhas Diggavi, respectively. Currently, the only upcoming new initiatives are the online instructional initiative and the Latin America school.

    Motion: Suhas made, and Elza Erkip seconded, the following motion: "To allocate $10K USD to the effort to start up the online education initiative." The motion passed unanimously.

    The Schools Subcommittee recommended the following motion, moved by Committee Chair Aylin Yener:

    Motion: "To approve IEEE ITSoc BoG supports the Latin American Week of Coding and Information at the amount of $15K USD." The motion passed unanimously.

    The first of the above motions will be funded under the 3% rule, and the latter under the 50% rule, for new initiatives.

17) **Paper Award Discussion:** Rüdiger Urbanke initiated a discussion of the IT Paper Award. This year, for the first time in decades, the Award was given to two unrelated papers. It had been observed by many that part of the bottleneck resulted from the fact that the window of eligibility for the Paper Award extends only two years from the year of publication. Two years does not allow much time for smoothing out the flow of top-notch papers.Furthermore, such a short window can also cause problems because two related papers can appeared in distinct windows. Rudi proposed to lengthen the window from two to four years. Four years is not too long, but likely long enough to alleviate many issues. Rudi also mentioned the IEEE W.R.G. Baker Award. The Baker Award is currently scheduled to vanish as an IEEE-wide award. Several Societies are discussing the possibility of resurrecting it as a society-level award with a long time windows of eligibility (significantly longer than four years). The thought is that the (resurrected) Baker Award could be used to recognize papers of significance that have appeared in the past 15–20 years, the significance of which was not realized at the time of publication.

18) **Adjournment:** The meeting was adjourned at 2:15 CEST.

From the President

continued from page 1

specific core IT topics. This is perhaps the single-most important initiative for this year. It will influence our path for the foreseeable future.

We have significant financial reserves built up over the years. These are not easy to access, but it can be done. If you have suggestions how to reinvest them into our future and are willing to help, please let me know.

I would like to thank the members of the ``shift register'' for their service and dedication: Junior past president Alon Orlitsky, senior past president Michelle Effros, and Abbas El Gamal, who concludes a five-year tour of dedication through the society ranks. Please join me in congratulating and thanking them! And looking into the future, Elza Erkip has shifted into the position of 1st Vice President and Emina Soljanin has joined as 2nd Vice President. It is the first time in our history that the X outnumber the Y, time to Xelebrate!

Last but not least, I would like to thank Matt LaFleur, our ``inside'' man at IEEE. He has made the job of the officers significantly easier and many of the recent initiatives would not have been possible without his help.

On a final and more philosophical note. We, as scientists and engineers, are unusually lucky to speak a universal language. We can contribute to important problems no matter where we live and work. An open exchange of ideas and regular meetings in person are essential for us. As one president to another, let me suggest to keep it that way!

GOLOMB'S PUZZLE COLUMN™ COLLECTION, Part 3

Beyond his extraordinary scholarly contributions, Sol Golomb was a long time newsletter contributor enlightening us all, young and old, with his beautiful puzzles. In honor of Sol's immense contribution to the newsletter, a collection of his earlier puzzles dated back to 2001 appears in 4 compiled parts over previous, current, and upcoming issues. Part 3 is given below. He will be greatly missed.

Reprinted from Vol. 51, No. 2, June 2001 issue of Information Theory Newsletter

GOLOMB 'S PUZZLE COLUMN$^{\text{TM}}$ AN INGENUITY TEST SOLUTIONS

1. To solve the simultaneous equations for x and y in terms of a and b,

$$x^2+xy+x=a$$
$$y^2+xy+y=b,$$

where a and b are positive real numbers, take the sum and the difference of the two equations:

$$(x^2+2xy+y^2)+(x+y)=a+b;\ (x^2-y^2)+(x-y)=a-b$$
$$(x+y)^2+(x+y)-(a+b)=0;\ (x-y)(x+y+1)=(a-b).$$

$$(x+y)=\frac{-1\pm\sqrt{1+4(a+b)}}{2};\ (x-y)=$$

$$\frac{a-b}{(x+y)+1}=\frac{2(a-b)}{1\pm\sqrt{1+4(a+b)}}=\left(\frac{a-b}{a+b}\right)\left(\frac{-1\pm\sqrt{1+4(a+b)}}{2}\right).$$

Then

$$2x=(x+y)+(x-y)=\left(\frac{a-b}{a+b}+1\right)\left(\frac{-1\pm\sqrt{1+4(a+b)}}{2}\right),$$

and

$$x=\left(\frac{a}{a+b}\right)\left(\frac{-1\pm\sqrt{1+4(a+b)}}{2}\right),$$

$$y=\left(\frac{b}{a+b}\right)\left(\frac{-1\pm\sqrt{1+4(a+b)}}{2}\right).$$

For example, if a=4, b =2, the two solutions are (x,y)=$(-2,-1)$ and $(x,y)=\left(\frac{4}{3},\frac{2}{3}\right)$.

2. When $n(n+1)/2$ points are arranged to form an equilateral triangle with n points on a side,the number $f(n)$of three-point subsets (of any size, in any orientation) which form the vertices of an equilateral triangle is $\binom{n+2}{4}$ for all $n\geq 1$. The shortest proof I've seen so far (from Joe Buhler) is longer than I'd like. I'm still hoping that some reader will find a simple, clever proof.

3. Given an $m\times n$ "square array"of dots, a continuous path P is drawn from the upper left to the lower right corner, where P consists entirely of straight line segments, goes through all mn dots, changes direction only at dots, stays inside the $m\times n$ rectangle, and never intersects itself. The interior of the rectangle can then be two-colored from the way this region is partitioned by P, where adjacent regions separated by P have opposite colors. The problem was to show that within the rectangle, the two colors cover equal areas.

   This result is a direct corollary of *Pick's Theorem* [1], [2], which asserts: "Suppose a 'lattice polygon' P has all its vertices at points of a square lattice L . Then the area of (the interior of) P is $i+\frac{b}{2}-1$, where i is the number of lattice points in the interior of P, and b is the number of lattice points on the boundary of P". In our application, all mn points of the lattice are "on the boundary", so the areas of the two colors are equal.

4. On an $m\times n$ "square array" of dots, a continuous path P consisting entirely of straight line segments goes through all mn dots. In this problem the path P may go outside the $m\times n$ rectangle, turn at arbitrary locations, and intersect itself. You were asked for the smallest number of segments that P can contain, in terms of m and n. The answer is min($2m-1$, $2n-1$, $m+n-2$). For a detailed treatment, see [3].

5. "Given a cubic polynomial $g(x)$ with non-zero roots r_1, r_2, r_3 such that $\frac{g(\alpha)+g(-\alpha)}{g(0)}=K$, where α and K are real, $\alpha\neq 0$ and $K\neq 2$, find the value of $\frac{1}{r_1r_2}+\frac{1}{r_2r_3}+\frac{1}{r_3r_1}$ in terms of α and K."

   This value is $\frac{K-2}{2\alpha^2}$, as follows: Let $g(x)=ax^3+bx^2+cx+d$. Then $g(\alpha)+g(-\alpha)=2b\alpha^2+2d$, and $g(0)=d$, so $K=\frac{2b\alpha^2}{d}+2$. Now also, $g(x)=a(x-r_1)(x-r_2)(x-r_3)=ax^3-\mathrm{a}(r_1+r_2+r_3)x^2+a(r_1r_2+r_2r_3+r_3r_1)x-ar_1r_2r_3=ax^3+bx^2+cx+d$. Next, $\frac{b}{d}=\frac{r_1+r_2+r_3}{r_1r_2r_3}=\frac{1}{r_1r_2}+\frac{1}{r_2r_3}+\frac{1}{r_3r_1}$, but $\frac{b}{d}=\frac{K-2}{2\alpha^2}$.

6. "If A, B, C are positive integers with $A+\frac{1}{B+\frac{1}{C+1}}=\frac{115}{36}$, find $A^2+B^2+C^2$."

   Clearly, A is the integer part of $\frac{115}{36}=3\frac{7}{36}$, so A=3. Subtracting 3 from both sides, $B+\frac{1}{C+1}=\frac{36}{7}=5\frac{1}{7}$, so B=5, and then $C+1$=7 so C=6. Therefore, $A^2+B^2+C^2=3^2+5^2+6^2=70$.

References

[1] H. Steinhaus, *Mathematical Snapshots*, Oxford Univ. Press, New York, 1969.

[2] B.Grünbaum and G.C. Shephard, "Pick 's Theorem", *American Math. Monthly*, vol. 100, no. 2, February, 1993, 150-161.

[3] S.W. Golomb and J.L. Selfridge, "Unicursal Polygonal Paths and Other Graphs on Point Lattices", *Pi Mu Epsilon Journal*, vol. 6, no. 3, Fall, 1970, 107-117.

Reprinted from Vol. 51, No. 3, September 2001 issue of Information Theory Newsletter

GOLOMB'S PUZZLE COLUMN™

Sums and Products of Digits Solutions

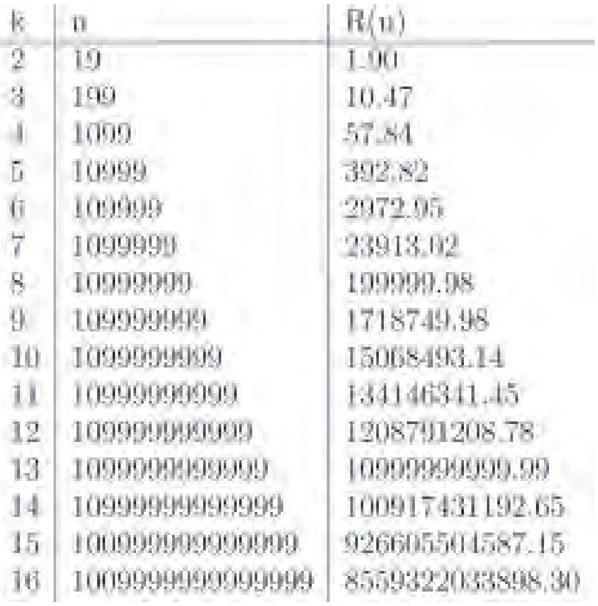
Recall that for each positive integer n, $S(n)$ is the sum of the decimal digits of n, $P(n)$ is the product of the decimal digits of n, and $R(n) = n/S(n)$.

1. The known solutions to $S(n) \cdot P(n) = n$ are $n = 1$ (with $1 \cdot 1 = 1$), $n = 135$ (where $(1+3+5)(1 \cdot 3 \cdot 5) = 9 \cdot 15 = 135$), and $n = 144$ (where $(1+4+4)(1 \cdot 4 \cdot 4) = 9 \cdot 16 = 144$). These are the only solutions with $n < 10^7$. For all *very* large n (say $n > 10^{60}$), $S(n) \cdot P(n) < n$, so there are only finitely many solutions, but there may be more than the three just listed.

2. Not every positive integer m occurs in the form $R(n) = n/S(n)$. The values of $m \leq 100$ not of this form are (only) $m = 62$,63, 65, 75, 84, and 95.

If $m = R\ (n) = n/S(n)$, we have $n = mS(n)$, and n must be a multiple of m. We know that 9 divides n if and only if 9 divides $S(n)$, so if $S(9m) = 9$, then $R(9m) = (9\ m)/9 = m$. For $1 \leq m \leq 100$, $S(9m) = 9$ in 55 cases.The other 45 cases are the numbers from $10\,j+1$ to $10\,j+j$, for each j from 1 to 9. In 35 of these remaining 45 cases, $S\ (18m) = 18$, so in these cases $R(18m) = m$. The ten remaining values of m are: 62, 63, 64, 65, 73, 74, 75, 84, 85, and 95. Four of these occur as values of $R(n)$ as follows: $R(320) = 64$, $R(511) = 73$, $R(1998) = 74$, $R(1275) = 85$. (The case $m = 74$ corresponds to the situation where $S(27m) = 27$). It is easy to show that for any $x > 0$,we have $R(n) > x$ for all $n > N_x$, so it is a finite verification process to show that a given m never occurs as $R(n)$.

3. The k-digit number n for which $R(n)$ is a minimum, for all $k > 1$, has the following characteristics: It consists of a 1 followed by r 0 's followed by k - r - 1 9 's. Since we are trying to minimize $R(n) = n/S(n)$ over all k-digit numbers, we are trying simultaneously to make n small and to make $S(n)$ large. The extremal value of n must clearly have the form $10 \cdots 099 \cdots 9$ to achieve this minimum, though the value of r (the number of consecutive 0's) requires a more careful argument. The cases with $2 \leq \mathrm{k} \leq 16$ are as follows:

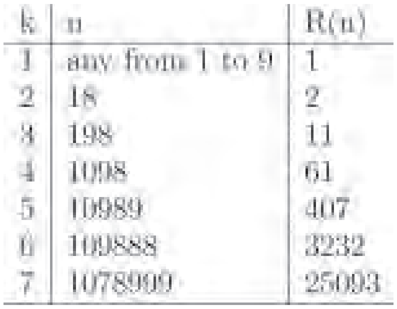


k	n	R(n)
2	19	1.90
3	199	10.47
4	1099	57.84
5	10999	392.82
6	109999	2972.95
7	1099999	23913.02
8	10999999	199999.98
9	109999999	1718749.98
10	1099999999	15068493.14
11	10999999999	134146341.45
12	109999999999	1208791208.78
13	1099999999999	10999999999.99
14	10999999999999	100917431192.65
15	100999999999999	926605504587.15
16	1009999999999999	8559322033898.30

Note that exponentially many more 9's are adjoined for each additional 0 inserted.The first 0 appears at $k = 4$, the second 0 at k =15, the third 0 at $k = 116$, and in general, the r^{th} 0 (between the initial 1 and the left-most 9) appears at $k = \left(\frac{10^r - 1}{9}\right) + (r+2)$, for all $r \geq 0$.

4. Among all k-digit integers, $R(n)$ is an integer $I(k)$ times, with $I(1) = 9$, $I(2) = 23$, $I(3) = 180$, $I(4) = 1325$, $I(5) = 10334$, $I(6) = 83556$, and $I(7) = 710667$. Did you find further values of $I(k)$, or detect any patterns?

5. The k-digit numbers which give minimum *integer* values for $R(n)$ are as follows:



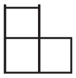
k	n	R(n)
1	any from 1 to 9	1
2	18	2
3	198	11
4	1098	61
5	10989	407
6	109888	3232
7	1078999	25093

Were you able to extend this table, or to detect any pattern?

Reprinted from Vol. 51, No. 4, December 2001 issue of Information Theory Newsletter

GOLOMB'S PUZZLE COLUMN ™

TILINGS WITH RIGHT TROMINOES SOLUTIONS

1. To prove, by mathematical induction on n, that a single square (a "monomino") can be removed from anywhere on the $2^n \times 2^n$ board and then the rest can be tiled with "right trominoes" (three quadrants of a 2 × 2 square, ), we start at $n = 1$, and observe that whichever square is removed from a $2^1 \times 2^1$ board, what is left is a single right tromino. (It is more sophisticated to start the induction at $n = 0$, where after removing a monomino from the $2^0 \times 2^0$ board *nothing* is left, which can be tiled using zero right trominoes!)

The inductive assumption is then that when a single square is removed from anywhere on the $2^k \times 2^k$ board, the rest can be tiled with right trominoes. Now consider the $2^{k+1} \times 2^{k+1}$ board. Divide it into four $2^k \times 2^k$ quadrants. Wherever a monomino is removed from the original $2^{k+1} \times 2^{k+1}$ board, the rest of that quadrant can be tiled with right trominoes by the inductive assumption. From each of the other three quadrants, remove the square touching the center of the $2^{k+1} \times 2^{k+1}$ board. The rest of those quadrants can be tiled with right trominoes by the inductive assumption, and the three removed squares can be replaced by a single right tromino. (See Figure 1.)

Note. This first appeared in December, 1954, in [1], which was the text of a talk I gave in November, 1953, to the Harvard Math Club. This result has reappeared so often that to many people it now has the status of a "folk theorem".

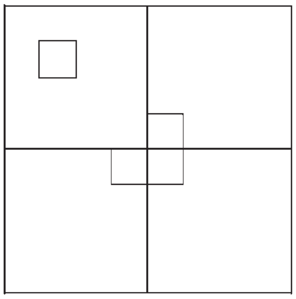


Figure 1: $2^{k+1} \times 2^{k+1}$ board partitioned into quadrants.

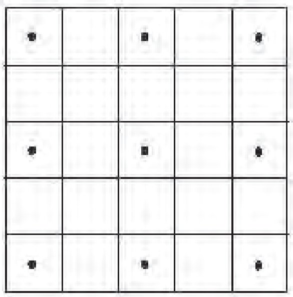


Figure 2: The 9 locations where a monomino can be removed.

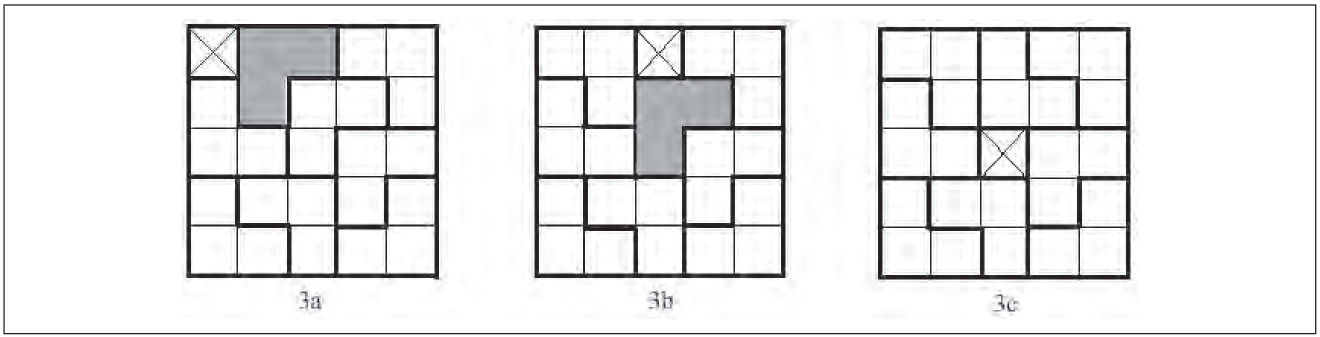


Figure 3: Tilings of the 5 × 5 board with a monomino removed.

2. There are nine locations on the 5 × 5 board where a single square (monomino) can be removed such that the rest of the board can be tiled with right trominoes. These 9 locations are marked by dots in Figure 2. Note that no two of the dotted squares can be covered by the same right tromino. Therefore, if none of these squares is removed, a tiling will require 9 right trominoes, for a total area of 9 × 3 = 27, which is impossible on a board whose total area is 25.

To show that all 9 of these locations are possible, we note that only 3 locations are inequivalent relative to the symmetries of the 5 × 5 square. Examples of the three tilings are shown in Figure 3.

Note the similarity of these three examples. To get from 3*a* to 3*b*, flip the shaded monomino in 3*a*. To get from 3*b* to 3*c*, flip the shaded monomino in 3*b*.

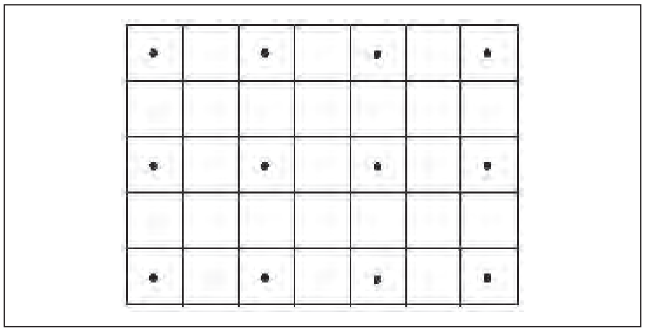
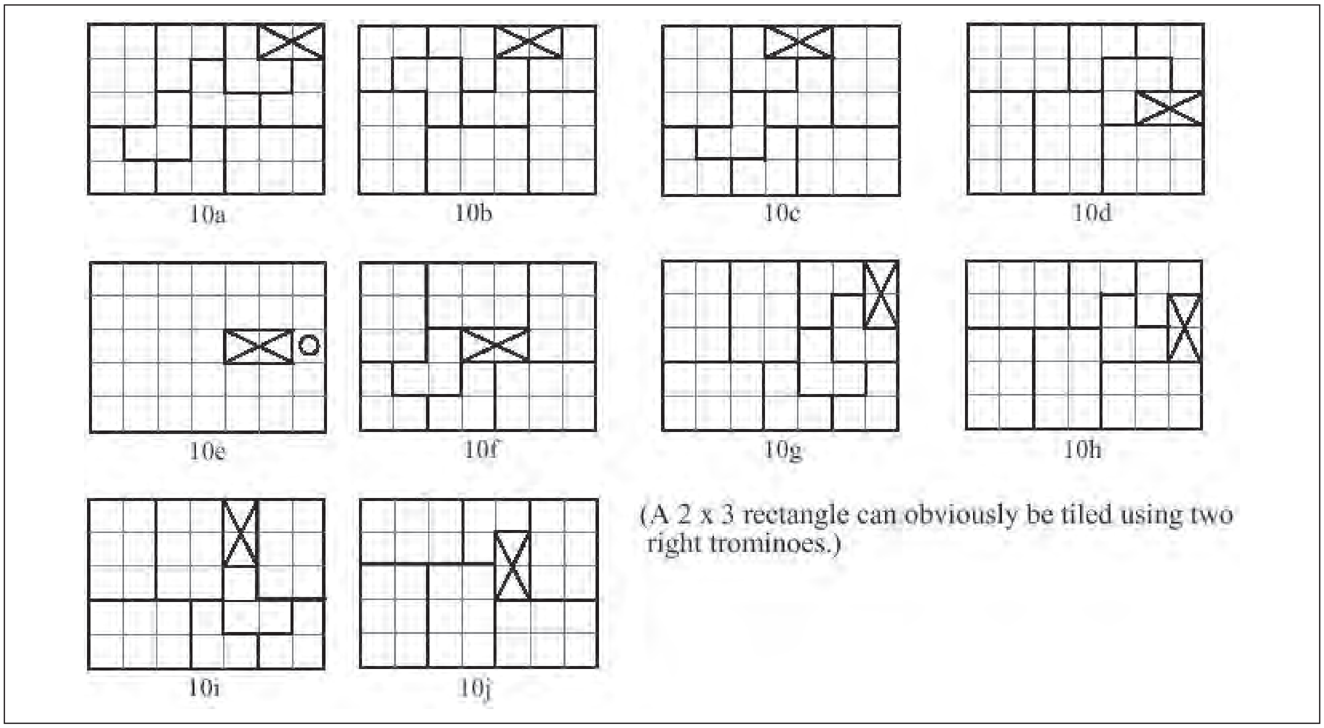


Figure 4: The "dotted" squares on the 5 × 7 board.

3. There are 9 inequivalent locations (relative to the symmetries of the 5 × 7 rectangle) where a domino can be removed, such that the rest can be tiled by right trominoes.



(A 2 x 3 rectangle can obviously be tiled using two right trominoes.)

Figure 5: The ten inequivalent locations for a domino that covers a dotted square on the 5 × 7 board.

Reprinted from Vol. 51, No. 4, December 2001 issue of Information Theory Newsletter continued

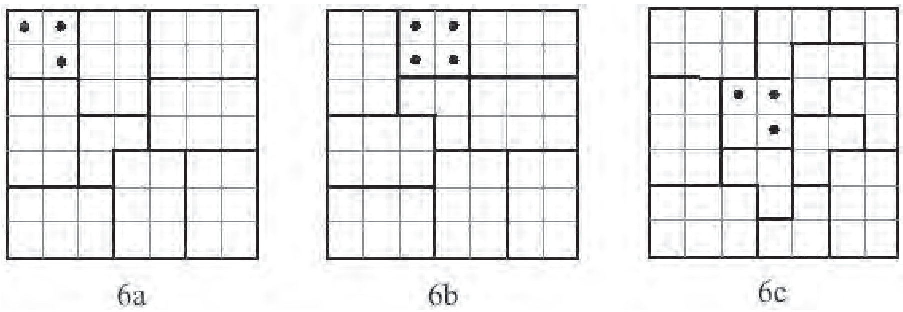


Figure 6: Wherever a monomino is removed from the 7 × 7 board, the rest can be tiled with right trominoes.

Note that for a successful tiling, the removed domino must cover one of the 12 "dotted" squares in Figure 4.

Since no two of the dotted squares can be covered by the same right tromino, if all 12 remain unremoved, a tiling will require at least 12 right trominoes, for a total area of 3 × 12 = 36, which exceeds the area of the 5 × 7 board.

There are 10 inequivalent locations for a single domino that covers one of the 12 dotted squares, as shown in Figure 5, with tilings by right trominoes on 9 of them.

Note that in figure 10e, the square containing "0", to the right of the domino, cannot be filled in by part of a right tromino without creating an impossible situation for completing the tiling.

4. A monomino can be removed from *anywhere* on the 7 × 7 board, and the rest can be tiled with right trominoes! The three cases in Figure 6 suffice to show this, where the ten dotted squares represent all the inequivalent positions for the monomino.

5. For the proof that "for all $m > 5$ with m not a multiple of 3, a monomino can be removed from anywhere on the $m \times m$ board and the rest can be tiled by right trominoes", see [2].The proof is inductive, but not nearly so simple and elegant as the inductive proof in problem 1.

6. For an $a \times b$ board to be tiled by right trominoes, it is clearly necessary that at least one of a and b must be a multiple of 3. This necessary condition is also sufficient except when one dimension (either a or b) is 3 and the other is odd, or when either a or b equals 1. (This result is Theorem 1 in [3], and the proof is not difficult, though dealing with the special cases may seem a bit tedious.)

References

[1] S.W. Golomb, "Checkerboards and Polyominoes", *American Math. Monthly*, vol.61, no. 10, December, 1954, 675-682.

[2] I.P. Chu and R. Johnsonbaugh, "Tiling deficient boards with trominoes", *Math. Mag*. 59 (1986), 34-40.

[3] J.M. Ash and S.W. Golomb, "Tiling rectangles and deficient rectangles with trominoes", in preparation.

Reprinted from Vol. 52, No. 1, March 2002 issue of Information Theory Newsletter

GOLOMB'S PUZZLE COLUMN™

WHAT COLOR IS MY HAT? SOLUTIONS

1. In this version, the members of the team are lined up single file, and each member sees the colors of all the hats ahead, but not his/her own or those behind. They are promised that not all the hats will be the same color; and they will be interrogated ("What color is your hat?") from the back of the line forward, one at a time. Each member can say either "white" or "black" or "pass". A single wrong color causes the whole team to lose, which also happens if they all say "pass".

A winning strategy is the following: When it is a member's turn, if all behind him/her have said "pass", that member will also say "pass" unless everyone in front has a white hat, in which case he/she should say "black". Thereafter, everyone ahead can say "pass" (or "white", which will also be correct). If everyone behind the first-in-line has said "pass", that person can correctly say "black".

Note that this strategy guarantees that the team will win.

2. In this version, the n members of the team are assembled in a room where the members can see the color of every hat but their own, and they are interrogated in random order, again with the assurance that not all hats have the same color.

In reality, the team members have more information (as a result of seeing more hats) than in the previous case. If they wish, they can adopt (and adapt) the winning strategy from that case. The first member to be asked "What color is your hat" plays the role of the last-in-line from Case 1; the second to be asked plays the role of the next-to-last- in- line from Case 1; and so on. The winning result is the same.

3. This version is substantially different. Here the n team members are in separate rooms, numbered from 1 to n, with no communication between them. Each is told the colors of the hats of all the others, but not of their own hats; and they do not hear how any other member has answered "What color is your hat?" Also, the n colors have been assigned independently and at random, with each hat being equally likely white or black. In particular, all hats might be the same color, though this would be unlikely for large n.

With three team members, they could agree in advance on the following strategy: If the other two hats have opposite colors, say "pass". If the other two hats have the same color, guess the other color. This strategy will win unless all three hats have the same color, which will happen only one-fourth of the time; so the team will win three-fourths of the time. (Note that when all three hats are the same color, all three team members guess wrong, while in the other cases, there is one correct guess and two "passes". Thus, over the ensemble of all situations, there are equally many correct and incorrect guesses, so the laws of probability are not violated.)

A simple generalization to the case of $n=2^r-1$ team members is as follows. The team members agree in advance on a single-error-correcting $(n,n-r)$Hamming code. Each member's room number becomes one of the *n positions* in the codewords. Each member rewrites the r parity-check equations of the code so that r–1 of the resulting equations do not involve his/her own *position*. Upon learning the colors of the others' hats, these r–1 equations are tested. If at least one *fails*, our team member says "pass". Only if all these other r–1 equations *check*, our team member picks the hat color that makes the r^{th} equation fail. By this strategy, the team will *win*, *unless* the random assignment of hat colors matches a Hamming codeword. When the pattern is not a codeword, the team member who "guesses" is at the error location, while all the others say "pass". When the pattern *is* a codeword, all n team members guess incorrectly. Since single errors are more common than codewords, this strategy succeeds with probability $1-2^{-r}$. (The special case of $n=3$, considered earlier, is the case of $r=2$.)

Between successive values of $n=2^r-1$, where the best strategy, just described, wins with probability $1-2^{-r}$, there may be covering codes which achieve intermediate results. These coding strategies for guessing hat colors are described in considerable detail in [1], which was my source for Case 3. This "hat problem" has actually inspired research leading to the discovery of new "covering codes".

Reference

1. "Why Mathematicians Now Care About Their Hat Color", by Sara Robinson, *The New York Times*, SCIENCE, April 10, 2001, page D5.

Reprinted from Vol. 52, No. 2, June 2002 issue of Information Theory Newsletter

GOLOMB 'S PUZZLE COLUMN™

Some Combinatorial Questions — Solutions

1. Q. "There are 15 balls on a billiard table, bearing the numbers from 1 to 15. Any one of these can be selected to be the first ball to go off the table; but thereafter, each subsequent ball must have a number consecutive (up or down by 1) with that of a ball already off the table. How many possible sequences are there for the order in which all 15 balls go off the table?"

A. There are 2^{14} =16,384 possible sequences. There are several ways to prove this.

Proof #1. Suppose the first ball to go off the table bears the number $k+1$, $0 \le k \le 14$. Of the remaining 14 balls, k are lower-numbered and 14-k are higher-numbered than the first ball. The length-14 sequences of L's (for "lower") and H's (for "higher") with k L's and 14-k H's are in one-to-one correspondence with the order in which the remaining balls can go off the table, since an L indicates that the highest remaining of the lower-numbered balls must go next; and an H indicates that the lowest remaining of the higher-numbered balls must go next. Thus, the total number of permitted sequences is $\sum_{k=0}^{14}\binom{14}{k}=2^{14}$.

Proof #2. Video-tape the game, and when it ends, replay the tape in reverse, where balls reappear on an initially empty table. The first ball to reappear must be numbered either 1 or 15, a binary choice, which leaves 14 consecutively numbered balls off the table. The next ball to reappear must be either the highest or lowest numbered of these 14, again a binary choice. This leaves 13 consecutively numbered balls off the table. The binary choices continue until only one ball is off the table, which reappears (without alternative) to restore the original situation on the table. Thus there are 2^{14} possible sequences.

For additional discussion and other proofs, see "The Fifteen Billiard Balls –A Case Study in Combinatorial Problem Solving", S.W. Golomb, *Mathematics Magazine*, vol. 58, no. 3, May, 1985, 156-159.

2. Q. "If n points are placed independently and at random on the unit circle, what is the probability that they will all lie on a semicircle (i.e. within an arc of length π, starting anywhere on the unit circle)? Generalize to the case of all lying on an arc of length α, $0 \le \alpha \le \pi$. What happens if $\pi < \alpha < 2\pi$?"

A. For $0 \le \alpha \le \pi$, the probability is $n\left(\frac{\alpha}{2\pi}\right)^{n-1}$, so that for the semicircle case, the probability is $\frac{n}{2^{n-1}}$.

Proof. Consider each of the n points as starting an arc of length α as we proceed clockwise around the unit circle. For a given starting point P, each of the remaining random points have the independent probability of $\frac{\alpha}{2\pi}$ of lying on the arc starting at P, for a combined probability of $\left(\frac{\alpha}{2\pi}\right)^{n-1}$; and provided that α does not exceed π, "success" for the arc starting at P_i is disjoint from "success" for the arc starting at P_j, for all $i \ne j$. Thus the disjoint event probabilities add, for a total of $n\left(\frac{\alpha}{2\pi}\right)^{n-1}$.

The case $\pi < \alpha < 2\pi$ no longer guarantees disjoint events for the n starting points, but this situation can be handled by an "inclusion/exclusion" argument. This solution has been discovered independently and published on several occasions. If any reader submits a particularly clever form of the solution, or a good reference, it will appear in a future issue.

3. Q. "Every permutation on n symbols $\{\alpha_1, \alpha_2, \ldots \alpha_n\}$ can be written as a product of disjoint cycles whose cycle lengths sum to n. Let L_n be the expected length of the longest cycle in a random permutation on n symbols, and let $\lim_{n\to\infty}\frac{L_n}{n}=\lambda$. Let $P_n^{(1)}$ be the probability that the first symbol, a_1, is on the longest cycle of a random permutation on n symbols.

a. Prove that the limit λ exists.

b. Express $\lim_{n\to\infty} P_n^{(1)}$ in terms of λ.

A. a. We will show that $\lambda_n = \frac{L_n}{n+1}$ is monotonically increasing as n increases; and since λ_n is clearly bounded from above (by 1), it must have a limit as $n \to \infty$. Since $\frac{L_n}{n}=\left(\frac{n+1}{n}\right)\frac{L_n}{n+1}$ and $\lim_{n\to\infty}\left(\frac{n+1}{n}\right)=1$, $\lim_{n\to\infty}\frac{L_n}{n}=\lambda$.

Reprinted from Vol. 52, No. 2, June 2002 issue of Information Theory Newsletter continued

Proof (that $\frac{L_n}{n+1}$ increases monotonically as n increases).

If we adjoin an $(n+1)^{st}$ element to a random permutation on n symbols, it will have $\frac{L_n}{n+1}$ chances of landing on the "expected longest cycle" of length L_n (by the linearity of *expectation*; but in fact it will do a bit better, because there is sometimes a tie for "longest cycle," and landing on any of these increases the longest cycle by 1. Thus, $L_{n+1} \geq L_n + \frac{L_n}{n+1}$, $(n+1)L_{n+1} \geq (n+2)L_n$, and $\frac{L_{n+1}}{n+2} \geq \frac{L_n}{n+1}$.

b. $\lim\limits_{n\to\infty} P_n^{(1)} = \lambda$, because $\lambda_n = \frac{L_n}{n}$ is the expected fraction of the elements $\{a_1, a_2, \ldots, a_n\}$ which will lie on the longest cycle, and any specific element, such as a a_1, has this probability. Whether $P_n^{(1)} = \lambda_n$ is complicated by the issue of "what happens if two or more cycles are tied for longest?" This issue disappears in the limit: $\lim\limits_{n\to\infty} P_n^{(1)} = \lim\limits_{n\to\infty} \lambda_n = \lambda$.

Note: This is treated in Chapter VII of *Shift Register Sequences* by S.W. Golomb, Holden-Day, Inc., 1967; Second Revised Edition, Aegean Park Press, 1982; and also in "On the number of permutations on n objects with greatest cycle length k ", by S.W. Golomb and P. Gaal, *Advances in Applied Mathematics*, vol. 20, 1998, pp. 98-107. The constant $\lambda = 0.62432965$ was named "Golomb's Constant" by Donald Knuth.

4. Q. "If n black beads and $n + 1$ white beads are placed on a string, and the ends of the string are joined to form a necklace, how many cyclically distinct necklaces can result?"

A. The answer is the Catalan Number $C_n = \frac{1}{n+1}\binom{2n}{n}$.

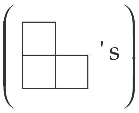
Proof. Clearly there are ways to form strings with the 2n + 1 beads. All 2n + 1 cyclic permutations of the beads are distinct as strings (since there is no common factor >1 of n and 2n + 1 which could allow a periodic substructure) so the number of cyclically distinct necklaces is $\frac{1}{2n+1}\binom{2n+1}{n} = \frac{(2n+1)!}{(2n+1)n!(n+1)!} = \frac{1}{n+1}\binom{2n}{n} = Cn.$

Note. This argument was used by David Singmaster to prove that C_n must be an integer for all $n \geq 0$.

Reprinted from Vol. 52, No. 3, September 2002 issue of Information Theory Newsletter

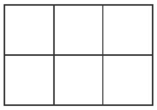
GOLOMB'S PUZZLE COLUMN™

Placing Pentominoes on Boards — Solutions

1. The first task was to find the inequivalent placements of a pentomino on a 5 × 7 board such that the rest of the board can be tiled with ten "right trominoes"  's

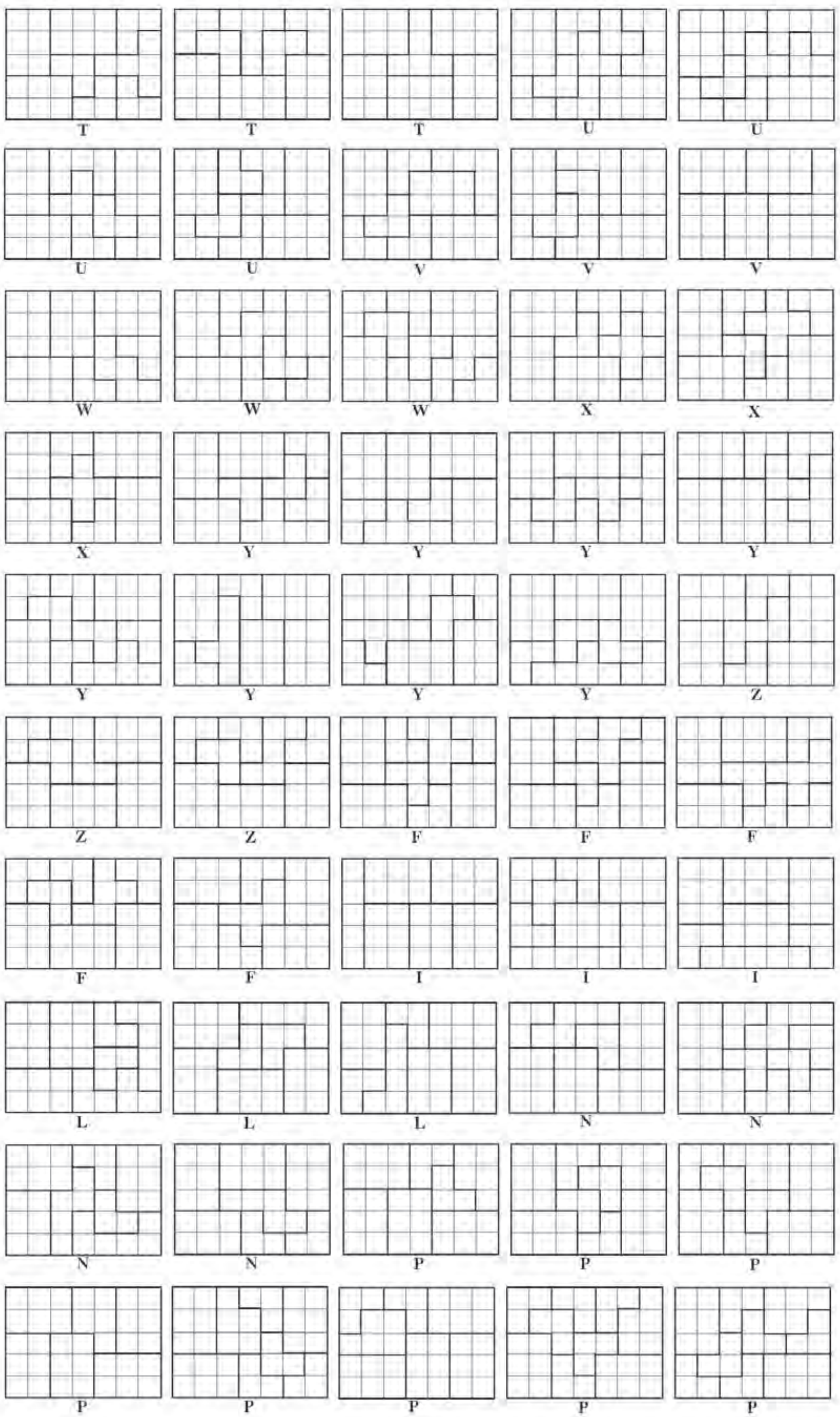
Note that a right tromino covers at most one of the twelve "dotted squares" on the 5 × 7 board. Hence the pentomino must cover at least two of the dotted squares in order for the rest to be tiled by ten right trominoes. (Each pentomino can be placed to cover two of the dotted squares, but only the I and the V are able to cover three.)

○		○		○		○
○		○		○		○
○		○		○		○

The 2×3 rectangle,  , can be tiled in two different ways by two right trominoes, so in the solutions which follow we leave this region undivided.

Here are the 50 solutions I have found. (There may be others that I missed.)

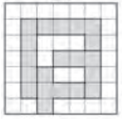
Reprinted from Vol. 52, No. 3, September 2002 issue of Information Theory Newsletter continued



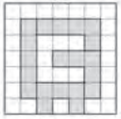
2. The second task was to find four-piece subsets of the 12 pentominoes which can be placed on a 7 × 7 board so as to prevent any of the remaining pentominoes from fitting on the board. In solutions 2.a. through 2.i., we see how to use the I, L, and V pentominoes with each of the other nine, in turn, to achieve this goal. (Most of these examples are not unique for the 4-set involved. There are quite a few configurations which use I, L, V, and U, for examples). Finally, in 2.j., we see a very different kind of solution, using T, U, L, and P, while using neither I nor V. (This example was a joint effort with Scott Kim.) These four pieces can be used in any cyclic order around the edges of the 7 × 7 square to achieve the same result.

Did any reader find an eleventh subset that also works? Or a twelfth? Or a subset that didn't use the L-pentomino?

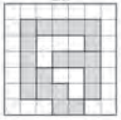
2.a.



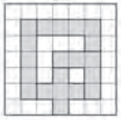
2.b.



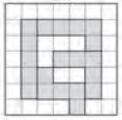
2.c.



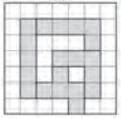
2.d.



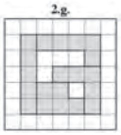
2.e.



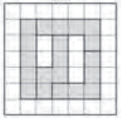
2.f.



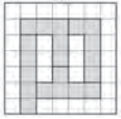
2.g.



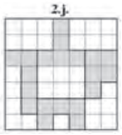
2.h.



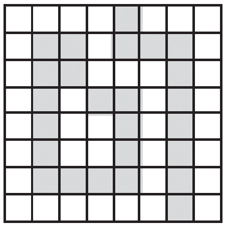
2.i.



2.j.



3. Here is a different set of five pentominoes placed to prevent any of the remaining seven from fitting on the 8 × 8 board.



Reprinted from Vol. 52, No. 4, December 2002 issue of Information Theory Newsletter

GOLOMB'S PUZZLE COLUMN™

On a Problem of Richard Epstein — Solutions

The numbers $n = \{5, 6, 25, 76, 376, 625\}$ have the property that n^2 ends in n, in standard decimal notation. The following questions were asked:

1. Are there other values of $n > 1$ with this property?

2. What is the general procedure for finding additional examples?

3. Is the "complete list" finite or infinite?

Here are short answers:

1. Yes, there are more values of n.

2. For $n > 1$,

a) no examples end in 0 or 1,

b) all examples end in 5 or 6,

c) if n is a t-digit example, $t > 1$, every shortening of n by removing digits from the left end of n is also an example.

3. The "complete list" is infinite, with infinitely many examples ending in 5, and infinitely many ending in 6.

Here are the first eighteen examples, separated into those ending in 5 and those ending in 6.

n	n^2
5	2**5**
25	6**25**
625	390,**625**
90,625	8,212,8**90,625**
890,625	793,212,**890,625**
2,890,625	8,355,71**2,890,625**
12,890,625	166,168,2**12,890,625**
212,890,625	45,322,418,**212,890,625**
8,212,890,625	67,451,572,41**8,212,890,625**

n	n^2
6	3**6**
76	5,**776**
376	141,**376**
9,376	87,90**9,376**
109,376	11,963,**109,376**
7,109,376	50,543,227**7,109,376**
87,109,376	7,588,043,3**87,109,376**
787,109,376	619,541,169 **787,109,376**
1,787,109,376	3,193,759,92**1,787,109,376**

Note three cases (all ending in 5) where an n^2 in the table reappears later as a value of n, namely: 25; 625; and 8,212,890,625. (Is this list finite or infinite?)

The following theorems apply in base $b \geq 2$, where "10" represents b written in base b. The set E_b consists of those integers $n > 1$ for which n^2 "ends in" n, when both n and n^2 are written in base b.

Theorem 1. No member of E_b ends in 0. (That is, no $n > 1$ in E_b is a multiple of b.)

Proof. Suppose n, when written in base b, ends in exactly $t \geq 1$ zeroes. Then n^2 ends in $2t > t$ zeroes, and does not end in n.

Theorem 2. (the Main Theorem). Suppose $n \epsilon E_b$ where n has $t \geq 2$ digits when written in base b. Then every "shortening" of n, by removing digits from the left of n, leaving between 1 and $t - 1$ digits, is again in E_b.

Proof. Suppose $n \epsilon E_b$ and n has $t > 1$ digits in base b notation. This says: $n^2 \equiv n(\text{mod } 10^t)$, or $n^2 - n \equiv 0(\text{mod} 10^t)$. But then also $n^2 - \text{n} \equiv 0(\text{mod } 10^t - 1)$, which says that n', which is n with its left-most digit removed, is also in E_b; and this process can be iterated to obtain the assertion of the Theorem.

Theorem 3. For base $b \geq 2$, no element $n > 1$ of E_b has its "units digit" equal to 1.

Proof. Suppose $n = c \cdot 10^t + 1$, where $0 < c < b$, and $t \geq 1$, is the "base b" representation of n (where $b = 10$ in base b). Then $n^2 - n = (c^2 \cdot 10^{2t} + 2c \cdot 10^t + 1) - (c \cdot 10^t + 1) = c^2 \cdot 10^{2t} + c \cdot 10^t$ (mod 10^t+1), since n has $t + 1$ digits in base b. But since $0 < c < b$, this says $n^2 - n \equiv c \cdot 10^t \not\equiv 0(\text{mod } 10^{t+1})$, so that $n \notin E^b$.

When b =ten, the elements of E_b must end in either 5 or 6, since these are the only "single digit" elements of E_{10}. Members of E_{10} ending in **5** are formed by starting with $n_1 = 5$, and obtaining n_{j+1} from n_j by taking one more digit to the left of n_j in the base-10 representation of n_j^2. (If this next digit is 0, go one additional digit to the left.) This is the method of generating the subsequence { 5, 25, 625, 90625, 890625, 2890625,…} of E_{10}.

The elements of E_{10} ending in **6** are formed in a similar way, starting with $m_1 = 6$, but instead of adjoining the new left-most digit r to m_j from the base-10 representation of m_j^2 to get m_{j+1}, adjoin $10 - r$ instead. This method leads to the subsequence {6, 76, 376, 9376, 109376, 7109376, …} of E_{10}. (If the next digit to the left is 0, we go one additional digit to the left, as with the previous subsequence.)

Each of these subsequences will continue to have new members by the recursive constructions just described.

The remaining three questions concerned E_b for other values of b. Note that the three Theorems above work for every base $b > 1$.

4. "For prime $b \geq 2$, E_b is empty".

Proof: Suppose $1 < n < b$, so that n is a single-digit number in base b, with $n > 1$, and suppose $n^2 \equiv n(\text{mod}b)$. But this says that the prime b divides $n^2 - n = n(n-1)$ where neither n nor n - 1 is a multiple of b, a contradiction. Then, in view of the Main Theorem (Theorem 2), since E_b has no one-digit members, E_b is empty. By Theorems 1 and 3, the units digits 0 and 1 generate no multi-digit examples.)

5. "When $b = 2p$, where $p > 2$ is prime, E_b contains p and $p + 1$."

Proof.

a. $p^2 - p = p(p-1) \equiv 0(\bmod b)$, because $p - 1$ is even and $b = 2p$.

b. $(p+1)^2 - (p+1) = p^2 - p = p(p-1) \equiv 0(\bmod b)$, because p +1 is even and $b = 2p$.

Since the quadratic $x^2 - x \equiv 0(\bmod p)$ has at most two roots in the field $GF(p)$, and x = 0 and $x = 1$ are both roots, it is easy to show that $x^2 - x \equiv 0(\bmod 2p)$ has precisely the four roots $\{0, 1, p, p+1\}$ in the ring of integers modulo $2p$.

6. The complete solution for E_b, where $b = 2p$ and $p > 2$ is prime, precisely parallels the special case $p = 5$, $b = 10$ considered earlier. One infinite subsequence of E_b consists of numbers with units digit p, and the other infinite subsequence of E_b consists of numbers with units digit p + 1. It is even the case that

$$p^2 - p \equiv (2p)\left(\frac{p-1}{2}\right) \equiv 0(\bmod b),$$

$$p^4 - p^2 \equiv (2p)^2\left(\frac{p+1}{2}\right)\left(\frac{p-1}{2}\right) \equiv 0(\bmod b^2)$$

$$p^8 - p^4 \equiv (2p)^4\left(\frac{p^2+1}{2}\right)\left(\frac{p^2-1}{2}\right) \equiv 0(\bmod b^4),$$

so that p, p^2, and p^4 all belong to $E_b = E_{2p}$.

Reprinted from Vol. 53, No. 1, March 2003 issue of Information Theory Newsletter

GOLOMB'S PUZZLE COLUMN™

Early Bird Numbers — Solutions

1. The 45 two-digit *early bird numbers* (e.b. nos.) can be described as follows. Let $n = ab$ (where the standard decimal notation ab stands for $10{\cdot}a+b$). If $0<b<a<9$, then $ba<ab$, and the sequence (∗) of all positive integers in natural order will contain $(ba)(ba+1)$ and will exhibit ab in the overlap. (E.g. if n=53=ab, then we see n in the overlap of $(3\underbrace{5)(3}6)$.) There are $\binom{8}{2}=28$ numbers of this type.

   Next, if $n=ab$ where $b=a+1$, and $0<a<9$, then we see n early in the sequence (∗) where the single-digit number a is followed by $a+1$. (Thus, n=23 occurs in $1\underbrace{23}456\ldots$.) There are 8 such values of n. Finally, the 9 numbers from 91 to 99 appear in the overlaps of $\underbrace{9\text{-}1}0$, $1\underbrace{9\text{-}2}0$, $2\underbrace{9\text{-}3}0$, …, $8\underbrace{9\text{-}9}0$. Altogether, this gives 28+8+9=45 two-digit e.b. nos., exactly half of the numbers from 10 through 99. (None of the others are e.b. nos.)

2. If n is a k-digit positive integer (k>1) such that there is another number n' consisting of a cyclic permutation of the digits of n, with $n'<n$, and the left-most digit of n' being from 1 to 9 inclusive, and the right-most digit of n' is other than 9, then n is an e.b. no. because it appears in the overlap of the consecutive integers n' and $n'+1$. (For example, if n=215, we may take n'=152, and then in (n') $(n'+1)$ we see 152-153 with the original n in the overlap.)

3. If, in the previous problem, there is a cyclic permutation n' of the digits of n, with $n'<n$, but where the right-most digit of n' is 9, the conclusion that n is an e.b. no. is still true, but the proof is more complicated. Here are the typical situations.

   a. If n=291, we take n'=129 and see n in the overlap of n' and $n'+1$: $(1\underbrace{29)(1}30)$, as in the previous solution.

   b. If n=9193, we cannot use n'=1939, since the overlap of n' and $n'+1$, (1939)(1940), does not contain n in its overlap. However, we *can* use n'' = 3919, since now $(n'')(n''+1) = (3\underbrace{919)(3}920)$ has n in its overlap, and we still have $n''<n$.

   c. If n=919, we cannot use n' =199, since $(n')(n'+1)$ = (199)(200) does not have n as an overlap. However, n already appears in the overlap of $(\underbrace{91)(9}2)$.

   d. If n=9199, we cannot use n'=1999; but n already occurs in the overlap of $(\underbrace{919)(9}20)$.

4. a. We already saw that every integer from 91 to 99 inclusive is an e.b. no. in the solution to problem 1.

   b. For the numbers from 901 to 999, problems 2 and 3 show that all are e.b. nos. with the possible exceptions of 909 and 999. (The others have cyclic permutations $n'<n$ with the required characteristics.) But 909 appears in the overlap of (90)(91); and 999 is found in the overlap of (899)(900).

   c. The generalization to all numbers from $9{\cdot}10^d + 1$ to $10^{d+1} - 1$ (inclusive) being e.b. nos. for all is false. As counter-examples, consider n=9090, n=900900, and more generally, $n=0.9(10^{2c}+10^c)$ for all $c \geq 2$. None of these is an e.b. no.

5. The 5-digit number n=11121 is an e.b. number for (at least) the following six overlap representations: a. $(\underbrace{11)(12)(1}3)$, b. $(11\underbrace{1)(112)(1}13)$, c. $(\underbrace{1112)(1}113)$, d. $(12\underbrace{11)(121}2)$, e. $(2\underbrace{111)(21}12)$, f. $(1\underbrace{1112)(1}1113)$.

6. It is true that, asymptotically, 100% of all positive integers are e.b. nos. That is, if $e(x)$ denotes the number of e.b. nos. ≤ x, then $\lim_{x\to\infty} \frac{e(x)}{x} = 1$ (There are infinitely many non-e.b. nos. also, but they become increasingly infrequent.)

   To see this, observe that the "typical" positive integer has a huge number of digits. (Paradoxically, although any specific integer has a finite number of digits, the *expected* number of digits in a "random" integer is infinite!) With so many digits in the typical integer n, it is overwhelmingly likely that there is a cyclic permutation of these digits satisfying the sufficient condition in Problem 2 (or Problem 3) for n to be an e.b. no.

   An open question is to determine how many of the 10^k-10^{k-1} k-digit integers are e.b. nos., for each k. (For k=1 it is 0 for 9, and for k=2 it is 45 out of 90.) It is very likely to be easier to answer this question if we only count those e.b. nos. n that appear in the overlap of *two* consecutive integers less than n.

Reprinted from Vol. 53, No. 2, June 2003 issue of Information Theory Newsletter

GOLOMB'S PUZZLE COLUMN ™

FACTS ABOUT $\binom{2n}{n}$ SOLUTIONS

1. a. $\binom{2n}{n} = \left(\frac{2n}{n}\right)\left(\frac{2n-1}{n-1}\right)\left(\frac{2n-2}{n-2}\right)\cdots\left(\frac{n+2}{2}\right)\left(\frac{n+1}{1}\right) > 2\cdot 2\cdots 2 = 2^n$ if $n > 1$.

$$4^n = (1+1)^{2n} = 1 + \binom{2n}{1} + \cdots + \binom{2n}{2n-1} + 1 > \binom{2n}{n} \text{ if } n > 0.$$

b. From Stirling's Formula, $n! \sim \sqrt{2\pi n}\left(\frac{n}{e}\right)^n$ as $n \to \infty$, we get

$$\binom{2n}{n} = \frac{(2n)!}{(n!)^2} \sim \frac{\sqrt{4\pi n}}{2\pi n}\frac{(2n)^{2n}}{n^{2n}} = \frac{1}{\sqrt{\pi n}}4^n \text{ as } n \to \infty.$$

2. a. $\binom{2n}{n}$ is the number of ways to select a subset of n objects from a set of $2n$ (distinguishable) objects. If we arbitrarily partition the $2n$-set into two n-sets, we can select n objects from the original $2n$-set by selecting k objects from the first n-set and the remaining $n-k$ objects from the second n-set, for each value of k, $0 \le k \le n$. Thus, $\binom{2n}{n} = \sum_{k=0}^{n}\binom{n}{k}\binom{n}{n-k} = \sum_{k=0}^{n}\binom{n}{k}^2$.

b. From $(1-t^2)^m = (1+t)^m(1-t)^m$ we have the binomial expansions $\sum_{k=0}^{m}(-1)^k\binom{m}{k}t^{2k} = \sum_{i=0}^{m}\binom{m}{i}t^i\sum_{j=0}^{m}(-1)^j\binom{m}{j}t^j$. When $m = 2n$, the coefficient of $t^m = t^{2n}$ on the left (at $k = n$) is $(-1)^n\binom{2n}{n}$, while the coefficient of t^{2n} on the right is the convolution

$$\sum_{k=0}^{m}(-1)^k\binom{m}{k}\binom{m}{m-k} = \sum_{k=0}^{m}(-1)^k\binom{m}{k}^2. \text{ Thus, } \binom{2n}{n} = (-1)^n\sum_{k=0}^{2n}(-1)^k\binom{2n}{n}.$$

c. From 2b, $\binom{2n}{n} = (-1)^n\sum_{k=0}^{2n}(-1)^k\binom{2n}{k}^2 = (-1)^n\sum_{k=0}^{2n}\left\{\binom{2n-1}{k-1}+\binom{2n-1}{k}\right\}^2 =$

$$(-1)^n\sum_{k=0}^{2n}(-1)^k\left\{\binom{2n-1}{k-1}^2 + 2\binom{2n-1}{k-1}\binom{2n-1}{k} + \binom{2n-1}{k}^2\right\},$$ since all the "perfect square" terms cancel.

d. We prove $\binom{2n}{n} = \sum_{j=1}^{n}\left(4-\frac{2}{j}\right)$ for $n \ge 1$ by mathematical induction on n. At $n = 1$, this says $2 = \binom{2}{1} = \left(4-\frac{2}{1}\right) = 2$, which is clearly true.

Next, assume the identity is true at $n = k$: $\binom{2k}{k} = \sum_{j=1}^{k}\left(4-\frac{2}{j}\right)$, and consider the case $n = k+1$:

$$\binom{2(k+1)}{k+1} = \frac{(2k+2)!}{(k+1)!(k+1)} = \frac{(2k+2)(2k+1)(2k)!}{(k+1)(k+1)(k!)^2} = \frac{2(2k+1)}{k+1}\binom{2k}{k} = \left(\frac{4k+4}{k+1}-\frac{2}{k+1}\right)\binom{2k}{k}$$

$$= \left(4-\frac{2}{k+1}\right)\sum_{j=1}^{k}\left(4-\frac{2}{j}\right) = \sum_{j=1}^{k+1}\left(4-\frac{2}{j}\right)$$

3. a. $\frac{1}{n+1}\binom{2n}{n} = C_n$, the n^{th} Catalan number, which counts the number of distinct ways to put parentheses in a non-commutative product of $n+1$ factors, so it must be a whole number. For a simpler direct proof, suppose there are n white beads and $n+1$ black beads to be placed on a string. This can be done in $\binom{2n+1}{n}$ ways. If the ends of the string are joined, a necklace results, *Reprinted from Vol. 53, No. 2, June 2003 issue of Information Theory Newsletter continued*

and $2n+1$ strings (the cyclic permutations of each other) form the same necklace (since no two of n, $n+1$, and $2n+1$ have a common prime factor), so $\frac{1}{2n+1}\binom{2n+1}{n}$ must be an integer. But $\frac{1}{2n+1}\binom{2n+1}{n} = \frac{1}{2n+1}\frac{(2n+1)!}{n!(n+1)!} = \frac{(2n)!}{(n+1)(n!)^2} = \frac{1}{n+1}\binom{2n}{n}$.

b. Since every prime p with $n < p \le 2n$ divides the numerator but not the denominator of $\binom{2n}{n} = \frac{(2n)(2n-1)\cdots(n+1)}{n(n-1)(n-2)\cdots 1}$, we have

$\frac{1}{p}\binom{2n}{n}$ is an integer for each such p.

c. If $R = 2\prod p_j$, where p_j runs through all the primes in $(n,2n]$, then $\frac{1}{R}\binom{2n}{n}$ is an integer by 3.b. and the fact that $\binom{2n}{n}$ is even for all $n > 0$. (It's even because $\binom{2n}{n} = \binom{2n-1}{n-1} + \binom{2n-1}{n} = 2\binom{2n-1}{n}$.)

4. a. Let $H_p(n)$ be the highest power of the prime p that divides $n!$ Clearly $H_p(n) = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \cdots$. (We don't need the fact that, exactly, $H_p(n) = \frac{n - w_p(n)}{p-1}$, where $w_p(n)$ is the sum of the digits of n written in base p notation.) Then the highest power of p that divides $\binom{2n}{n} = \frac{(2n)!}{(n!)^2}$ is $H_p(2n) - 2H_p(n) = \sum_{j=1}^{a}\left(\left\lfloor \frac{2n}{p^j} \right\rfloor\right) - 2\left\lfloor \frac{n}{p_j} \right\rfloor \le a$, where a is the largest exponent such that $p^a \le 2n$,

and we used $0 \le \lfloor 2x \rfloor - 2\lfloor x \rfloor \le 1$ for all real $x > 0$.

With $L(n) =$ l.c.m. $\{1,2,3,\ldots,n\}$, it is easily seen that $L(n) = \prod_{p^a \le n} p^a$, where p^a is the highest power of p not exceeding n, from

which $\binom{2n}{n}$ divides $\prod_{p^a \le n} p^a = L(2n)$.

b. A careful count of the exact power of each prime p, $1 < p \le 2n$, which divides $\binom{2n}{n}$, yields $\binom{2n}{n} = \prod_{k=0}^{m}\left\{L\left(\frac{2n}{k}\right)\right\}^{(-1)^k}$.

For details, see "An Identity for $\binom{2n}{n}$", by S. W. Golomb, *American Mathematical Monthly*, vol. 99, no. 8, October, 1992, pp. 746-748.

(Note that with $L(x) = L(\lfloor x \rfloor)$ for all positive real x, we have $L\left(\frac{2n}{k}\right) = 1$ for all $k > n$.)

Call for Nominations

(ordered by deadline date)

IEEE Information Theory Society Claude E. Shannon Award

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

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

IEEE Information Theory Society Aaron D. Wyner Distinguished Service Award

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

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

IEEE Fellow Program

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

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

IEEE Information Theory Society Paper Award

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

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

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

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

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

IEEE Awards

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

Recent Publications

IEEE Transactions on Information Theory

Table of content for volumes 62(12), 63(1), 63(2).

Vol. 62(12): Dec. 2016.

CODING THEORY

SHANNON THEORY

GAUSSIAN NETWORKS

SOURCE CODING

SECURE COMMUNICATION, COMPLEXITY

COMMUNICATION NETWORKS

COMMUNICATIONS

COMPRESSED SENSING, ESTIMATION, LEARNING, GROUP TESTING

SEQUENCES AND BOOLEAN FUNCTIONS

QUANTUM INFORMATION THEORY

Vol. 63(1): Jan. 2017.

PAPERS

SHANNON THEORY

CODING THEORY

COMMUNICATION NETWORKS

GAUSSIAN NETWORKS

COMMUNICATIONS

CRYPTOGRAPHY AND SECURE COMMUNICATION

SOURCE CODING

LEARNING, SPARSE RECOVERY, ESTIMATION, SIGNAL PROCESSING

QUANTUM INFORMATION THEORY

M. Tomamichel, M. M. Wilde, and A. Winter	Strong Converse Rates for Quantum Communication	715
G. De Palma, D. Trevisan, and V. Giovannetti	Gaussian States Minimize the Output Entropy of the One-Mode Quantum Attenuator	728

SEQUENCES AND BOOLEAN FUNCTIONS

C. Lv and J. Li	On the Non-Existence of Certain Classes of Generalized Bent Functions	738

Vol. 63(2): Feb. 2017.

SPARSE RECOVERY, SIGNAL PROCESSING, LEARNING, ESTIMATION

C. Aksoylar, G. K. Atia, and V. Saligrama	Sparse Signal Processing With Linear and Nonlinear Observations: A Unified Shannon-Theoretic Approach	749
J. C. Ye, J. M. Kim, K. H. Jin, and K. Lee	Compressive Sampling Using Annihilating Filter-Based Low-Rank Interpolation	777
K. Lee, Y. Li, M. Junge, and Y. Bresler	Blind Recovery of Sparse Signals From Subsampled Convolution	802
Y. Li, K. Lee, and Y. Bresler	Identifiability in Bilinear Inverse Problems With Applications to Subspace or Sparsity-Constrained Blind Gain and Phase Calibration	822
S. Chrétien and T. Wei	Sensing Tensors With Gaussian Filters	843
J. Sun, Q. Qu, and J. Wright	Complete Dictionary Recovery Over the Sphere I: Overview and the Geometric Picture	853
J. Sun, Q. Qu, and J. Wright	Complete Dictionary Recovery Over the Sphere II: Recovery by Riemannian Trust-Region Method	885
W. Han, P. Rajan, P. I. Frazier, and B. M. Jedynak	Bayesian Group Testing Under Sum Observations: A Parallelizable Two-Approximation for Entropy Loss	915
N. B. Shah, S. Balakrishnan, A. Guntuboyina, and M. J. Wainwright	Stochastically Transitive Models for Pairwise Comparisons: Statistical and Computational Issues	934

SHANNON THEORY

R. Xu, J. Chen, T. Weissman, and J.-K. Zhang	When is Noisy State Information at the Encoder as Useless as No Information or as Good as Noise-Free State?	960
M. Hayashi and V. Y. F. Tan	Equivocations, Exponents, and Second-Order Coding Rates Under Various Rényi Information Measures	975
S. Watanabe	Second-Order Region for Gray–Wyner Network	1006
W. Huleihel and N. Merhav	Random Coding Error Exponents for the Two-User Interference Channel	1019
K. Nakagawa, K. Watabe, and T. Sabu	On the Search Algorithm for the Output Distribution That Achieves the Channel Capacity	1043
R. Nasser	An Ergodic Theory of Binary Operations—Part II: Applications to Polarization	1063

CODING THEORY

Z. Wang, I. Tamo, and J. Bruck	Optimal Rebuilding of Multiple Erasures in MDS Codes	1084
Y. Wu	Generalized Integrated Interleaved Codes	1102
S. Engelberg and O. Keren	Reliable Communications Across Parallel Asynchronous Channels With Arbitrary Skews	1120
Q. Li and A. Jiang	Coding for Secure Write-Efficient Memories	1130

COMMUNICATION NETWORKS

U. Niesen and M. A. Maddah-Ali	Coded Caching With Nonuniform Demands	1146
M. Kiwi and C. Thraves Caro	FIFO Queues Are Bad for Rumor Spreading	1159

GAUSSIAN NETWORKS

X. Jin and Y.-H. Kim	The Approximate Capacity of the MIMO Relay Channel	1167
N. Ross and D. Schuhmacher	Wireless Network Signals With Moderately Correlated Shadowing Still Appear Poisson	1177
M. Wigger, R. Timo, and S. Shamai	Conferencing in Wyner's Asymmetric Interference Network: Effect of Number of Rounds	1199
E. Köken, D. Gündüz, and E. Tuncel	Energy-Distortion Exponents in Lossy Transmission of Gaussian Sources Over Gaussian Channels	1227

SOURCE CODING

O. Sabag, H. H. Permuter, and A. Cohen	Lossless Coding of Correlated Sources With Actions	1237
O. Ordentlich and U. Erez	Integer-Forcing Source Coding	1253

QUANTUM INFORMATION THEORY

R. Iten, J. M. Renes, and D. Sutter	Pretty Good Measures in Quantum Information Theory	1270
E. Wakakuwa, A. Soeda, and M. Murao	Markovianizing Cost of Tripartite Quantum States	1280
N. Yu, R. Duan, and Q. Xu	Bounds on the Distance Between a Unital Quantum Channel and the Convex Hull of Unitary Channels	1299

SECURE COMMUNICATION

T. C. Gulcu and A. Barg	Achieving Secrecy Capacity of the Wiretap Channel and Broadcast Channel With a Confidential Component	1311

SEQUENCES

M. Li and D. Lin	The Adjacency Graphs of LFSRs With Primitive-Like Characteristic Polynomials	1325
A. G. Castoldi, L. Moura, D. Panario, and B. Stevens	Ordered Orthogonal Array Construction Using LFSR Sequences	1336

Problems of Information Transmission Volume 52, Issue 4 (October 2016)

On some extremal problems for mutual information and entropy
V. V. Prelov
Pages 319–328

List decoding for a multiple access hyperchannel
V. Yu. Shchukin
Pages 329–343

On risk concentration for convex combinations of linear estimators
G. K. Golubev
Pages 344–358

Derivation of fast algorithms via binary filtering of signals
M. S. Bespalov, A. S. Golubev, A. S. Pochenchuk
Pages 359–372

On chromatic numbers of closetoKneser distance graphs
A. V. Bobu, A. E. Kupriyanov
Pages 373–390

A triangular class of skew maximumperiod polynomials
S. N. Zaitsev
Pages 391–399

JOHNS HOPKINS
WHITING SCHOOL
of ENGINEERING

CISS 2017: Deadline extended to 12/26/2016
Some notifications may not be received by Jan 15, but final manuscripts remain due Jan 31, 2017.

51st Annual Conference on Information Sciences and Systems

March 22 – 24, 2017

Hosted by the
Department of Electrical and Computer Engineering, Johns Hopkins University
and a Technical Co-Sponsorship with
IEEE Information Theory Society

ciss.jhu.edu

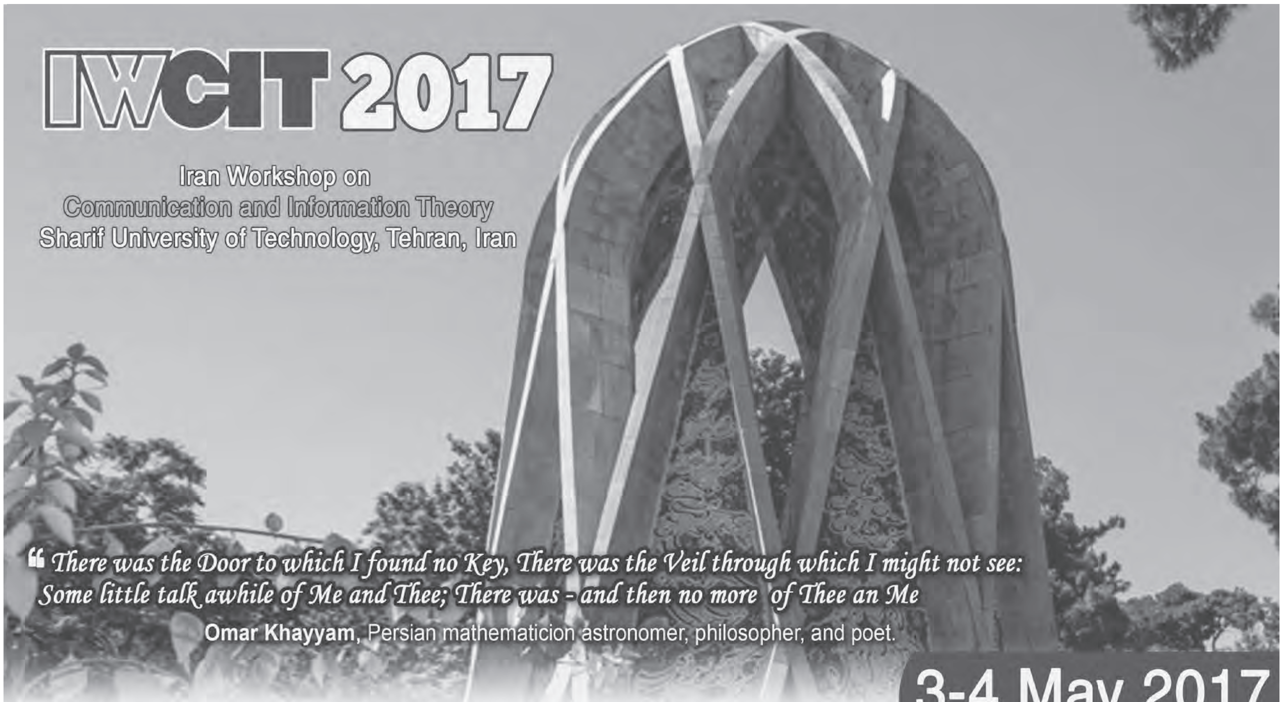
Authors are invited to submit previously unpublished papers describing theoretical advances, applications, and ideas in the fields of Information Sciences and Systems including:

- Information Theory
- Communication
- Networked Systems
- Signal Processing
- Image Processing
- Coding
- Systems and Control
- Biological Systems and Control
- Photonic and Quantum Systems
- Machine Learning
- Security and Privacy
- Inference
- Sensory Systems
- Neuroscience

Papers will require approximately 18 minutes for presentation and will be reproduced in full (up to six pages) in the conference proceedings.

Submissions of sufficient detail and length to permit careful reviewing must be submitted online, at ciss.jhu.edu only, by **December 26, 2016**. Authors will be notified of acceptance no later than **January 15, 2017**. Final manuscripts of accepted papers are to be submitted in PDF format no later than **January 31, 2017**. **These are firm deadlines that are necessary to ensure the timely availability of the conference program.** IEEE reserves the right to exclude a paper from distribution after the conference, including removal from IEEE Xplore®, if the paper is not presented by an author at the conference.

Conference Coordinator	Program Directors	Important Dates
Eileen Miller 410-516-7031 Department of Electrical and Computer Engineering Johns Hopkins University Baltimore, MD 21218 ciss@jhu.edu	Prof. Mark A Foster Prof. A. Brinton Cooper Department of Electrical and Computer Engineering Johns Hopkins University Baltimore, MD 21218	**Submission deadline:** ~~**December 11, 2016**~~ **Dec 26, 2016, 2200 GMT** **Notification of acceptance:** January 15, 2017 **Final manuscript due:** January 31, 2017



IWCIT 2017

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

> “ *There was the Door to which I found no Key, There was the Veil through which I might not see:*
> *Some little talk awhile of Me and Thee; There was - and then no more of Thee an Me*
>
> **Omar Khayyam,** Persian mathematicion astronomer, philosopher, and poet.

3-4 May 2017

Call for Papers

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

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

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

Coding Theory
- Compressed sensing
- Data compression
- Network coding

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

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

General Chairs:
- Aref, M. R.
Sharif University of Technology
- Salehi, J. A.
Sharif University of Technology

Technical Program Chair:
- Sharafat, A. R.
Tarbiat Modares University

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

IEEE
IRAN SECTION

Contact Us :

• Emails:
iwcit@sharif.ir

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

WWW . IWCIT . COM

15th Canadian Workshop on Information Theory

CWIT 2017 | Quebec City, Quebec, Canada | June 11–14, 2017

Photo credit: Martin St-Amant

Organizing Committee

General Co-Chairs
Jean-Yves Chouinard
Paul Fortier

Technical Program Co-Chairs
Benoit Champagne
Hugues Mercier
Xianbin Wang

Treasurer
Julian Cheng

Publication Chair
ÉricPlourde

Sponsorship and Industry Liaison Chair
Yongyi Mao

Webmaster
Andrew W. Eckford

CALL FOR PAPERS

The 15th Canadian Workshop on Information Theory will take place in Quebec City, Quebec, Canada, June 11 to 14, 2017. Previously unpublished contributions from a broad range of topics in information theory and its applications are solicited, including (but not limited to) the following areas:

- Coded modulation
- Coding theory and practice
- Cognitive radio
- Communication complexity
- Communication systems
- Cooperative communication
- Cryptology and data security
- Data compression
- Detection and estimation
- Information theory and statistics
- Information theory in biology
- Interactive information theory
- Multi-terminal information theory
- Network coding
- Pattern recognition and learning
- Quantum information processing
- Shannon theory
- Signal processing

Manuscripts (both review and final versions) must be submitted through EDAS (http://edas.info) in standard IEEE two-column format. Manuscripts can be up to 5 pages in length. Accepted papers will be presented at the workshop by the authors, and at least one author of each accepted paper is expected to attend the workshop.Conference content will be submitted for inclusion into IEEE Xplore.

IMPORTANT DATES

• Review manuscript due	**February 3, 2017**
• Paper acceptance notification	**March 31, 2017**
• Final papers due	**April 14, 2017**

CONTACT

Website: http://cwit.ca/2017/

Enquiries: Jean-Yves Chouinard
Email: jean-yves.chouinard@gel.ulaval.ca

Paul Fortier
Email: paul.fortier@gel.ulaval.ca

2017 IEEE International Symposium on Information Theory
Aachen, Germany | June 25-30, 2017

©Peter Winandy

Call for Papers

The *2017 IEEE International Symposium on Information Theory* will take place in the historic city of Aachen, Germany, from June 25 to 30, 2017.

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

Topics

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

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

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

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

We look forward to your participation in ISIT 2017.

General Co-Chairs
Rudolf Mathar
Gerhard Kramer

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

Finance
Meik Dörpinghaus
Volker Schanz

Publications
Giuseppe Durisi
Christoph Studer

www.isit2017.org

5th International Castle Meeting on Coding Theory and Applications

PRELIMINARY CALL FOR PAPERS

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

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

Organization:

General chair: *Vitaly Skachek*

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

Publicity: *Yauhen Yakimenka*

Scientific Committee

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

Important dates:

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

Call-for-Papers

IEEE Transactions on Information Theory

Special Issue on

Shift-Register Sequences, Codes and Cryptography in Memory of Solomon W. Golomb

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

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

The topics of interest include but are not limited to:

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

Important Dates:
Manuscript submission: May 31, 2017
Completion of first round of reviews: September 30, 2017
Revised manuscript submission: October 31, 2017
Notification of final decision: November 30, 2017
Final manuscript submission: December 31, 2017

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

Guest Editors
Guang Gong, University of Waterloo, Canada
Tor Helleseth, University of Bergen, Norway
Vijay Kumar, Indian Institute of Science, India

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

Conference Calendar

DATE	CONFERENCE	LOCATION	WEB PAGE	DUE DATE
March 19–22, 2017	**IEEE Wireless Communications and Networking Conference (WCNC).**	San Francisco, CA	http://wcnc2017.ieee-wcnc.org/	Passed
March 22–24, 2017	**Conference on Information Sciences and Systems (CISS).**	Baltimore, Maryland	http://ciss.jhu.edu/	Passed
May 3–4, 2017	**5th Iran Workshop on Communication and Information Theory (IWCIT).**	Sharif University of Technology, Tehran, Iran	http://iwcit.com/	Passed
May 8–11, 2017	**European School of Information Theory (ESIT).**	Madrid, Spain	http://www.itsoc.org/conferences/schools/european-school-2017	—
May 15–19, 2017	**15th International Symposium on Modeling and Optimization in Mobile, Ad-Hoc, and Wireless Networks (WiOpt).**	Telecom ParisTech, Paris, France	http://wiopt.telecom-paristech.fr/	Passed
June 11–14, 2017	**15th Canadian Workshop on Information Theory.**	Quebec City, Quebec, Canada	http://cwit.ca/2017/	Passed
June 25–30, 2017	**IEEE International Symposium on Information Theory (ISIT).**	Aachen, Germany	http://www.isit2017.org	Passed
July 3–6, 2017	**The 18th IEEE International Workshop on Signal Processing Advances in Wireless Communications.**	Sapporo, Japan	http://www.spawc2017.org/public.asp?page=home. html	March 1, 2017
August 28–31, 2017	**Fifth International Castle Meeting on Coding Theory and Applications (5ICMCTA).**	Vihula Manor, Estonia	http://www.castle-meeting-2017.ut.ee/	May 1, 2017

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