

President's Column

Alon Orlitsky

ISIT in Barcelona was true joy. Like a Gaudi masterpiece, it was artfully planned and flawlessly executed. Five captivating plenaries covered the gamut from communication and coding to graphs and satisfiability, while Alexander Holevo's Shannon Lecture reviewed the fascinating development of quantum channels from his early theoretical contributions to today's near-practical innovations. The remaining 620 talks were presented in 9 parallel sessions and, extrapolating from those I attended, were all superb. Two records were broken, with 888 participants this was the largest ISIT outside the US, and at 540 Euro registration, the most economical in a decade.



sion for our community along with extensive experience as board member, associate editor, and a first-class researcher. Be-earled congratulations, Madam President.

Other decisions and announcements concerned the society's major awards, including three Jack Wolf student paper awards and the James Massey Young Scholars Award that went to Andrea Montanari. Surprisingly, the IT Paper Award was given to two papers, "The Capacity Region of the Two-Receiver Gaussian Vector Broadcast Channel With Private and Common Messages" by Yanlin Geng and Chandra Nair, and "Fundamental Limits of Caching" by Mohammad Maddah-Ali and

Apropos records, and with the recent Rio Games, isn't ISIT like the Olympics, except even better? As with the ultimate sports event, we convene to show our best results, further our reach, and meet old friends. But beyond the Summer Games, we don't just compete – we collaborate, we don't merely celebrate – we cerebrate, and instead of quadrennially – we see our friends and colleagues yearly. I would therefore like to congratulate and thank the IT Olympics general chairs, Albert Guillen y Fabregas, Alfonso Martinez, and Sergio Verdu, and technical chairs, Venkat Anantharam, Ioannis Kontoyiannis, Yossef Steinberg, and Pascal Vontobel, for an excellent event. And if you concur, please let them know too.

As Barcelona ends, we pass the torch to Aachen 2017, and Vail and Paris in 2018 and 2019. At our annual Board of Governors meeting in Barcelona we added two more ISIT Olympic Cities: Los Angeles 2020 and Melbourne 2021. In fact, to permanently cement the pecking order, ISITs are now scheduled further into the future than the Summer Olympics!

Another important sequence, the presidential succession line, was augmented by Emina Sojanin, our next Second VP, succeeding Elza Erkip and Ruediger Urbanke. Emina embodies a unique fusion of passion for our profession and compas-

Urs Niesen. While Paper Awards were given to two related papers recently, not since 1972 were papers on different topics jointly awarded. But the board found both papers excellent yet so different in topic and focus that choosing between them would have been arbitrary.

Two career awards were also given. The Aaron D. Wyner Distinguished Service Award went to Frank Kschischang. Frank has performed essentially all our major service tasks, including associate editor (3 years), editor in chief (3), ISIT general and technical chair (1+1), board of governors (3), and president (5). A grand total of 16 years at the society's service. Frank once told me that his parents immigrated to Canada so they could do four times less work for the same pay. Thankfully, when it came to our society, Frank espoused the opposite philosophy: infinitely more work, for no pay.

Finally and importantly, the 2017 Shannon Award, our society's most prestigious distinction, went to David Tse. Like the award's eponym, David distills practical challenges into elegant mathematical problems that he solves to obtain important fundamental insights on the original problem. Applying

continued on page 35

From the Editor

Michael Langberg



Dear colleagues,

As fall settles in, we are glad to present the September issue of our society newsletter. The issue opens by joining our Society President Alon Orlitsky in congratulating our fellow colleagues for their outstanding research accomplishments and service recognized by our community. We are then delighted to include an article by Richard Brown, the NSF Program Director in the Communication and Information Foundations (CIF) cluster in the Division of Computing and Communication Foundations (CCF), which outlines NSF's continued commitment to fundamental research through several concrete programs of interest to the society. Following the efforts in our community to reach out and influence societies beyond on own, we are glad to have an intriguing article by Eimear Byrne "Subspaces, Matrices and Codes" which outlines recent results and open problems in the context of subspace and rank-metric codes alongside explicit connections to

index-coding and coded-caching. Many thanks to the contributors for their efforts!

The issue continues with a number of our regular columns including Tony Ephremides's Historian's column; our "Students' Corner" column presenting two student articles, by Onur Günlü and Jennifer Tang (compiled by Parham Noorzad), summarizing their experiences at recent Shannon Centenary events; the column "From the field" highlighting the recent activities of the recipient of this year's Chapter of the Year Award, the Benelux Chapter on Information Theory; the IEEE Information Theory Society Board of Governors meeting minutes from their meeting in ITA (La Jolla California) in January; and reports from the Munich Workshop on Causal Inference and Information Theory (MCI 2016), the Bertinoro Workshop on Communications and Coding (BCC 2016), two major events in South Africa (the IEEE Seminar on Future Directions in Information Theory and Communications and the 2nd African Winter School on Information Theory and Communications), the International Conference on Information Geometry and its Applications IV, the 2016 European School of Information Theory, and the 2016 International Zurich Seminar on Communications.

The festivity of the Shannon Centenary has been felt throughout our community over the past months. This issue includes a collection of reports from several of the workshops, exhibits, and celebrations that took place world-wide. The collection includes reports from: Bell Labs, New Jersey; MIT; Paderborn, Germany; Hefei, China; IIT Madras, Information Theory Society Madras Chapter; Monash University; Chinese University and City University of

continued on page 16

IEEE Information Theory Society Newsletter

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

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

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

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

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

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

Table of Contents

President's Column	1
From the Editor	2
Awards	3
Guest Column: News from the National Science Foundation	4
Subspaces, Matrices and Codes	5
The Historian's Column	13
Students' Corner	14
From the Field: 2016 Chapter of the Year Award for the Benelux IT Chapter	15
Report on the Munich Workshop on Causal Inference and Information Theory (MCI 2016)	17
Report on the Bertinoro Workshop on Communications and Coding (BCC 2016)	17
Report on Two Major Events on Information Theory in South Africa	18
Report on International Conference on Information Geometry and its Applications IV	18
Report on 2016 European School of Information Theory	19
The 2016 International Zurich Seminar on Communications	20
Shannon Centenary Workshop and Celebration Reports	21
A Numerical Tribute to Claude Shannon for his Centennial Birthday	30
IEEE Information Theory Society Board of Governors Meeting	31
Golomb's Puzzle Column™: Latin Squares Solutions	36
In Memoriam: Professor Rudolf Emil Kalman	37
In Memoriam: Solomon W. Golomb	38
Golomb's Puzzle Column™, Part 1	41
Call for Papers	51
Conference Calendar	56

Awards

Congratulations to the members of our community that have recently received recognition for their exceptional scholarly contributions.

David Tse: 2017 Claude E. Shannon Award

The Claude E. Shannon Award is the highest honor from the IEEE Information Theory Society. The award has been instituted to honor consistent and profound contributions to the field of information theory.

Frank R. Kschischang: 2016 Aaron D. Wyner Distinguished Service Award

The Aaron D. Wyner Distinguished Service Award of the IT Society has been instituted to honor an individual who has shown outstanding leadership in, and provided long-standing, exceptional service to, the Information Theory community.

Information Theory Society Paper Award

The purpose of the Information Theory Paper Award is to recognize exceptional publications in the field and to stimulate interest in and encourage contributions to fields of interest of the Society. The 2016 award winning publications are:

- **Yanlin Geng and Chandra M. Nair**, "The Capacity Region of the Two-Receiver Gaussian Vector Broadcast Channel With Private and Common Messages", *IEEE Transactions on Information Theory*, Apr., 2014.
- **Mohammad Ali Maddah-Ali and Urs Niesen**, "Fundamental Limits of Caching", *IEEE Transactions on Information Theory*, May, 2014.

Joint Communications Society/Information Theory Society Paper Award

The Joint Communications Society/Information Theory Society Paper Award recognizes outstanding papers that lie at the intersection of communications and information theory.

The 2016 award winning publication is:

- **Angel Lozano, Robert W. Heath Jr., and Jeffrey G. Andrews**, "Fundamental Limits of Cooperation", *IEEE Transactions on Information Theory*, Mar., 2013.

Andrea Montanari: 2016 James L. Massey Research & Teaching Award for Young Scholars

The 2016 James L. Massey Research & Teaching Award for Young Scholars recognizes outstanding achievement in research and teaching by young scholars in the Information Theory community.

Kartik Venkat: 2016 Thomas M. Cover Dissertation Award

The IEEE Information Theory Society Thomas M. Cover Dissertation Award, established in 2013, is awarded annually to the author of an outstanding doctoral dissertation contributing to the mathematical foundations of any of the information sciences within the purview of the Society.

- **Kartik Venkat**, "Relations Between Information and Estimation: A Unified View", Ph.D. Thesis, Stanford University, Stanford, CA, USA, Dec. 2015.

Jack Keil Wolf ISIT Student Paper Award

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. The award is based on the paper's technical contribution as well as the quality of its presentation. The prize was awarded to 3 papers this year:

- **David Sutter, Marco Tomamichel, and Aram W. Harrow**, Strengthened Monotonicity of Relative Entropy via Pinched Petz Recovery Map.
- **Hua Sun and Syed A. Jafar**, Blind Interference Alignment for Private Information Retrieval.
- **Cheuk Ting Li and Abbas El Gamal**, Distributed Simulation of Continuous Random Variables.

2016 Chapter of the Year Award

The Chapter of the Year Award recognizes a chapter that has provided their membership with the best overall set of programs and activities. The 2016 winner is the

- **Benelux Chapter on Information Theory: Frans M.J. Willems** (Chair), **Peter H.N. de With** (Vice-Chair), **Vincent Rijmen** (Treasurer), **Jos Weber** (Secretary), **Jasper Goseling**.

Helmut Bölcskei: 2016 Padovani Lecturer

The Padovani Lecture is held annually at the North-American School of Information Theory.

Guest Column: News from the National Science Foundation

D. Richard Brown III, Program Director, Division of Computing and Communication Foundations

Greetings from the National Science Foundation!

Let me begin by thanking Alon Orlitsky for the invitation to submit an article to the IEEE ITS newsletter. I have read this newsletter for quite a few years and have saved many of Solomon Golomb's puzzles for use in qualification exams. I've always enjoyed the concise and relatively informal format of this newsletter and I appreciate the opportunity to reach out to the members of the IEEE ITS through this channel.

By way of introduction, I joined NSF in January as a Program Director in the Communication and Information Foundations (CIF) cluster in the Division of Computing and Communication Foundations (CCF), which is one of four divisions in the Computer and Information Sciences and Engineering (CISE) Directorate. Many, perhaps all, of you know my predecessor Phil Regalia. Phil finished his four years of service at the NSF shortly after I arrived. While there are big shoes to fill, I have been doing my best to quickly come up to speed and take over Phil's responsibilities in CIF and other related programs. I'm grateful for the unique opportunity to serve the community in this role, especially during the Shannon Centenary, and am looking forward to meeting and working with many of you during my time at NSF.

As many of you know, NSF has a very broad research portfolio, from biology to polar programs to astronomical sciences to, of course, information science and engineering. NSF has long supported fundamental research on a variety of topics of interest to the information theory community primarily through CISE/CCF/CIF. It is probably no coincidence that the missions of the IEEE ITS and the CIF cluster are closely aligned. The ITS states its purpose is to "connect people interested in processing, transmission, storage, and use of information, as well as theoretical and applied aspects of coding, communications, and communications networks". The CCF Core Solicitation¹ describes research relevant to the CIF cluster as addressing "information acquisition, transmission, and processing in communications and information processing systems". Through CISE/CCF/CIF, NSF has made (and continues to make) significant investments in fundamental research in information theory, communication systems, networking, and signal processing. And, in light of our increasingly connected world, the importance of continued investment in these areas is only escalating. As one example of NSF's continued commitment to fundamental research in areas of interest to many members of the IEEE ITS, you may have seen the recent announcement from NSF regarding investments of more than \$400 million over the next seven years in support of the White House's Advanced Wireless Research Initiative.² The NSF Director, Dr. France Córdova also recently presented "ten big ideas" for NSF,³ which includes a strong commitment to fundamental research in data sciences through the "Harnessing Data for 21st Century Science and Engineering" initiative.

Many members of the IEEE ITS are also members of other IEEE societies and conduct research in domains outside of pure information theory and coding theory including communications, networking, security, and signal processing. These research topics may overlap with other divisions and programs at NSF. For example:

- The Computer and Network Systems⁴ (CNS) division and specifically the Networking and Technology Systems (NeTS) cluster in CISE funds basic research on wired and wireless networking.
- The Division of Electrical, Communications and Cyber Systems⁵ (ECCS) and specifically the Communications, Circuits, and Sensing-Systems (CCSS) cluster in the Engineering (ENG) Directorate funds research that leverages "computation, communication, and algorithms integrated with physical domains".
- The cross-directorate Secure and Trustworthy Cyberspace⁶ (SaTC) led by CISE funds research in various areas of security and privacy.

I am happy to try to answer any questions you might have regarding which program is the best fit for a particular proposal. I can also put you in touch with other program officers that can help you find the best fit for your work. While it is always in your best interest to submit proposals to the program that best fits your research, NSF Program Directors also interact regularly to discuss proposals of mutual interest, form joint panels, suggest expert reviewers, and transfer proposals between programs as appropriate.

A special NSF program that I'd like to mention is the Research Experience for Undergraduates (REU) program.⁷ The REU program supports the training of the next generation of information scientists and engineers by providing support to engage undergraduate students in fundamental research. In particular, REU Sites and Supplements provide support for these experiences. If you have an active NSF grant and would like to involve undergraduate students in your research, you can apply for an "REU Supplement" to support the undergraduate students involved in this activity. As I've discovered by mentioning this to reviewers and Principle Investigators, not everyone in our community is aware of this opportunity. In CISE, we generally look for short proposals for REU Supplements (3–5 pages, typically) to be submitted between January 1 and March 30. While the deadline for 2016 submissions has passed, I expect the guidelines for 2017 will be similar to those in 2016.⁸ Many of you are already taking advantage of this opportunity, but if you aren't, I encourage⁹ you to consider how you might be able to involve undergraduate students in your research.

I could go on about other programs of potential interest including programs to establish international collaborations such as our programs with the United States – Israel Binational Science Foundation (BSF) and the Academy of Finland, but I will leave that as a homework assignment to the reader. Instead, I'd like to conclude with a "thank you" and a "call to service". Thank you to all of the reviewers who have served on NSF panels over the years and especially to those who served (or provided ad hoc reviews) on CIF panels earlier this year. I realize carefully reviewing 8–10 proposals requires a significant commitment of time and energy, and I appreciate all of the effort reviewers put into the NSF merit review process. If you haven't served on a panel in a while (or ever), please take this as a "call to service". Please consider serving your community by volunteering (email me directly at ribrown@nsf.gov) and by agreeing to participate in a panel when invited. There are many rewards

for serving on a panel including closely interacting with other active researchers in the community, staying abreast of trends in the field, and having a chance to learn about new developments at NSF. Your participation is critical. I sincerely appreciate your willingness and flexibility in serving as a reviewer and in serving an important role in helping NSF achieve its mission to further the progress of science and educate the next generation of scientists and engineers.

- 1) https://www.nsf.gov/funding/pgm_summ.jsp?pims_id=503220
- 2) http://www.nsf.gov/news/news_summ.jsp?cntn_id=139179
- 3) https://www.nsf.gov/about/congress/reports/nsf_big_ideas.pdf

- 4) <http://www.nsf.gov/cise/cns/about.jsp>
- 5) <http://www.nsf.gov/eng/eccs/about.jsp>
- 6) https://www.nsf.gov/funding/pgm_summ.jsp?pims_id=504709
- 7) http://www.nsf.gov/funding/pgm_summ.jsp?pims_id=5517&from=fund
- 8) <http://www.nsf.gov/pubs/2016/nsf16018/nsf16018.jsp>
- 9) <http://cra.org/crn/2016/05/quality-research-experiences-anchor-future-cise-undergraduate-education/>

Subspaces, Matrices and Codes

Eimear Byrne

I. Introduction

The landscape of algebraic coding theory has undergone major changes in the last fifteen years. Network coding in particular has had a major impact on associated areas of discrete mathematics, giving rise to new research topics and reviving old ones.

This has been particularly apparent in the field of network error correction, after the seminal papers of [43], [61]. In the first of these, the authors offered a solution to multicast communication across noisy networks, using *random network coding*. In this model, at an intermediate node, random linear combinations of the incoming packets are output before continuing through the network. A set of some n transmitted packets can then only be distinguished from another up to taking linear combinations. For this reason, they proposed using *subspace codes*, which are codes whose codewords are row spaces of sets of matrices with n rows. In order to facilitate error correction, a distance function was identified, namely the subspace metric.

Aside from the practical applications to network communications, other aspects of the theory of subspace codes were met with great enthusiasm. Researchers with expertise in classical coding theory immediately set about tackling the question of optimality of subspace codes, finding upper bounds on the size and constructions of good codes [13], [25], [28], [29], [37], [40], [59], [63]. Work on code optimality led to a significant revival of interest in q -analogues of various combinatorial objects such as designs over finite fields. Since the original papers of Thomas [64], [65], there had been little written on the subject until very recently [6], [10], [11], [32], [41], [44], [46].

Central to the topic of subspace codes is that of *rank metric codes*, which are matrix codes, equipped with the *rank distance* function. Rank-metric codes provide constructions of some of the best subspace codes. Optimal matrix codes [18], [33] have been known for some decades. Delsarte-Gabidulin codes (also known as Gabidulin or generalized Gabidulin codes) became a subject of intense study especially after the connection to network error correction was made. They had already been considered for coding-based cryptographic schemes [12] and there are many papers on decoding algorithms for such codes [7], [14], [33], [38], [47], [71]. This made them ideal for constructions of subspace codes, since in addition to

yielding near-optimal codes, they brought with them ready-made decoding. Since then there have been numerous papers on the subject and more generally on the topic of *maximum rank distance* (MRD) codes, which are the rank-metric analogue of MDS codes.

As MRD codes exist in the form of Delsarte-Gabidulin codes for all parameters without restriction on the field size, it has only been very recently that any efforts were made to obtain infinite families outside of the class of Delsarte-Gabidulin codes [57]. The structure of MRD codes has generated a lot of interest as a topic in its own right [19], [20], [42], [51], [54], [56].

The relevance of rank-metric codes to network coding problems has not been confined to error correction in random network coding. They also arise in applications of linear coding to problems of *broadcast with side-information*. This is implicit in the literature for broadcast problems with coded-side information, although not commonly remarked upon explicitly. Such problems include index coding and coded-caching. The importance of index coding in network coding was established in [26], [31], where equivalences between the two problems were shown. Coded-caching in particular is currently a very active area of research after the work [52]. These broadcast problems involve efficient delivery of big data files to many users, each of whom already has some data stored locally in its cache via some form of placement, either randomly or by design. There is an extensive literature on the subject: [2], [3], [4], [5], [8], [9], [15], [52], [22], [23], [58], [68], [70]. In the case of linear coding, the structure of the cached data or side information can be expressed as a rank-metric code. The fundamental limits of transmission in these problems then relate to covering properties of matrix codes of this type.

In this letter we will give a brief survey of recent results on subspace codes and rank-metric codes which have evolved since random network coding for error correction became known to the community working in algebraic coding theory. Furthermore, we will make an explicit connection of rank-metric codes to broadcast with side-information problems. We will outline some achievements and identify open problems.

Throughout, we will let \mathbb{F}_q denote a finite field of q elements, for some prime power q . We write $\mathbb{F}_q^{n \times m}$ to denote the set of $n \times m$ matrices with entries in \mathbb{F}_q . In most of what follows we will assume that all matrices and vectors have coefficients in \mathbb{F}_q .

II. Subspace and Matrix Codes

A matrix code C is a set of $n \times m$ matrices with entries in \mathbb{F}_q and is referred to as a rank-metric code when associated with the rank distance function:

$$d_{\text{rk}}(X, Y) = \text{rk}(X - Y).$$

Without loss of generality we assume that $m \geq n$. If $C \subset \mathbb{F}_q^{n \times m}$ is \mathbb{F}_q -linear of dimension k and minimum distance d we say it has parameters $[n \times m, k, d]_q$. In [18], (analogous to the Singleton bound) Delsarte showed that if C has minimum rank distance d then

$$|C| \leq q^{m(n-d+1)}.$$

Codes that meet Delsarte's bound are called *maximum rank distance* (MRD) codes.

Rank metric codes have been considered for several applications in communications theory and cryptography. An explicit construction for MRD codes was given independently in [18] and [33]. Several authors have worked extensively on decoding algorithms for this class of Delsarte-Gabidulin codes [7], [14], [38], [47], [71].

We briefly explain the connection to subspace codes for random network coding with error correction. One noisy channel model for matrix codes is represented by

$$X \rightarrow Y = AX + BZ,$$

where the matrix X is transmitted and the matrix Y is received. This can be associated with a network, where Z is an error matrix and A and B are the *transfer matrices* [45], which are unknown, so no knowledge of the network topology is assumed (which is the point of random coding). In the error-free case, A is invertible and Z is zero. Then AX is received, from which a user cannot deduce X but can identify its row space, $\langle X \rangle$. For this reason each message is encoded to a unique subspace, which can be identified with a unique reduced-row echelon form matrix.

A subspace code is a set of subspaces of \mathbb{F}_q^m . If all its codewords have the same dimension k (as we'll assume here), it is called a *constant dimension* subspace code (CDC). It is usually equipped with the subspace distance:

$$\begin{aligned} d_s(U, V) &= \dim(U + V) - \dim(U \cap V) \\ &= 2k - 2\dim(U \cap V). \end{aligned}$$

Given a pair of matrices X, Y , we can form a new pair of matrices in canonical form, $[I, X], [I, Y]$ and we get

$$d_s(\langle [I, X] \rangle, \langle [I, Y] \rangle) = 2d_{\text{rk}}(X - Y).$$

Then a rank-metric code in $\mathbb{F}_q^{n \times m}$ yields a CDC of constant dimension n . This is the *lifting* construction used in [61] which gives a practical scheme for decoding subspace codes using a rank-metric decoder, in particular, one for the Delsarte-Gabidulin codes. Asymptotically, the resulting codes are optimal, but for smaller parameters are not.

We remark at this point that there is a simple, low-complexity encoding/decoding scheme for matrix channels given in [60] that corrects error matrices of some fixed rank t , under the assumption

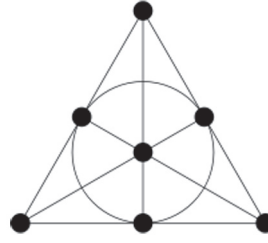


Fig. 1. A graphical representation of the classical Fano plane, with 7 points and 7 lines. Every pair of points is contained in a unique line.

that a basis of the error matrix occurs in the first v rows. The authors refer to this as *error trapping*. The probability of a decoding error under this scheme is at most

$$2t(q^{1+v-t})^{-1}.$$

A. The Main Subspace Coding Problem

This still leaves open the general question of optimality of subspace codes, the Main Subspace Coding problem. Many variants on lifting constructions have been explored using ideas from combinatorics and geometry [28], [27], [63] and many bounds on the size of an optimal subspace code have been derived (see [25], [37], [40] and the references therein). Many of these constructions have the simple lifted MRDs of [61] as subcodes. A highly useful resource for interested researchers is given by [40], where the authors have written a collection of the known upper bounds on the size of an optimal subspace code, which includes links to parameter tables and an extensive list of the literature.

The *multilevel construction* of [28] was very successful in producing good CDCs. Their approach uses constant weight Hamming codes and Ferrers diagrams [69, Chapter 16]. A Ferrers diagram arises in combinatorics as a means of representing partitions of an integer. For example, the sum $4 + 2 + 2$ is represented as a 3×3 array of dots and blanks, with 4 dots in the first row and 2 dots in the 2nd and 3rd rows. The dots of the array are arranged to have an echelon type form. Then a rank-metric *Ferrers diagram code* is constructed and lifted to yield a subspace code. An $[n, m, \delta]$ Ferrers diagram rank-metric code is formed by completions of an $n \times m$ matrix associated with a given Ferrers diagram \mathcal{F} , with zeroes appearing outside of the coordinates corresponding to the dots of \mathcal{F} in such a way that the resulting code has minimum rank distance δ . Theorem 1 of [28] gives an upper bound on the dimension of such a code as the minimum number of dots that do not appear in the first i rows and the rightmost $\delta - 1 - i$ rows over all $i \in \{0, \dots, \delta - 1\}$.

Example II.1. Let $x = [1001100]$. To construct a 3-dimensional space over \mathbb{F}_q , identify x with its unique echelon-Ferrers form matrix:

$$\begin{bmatrix} 1 & \cdot & \cdot & 0 & 0 & \cdot & \cdot \\ 0 & 0 & 0 & 1 & 0 & \cdot & \cdot \\ 0 & 0 & 0 & 0 & 1 & \cdot & \cdot \end{bmatrix} \begin{matrix} \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \end{matrix}$$

The Ferrers diagram on the right is used to produce a rank-metric Ferrers diagram code, whose dimension is at most 2 for $\delta = 2$, according to the bound of [28]. This rank-metric code is lifted to a CDC of constant dimension 3 by embedding its matrices into the echelon-Ferrers matrix of x and taking all row spaces as subspaces. If we repeat this procedure with other binary vectors that form a

constant Hamming weight code and take the union of the resulting subspace codes, we arrive at a larger CDC.

These ideas were further developed in [63], additionally using matchings of the complete graph to obtain some of the best known CDS for the *injection distance*.

Open Problem II.2. In [27], the authors give a number of constructions of optimal Ferrers diagram rank metric codes, which are optimal or near-optimal with respect to the Ferrers diagram bound [28, Theorem 1]. Such codes can be lifted to give good subspace codes. However, it is not known if the bound cannot be attained in some cases. The authors suggest that this question could be answered by finding large non-linear rank-metric anticodes, which are codes whose words have ranks upper-bounded by a given number. Anticodes for the rank metric are studied in much more detail in [34].

An intriguing example of an optimal subspace code relates to a q -analogue of design theory. Let C be a CDC of constant rank k in \mathbb{F}_q^n such that every t -dimensional subspace of \mathbb{F}_q^n is contained in exactly one member of C . Then C is called an $S_q(t, k, n)$ Steiner structure (or a q -Steiner system), which is also an optimal subspace code. A *spread*, which is a splitting of a vector space into subspaces with trivial intersection, is an example of an $S_q(1, k, n)$. A tantalizing first question is on the existence of a q -analogue of the *Fano Plane*, which for $q = 2$ would be an $S_2(2, 3, 7)$ having 381 3-dimensional spaces (planes) as codewords (from a choice of 11811 in \mathbb{F}_2^7) with every pair of lines (2-dimensional spaces) contained in a unique plane. It is still unknown if this 2-design over \mathbb{F}_2 exists.

It was a few years before the existence question of a non-trivial $S_q(t, k, n)$ was rewarded with an actual example. It was finally shown in [6] there exists an $S_2(2, 3, 13)$ (in fact at least 401 non-isomorphic ones). This sporadic example was discovered by computer search, applying the Kramer-Mesner method under the assumption of it having a large group of symmetries, making the computation feasible. To give an idea of the scale of such a problem, this parameter set produces a code with 1,597,245 3-dimensional spaces as codewords. Searching for the next cases using this method is not tractable at this time. No other non-trivial examples are known. If the q -Fano plane does exist, its symmetry group would be very small, possibly trivial [44] making a search by computer infeasible (for now). An interesting connection to the existence of *skew affine q -Steiner systems* was given in [72].

Open Problem II.3. Does there exist an $S_2(2, 3, 7)$? A computer-free construction of a CDC of constant dimension 3 and minimum subspace distance 4 in \mathbb{F}_2^7 with largest known number of codewords (329) is given in [41], as an example of a general method for dimension 3 CDCs. The authors use expurgation and augmentation to modify a lifted Delsarte-Gabidulin code with the aim of obtaining an optimal code or indeed the q -Fano plane. If the $S_2(2, 3, 7)$ does exist, it may be possible to obtain it by modifying this approach, using a different class of MRD codes.

Open Problem II.4. Does the $S_2(2, 3, 13)$ example occur as part of an infinite family of q -Steiner systems? Do other examples exist? Are there algebraic constructions for q -Steiner systems?

B. MRD Codes

There are a few equivalent representations of the Delsarte-Gabidulin MRD codes. An elegant construction uses *linearized polynomials*

(see [50], [55] for properties of such polynomials). A linearized polynomial in $\mathbb{F}_{q^n}[x]$ is one of the form:

$$f = f_0x + f_1x^q + \dots + f_{k-1}x^{q^{k-1}},$$

with $f_i \in \mathbb{F}_{q^n}$. Then f represents an \mathbb{F}_q -linear map on \mathbb{F}_{q^n} and so can be identified with an $n \times n$ matrix with coefficients in \mathbb{F}_q , after choosing some basis of \mathbb{F}_{q^n} for the scalar field \mathbb{F}_q . We refer the reader to [57] to see an explicit worked example of this correspondence, which we omit here due to space constraints. Matrix multiplication corresponds to composition of functions modulo $x^q - x$ and the rank of f is at least $n - k + 1$, as the dimension of its kernel is at most $k - 1$. The polynomial representation can offer useful insights to the structure of rank-metric codes.

The most general infinite family of MRD codes known to date was presented by Sheekey in [57]. For brevity we'll give this for $m = n$, so for $[n \times n, nk, n - k + 1]_q$ codes. Such a code has the form: $\mathcal{H}_k(\nu, h) :=$

$$\{f_0x + f_1x^q + \dots + f_{k-1}x^{q^{k-1}} + \nu f_0^h x^k : \nu, f_i \in \mathbb{F}_{q^n}\},$$

where $\nu(q^n - 1)/(q - 1) \neq (-1)^{nk}$. This includes the family of Delsarte-Gabidulin codes, which are precisely those for which $\nu = 0$. Note that the Delsarte-Gabidulin codes in $\mathbb{F}_q^{n \times m}$ are \mathbb{F}_{q^n} -linear, whereas for $\nu \neq 0$, $\mathcal{H}_k(\nu, h)$ may not be, depending on the value of h .

In [42], the authors give a simple criterion for checking if an MRD code is a Delsarte-Gabidulin code and use this to produce sporadic examples of MRD codes that do not fall into this category. In fact 'most' MRD codes are not Delsarte-Gabidulin codes; that is, the property of being MRD and non-Delsarte-Gabidulin are *generic* [53]. It is likely, although not yet proven in the literature, that the codes $\mathcal{H}_k(\nu, h)$ also do not encompass 'most' MRD codes.

The rank *weight distribution*, (the number of codewords of each possible weight) of an MRD code is determined by its parameters $[n \times m, m(n - d + 1), d]_q$ [18]. The dual code of an \mathbb{F}_q -linear matrix code $C \subset \mathbb{F}_q^{n \times m}$ is given by

$$C^\perp := \{Y \in \mathbb{F}_q^{m \times n} : \text{Tr}(XY^T) = 0 \forall X \in C\},$$

where $\text{Tr}(A)$ is the usual trace of a square matrix A , the sum of its diagonal elements. This definition follows from the fact that $\langle X, Y \rangle := \text{Tr}(XY^T)$ is an inner product on $\mathbb{F}_q^{n \times m}$. As is usual in algebraic coding theory, study of the dual code plays an important role. C is a linear MRD code if and only if its dual is MRD, equivalently, if and only if

$$d + d^\perp = n + 2.$$

There has been much recent activity on the structure of MRD codes [19], [20], [35], [54], [51]. Unlike MDS codes, their classical analogues, MRD codes exist for all choices of q, m, n, d . Mac Williams' duality theorem holds for rank-metric codes [18], [36], [56] (although Mac Williams' extension theorem does not).

Gadouleau and Yan are among the few authors who have considered covering properties of rank-metric codes [35]. The covering radius of a rank-metric code $C \subset \mathbb{F}_q^{n \times m}$ is defined as

$$\begin{aligned} \rho(C) &:= \max\{\min\{d_{\text{rk}}(R, C) : C \in \mathcal{C}\} : R \in \mathbb{F}_q^{n \times m}\} \\ &:= \max\{d_{\text{rk}}(R, C) : R \in \mathbb{F}_q^{n \times m}\}. \end{aligned}$$

The covering radius of a code is a fundamental parameter that reflects the maximum weight of any error correctable by that code. The general covering problem is to determine the least number of spheres of a given radius that cover the underlying space. The most interesting codes in this respect are those with low covering radius. It has been extensively studied in the Hamming metric, where it has played a role in different applications, such as data compression. In general, determining the covering radius of a code is hard, as are constructing families with specified covering radius.

There are however, some bounds on the covering radius for the Hamming case [16] that follow without much difficulty to the rank-metric case. It can be shown, for example, following the arguments of [17], that the covering radius of a rank-metric code is upper bounded by the number of weights of its dual code (or in the non-linear case by its *external distance*).

Example II.5. Let $n = rs$ and let C be the $[n \times n, nr, s]_q$ code

$$C = \left\{ \sum_{i=0}^{r-1} f_i x^{q^i} : f_i \in \mathbb{F}_{q^s} \right\}.$$

Then C has r non-zero rank weights $\{s, 2s, \dots, rs\}$ over \mathbb{F}_q , so that $\rho(C^\perp) \leq r$.

We mention a few fundamental upper and lower bounds on the covering radius that are independent of the metric used.

- The *sphere-covering bound* gives a lower bound on the covering radius of a code:

$$\rho(C) \geq \{N : V_q(n, m, N) | C | \geq q^{nm}\},$$

where $V_q(n, m, N) = \{A \in \mathbb{F}_q^{n \times m} : \text{rk}(A) \leq N\}$ is the volume of a sphere of radius N about a matrix in $\mathbb{F}_q^{n \times m}$.

- If $C \subset C' \subset \mathbb{F}_q^{n \times m}$ then the covering radius of C is lower-bounded by the minimum distance of C' :

$$\rho(C) \geq d_{\text{rk}}(C').$$

- If C is *maximal*, i.e. is not a proper subset of another code for the same minimum distance d , then

$$\rho(C) \leq d - 1.$$

Many other upper and lower bounds appear in [35].

While the weight distribution of an MRD code in $\mathbb{F}_q^{n \times m}$ is determined by its minimum distance, its covering radius is not. Any MRD code C is clearly maximal, being optimal. In the case of the MRD codes $\mathcal{H}_k(v, h)$, the covering radius attains this last bound with equality; that is, it is an $[n \times n, n(n-d+1), d]_q$ rank metric code with covering radius $d-1$. This can be seen by observing that these form a nested class of MRD codes. However, there are examples of MRD codes outside this class with covering radius less than $d-1$.

Open Problem II.6. Can the construction of [57] be extended, or is this the largest infinite family of MRD codes that contains the Delsarte-Gabidulin codes? Do there exist other infinite families of MRD codes?

Open Problem II.7. Can the criterion for Delsarte-Gabidulin codes of [42], or a variant of it, be extended to include the larger class of MRD

codes [57]? If so then the probability of an arbitrary MRD code being in this family of codes could be upper-bounded.

Open Problem II.8. Find other infinite families of rank-metric codes with covering radius $d-1$.

III. Broadcast with Side-Information

Rank-metric codes also appear in broadcast problems. Consider the following broadcast with side information scenario. The data vector x below may have coefficients in a field $\mathbb{F}_{q'}$, but we assume that all other matrices and vectors have coefficients in \mathbb{F}_q .

- There is a single sender and m receivers.
- $x = [x_1, \dots, x_n]$ is the uncoded data held by the sender.
- User i has side information (V_i, xV_i) , for some $n \times v_i$ matrix $V_i = [V_i^1, \dots, V_i^{v_i}]$ of rank v_i .
- User i has request matrix $R_i = [R_i^1, \dots, R_i^{r_i}]$ an $n \times r_i$ matrix of rank r_i .
- User i demands request packet xR_i .
- The sender, after receiving each request R_i , broadcasts

$$Y = xL$$

for some $n \times N$ matrix L , $N < n$.

- Each user decodes xR_i by solving a linear system of equations in the received Y and its side-information.

The sender is faced with the following broadcast problem: find an encoding matrix L that minimizes N such that the demands of all users satisfied.

We say that L realizes a length N code for this problem if indeed each user can retrieve its demand xR_i for any source data vector x , given knowledge of

$$L, xL, V_i, xV_i.$$

The source data x should be thought of as a variable in the above *instance* of the broadcast with side-information problem. If such an L exists, we say that the length N is achievable for the given instance. It is a computationally hard problem, NP-hard in fact, to find such L realizing a minimal length encoding.

User i can retrieve its demand xR_i , for all possible choices of x if and only if there exist matrices A_i, B_i satisfying

$$R_i = V_i A_i + L B_i,$$

from which it decodes xR_i , knowing xV_i (as its side information) and xL (which was transmitted). It is generally assumed that a user does not demand xR_i if it already has it in its cache. Therefore, we assume that no column of $R_i = [R_i^1, \dots, R_i^{r_i}]$ is contained in the column space of V_i , so in other words $R_i^j \neq V_i a$ for any vector a .

We now describe this in terms of a matrix code. First let $r = \sum_{j=1}^m r_j$ and let R be the $n \times r$ matrix

$$R = [R_1, R_2, \dots, R_m].$$

We call R the request matrix. For each i , let

$$C_i = \{V_i A : A \in \mathbb{F}_q^{v_i \times r_i}\} \subset \mathbb{F}_q^{n \times r_i}.$$

So C_i is a vector space of $n \times r_i$ matrices for the scalars \mathbb{F}_q . It can be thought of as r_i copies of the length n linear code generated by the columns of V_i . Now define

$$C = \{[U_1, U_2, \dots, U_m] : U_i \in C_i\} \subset \mathcal{F}_q^{n \times r},$$

which is a vector space of $n \times r$ matrices for the scalars \mathbb{F}_q . We call this matrix code C the side-information code.

We say that the pair (R, C) is an instance of the broadcast with side-information problem. The problem of determining the optimal code length of the instance (R, C) and a corresponding encoding matrix L is a *delivery* problem.

It can easily be shown that the minimum length of a code for (R, C) is

$$\kappa(R, C) := \min\{\text{rk}(R + C) : C \in C\}.$$

The set $R + C := \{R + C : C \in C\}$ is a coset or translate of C , so $\kappa(R + C)$ is the minimum rank of any member of this coset. It is also the rank distance of the matrix R to the side information code C . This generalizes the *minrank* of a *side-information graph* or hypergraph, as it arises in the *index coding problem* (cf. [3], [4], [49], [23]). Implicit in this is the fact that any full-rank matrix L that realizes the instance (R, C) can be obtained by rank-factorization of a member of $R + C$. Note that

$$\dim C = \sum_{i \in [m]} r_i v_i$$

over \mathbb{F}_q , so $|R + C| = q^s$ where $s = \sum_{i \in [m]} r_i v_i \leq rn$.

For a given side-information code C , the sender can satisfy any set of requests in at most $\rho(C)$ transmissions, the rank-metric covering radius of the code C . So if the side-information code C has low covering radius, then all instances of this broadcast problem require a small number of transmissions. Different variations and applications of the problem will however assume some restriction on the choice of possible request matrices R that give a *valid* instance (R, C) . Then for given C , the sender can satisfy any valid set of requests using at most

$$\begin{aligned} \rho_{\mathcal{R}}(C) &:= \max\{\kappa(R, C) : R \in \mathcal{R}(C)\} \\ &= \max\{d_{\text{rk}}(R, C) : R \in \mathcal{R}(C)\} \end{aligned}$$

transmissions, where $\mathcal{R}(C)$ denotes some set of valid request matrices in $\mathbb{F}_q^{n \times r}$.

This relates to a *placement* problem: that of determining side-information codes C with smallest covering radius or smallest restricted covering radius (where the radius is restricted to a subset $\mathcal{R}(C) \subset \mathbb{F}_q^{n \times r}$).

As both quantities $\kappa(R, C)$ and $\rho_{\mathcal{R}}(C)$ are hard to compute, bounds and estimates are sought on them.

We remark that if $\mathcal{R}(C)$ is the set of request matrices R such that no column of R_i is contained in the column space of V_i for any i , i.e. if

$$\mathcal{R}(C) = \{R \in \mathbb{F}_q^{n \times r} : R_i^j \neq V_i a, \text{ any } a \in \mathbb{F}_q^{v_i}, i \in [m], j \in [r_i]\}$$

then

$$\rho_{\mathcal{R}}(C) = \rho(C).$$

Clearly, $\rho_{\mathcal{R}}(C) \leq \rho(C)$. To see the converse, let $R \in \mathbb{F}_q^{n \times r} \setminus \mathcal{R}(C)$ satisfy $d_{\text{rk}}(R, C) = \rho(C)$. Without loss of generality, we may assume that R has the form

$$R = [X_1, O | X_2, O | \dots | X_m, O],$$

for some matrices $X_i \in \mathbb{F}_q^{n \times c_i}$ such that no column of X_i is contained in the column space of V_i for any i and where O is the $n \times (r_i - c_i)$ zero matrix. Let $R' = [X_1, \dots, X_m]$ and let C' be the matrix code found by deleting the coordinates of C in $[r]$ corresponding to the zero columns of R . Let

$$S = [X_1, Y_1 | X_2, Y_2 | \dots | X_m, Y_m] \in \mathcal{R}(C),$$

for some matrices Y_i . Then

$$\rho(C) = d_{\text{rk}}(R, C) = d_{\text{rk}}(R', C') \leq d_{\text{rk}}(S, C) \leq \rho(C).$$

It follows that given any $R \in \mathbb{F}_q^{n \times r} \setminus \mathcal{R}(C)$ at distance $\rho(C)$ to C , there exist some $S \in \mathcal{R}(C)$ at distance $\rho(C)$ to C . In particular, any lower bounds on $\rho(C)$ may be applied to $\rho_{\mathcal{R}}(C)$ for this set of valid request matrices.

Open Problem III.1. Obtain further bounds on $\kappa(R, C)$ and $\rho(C)$ for codes C with the structure of a side-information code. There are several bounds on $\kappa(R, C)$ already known from the index coding with side information problem, but the best of these are inexplicit bounds [4], [5], [9], [58], [67].

Open Problem III.2. There has been limited activity so far on the subject of error correction in the broadcast with side information problem. Many of the known algorithms are based on syndrome decoding [4], [23]. Find lower complexity algorithms for error correction with respect to the injection/subspace distance.

Open Problem III.3. Design side-information codes C with low rank metric covering radius, or infinite families of such codes.

A. The Index Coding Problem

The delivery problem for a fixed instance (R, C) is a *scalar* linear index coding problem if x has coefficients in \mathbb{F}_q and is a *vector* linear index coding problem if x has coefficients in \mathbb{F}_q^t for $t > 1$. In the vector linear case, x has components of block length t . The block length does not affect the minrank parameter, however, due to overhead transmission costs, the gains of index coding are greater as t increases.

It is common in the index coding literature to assume that R_i is a vector over \mathbb{F}_q of length n , so that each user requests a single packet (so $r_i = 1$ for each i and $r = m$). This is because in the event of a user requesting two packets, that user can be represented as two users with the same side-information and the problem essentially remains unchanged, from the index coding point of view.

In the original version of the index coding problem [2], [3], [8], [9], we have $m = n$, R_i is a standard basis vector e_i (so the i th component of x is demanded by the i th user) and the matrices V_i all have standard basis vectors as columns (so each user has components x_j if the j th row of V_i is non-zero). This formulation identifies an instance with an underlying graph, or more generally, for $m > n$,

a hypergraph [22], [23]. In [21] the authors introduce the problem for arbitrary request vectors R_i and matrices V_i using the term index coding with *coded side information*.

Example III.4. We describe an instance of the original index coding problem. Let $m = n = 7$ and $q = 2$. Let

$$V_1 = \begin{bmatrix} 0100000 \\ 0010000 \end{bmatrix}, V_2 = \begin{bmatrix} 0000010 \\ 0000001 \end{bmatrix}, V_3 = \begin{bmatrix} 0000100 \\ 0000001 \end{bmatrix}, V_4 = \begin{bmatrix} 0100000 \\ 0000100 \end{bmatrix},$$

$$V_5 = \begin{bmatrix} 1000000 \\ 0000010 \end{bmatrix}, V_6 = \begin{bmatrix} 0010000 \\ 0001000 \end{bmatrix}, V_7 = \begin{bmatrix} 1000000 \\ 0001000 \end{bmatrix}$$

and $R_i = e_i$ (i th standard basis vector) for $i = 1, \dots, 7$. So R is the identity matrix and the i th user wants the i th bit of x . The coset $R + C$ is a set of $2^{14} = 16384$ matrices of the form

$$\begin{bmatrix} 1 & \cdot & \cdot & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & \cdot & \cdot \\ 0 & 0 & 1 & 0 & \cdot & 0 & \cdot \\ 0 & \cdot & 0 & 1 & \cdot & 0 & 0 \\ \cdot & 0 & 0 & 0 & 1 & \cdot & 0 \\ 0 & 0 & \cdot & \cdot & 0 & 1 & 0 \\ \cdot & 0 & 0 & \cdot & 0 & 0 & 1 \end{bmatrix}$$

where each dot \cdot may be filled with 0 or 1. It can be checked that this coset has rank weight distribution

$$(4,1), (5,238), (6,6575), (7,9570).$$

In particular, it has exactly one matrix of minimal rank 4, which is

$$\begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}$$

In fact this is the incidence matrix of the Fano plane. (It is known that incidence matrices of structures like these have rank at most $(n+1)/2$.) Let $\mathcal{R}(C) = \{R \in \mathbb{F}_q^{7 \times 7} : R_i \notin C_i \text{ any } i \in [7]\}$. If we compute for C as above and for R a permutation matrix in $\mathcal{R}(C)$, we find that it takes the value 3 for 1% of instances, 4 for 62% of instances and 5 for 37% instances so the expected optimal number of transmissions if the request vectors are linearly independent is 4.35.

Feasible (not necessarily optimal) solutions to the index coding problem, i.e. determination of an encoding matrix L , can be found by various methods of partitioning an instance into simpler ones, for which an optimal solution is known. In the literature, these first appeared as graph-theoretic algorithms based on *clique covering*, *multicast partition* and their variants [9], [58], [67], but have been shown also to have analogues in the general case [5]. These use integer and linear programming to obtain coding partitions.

If we have $m > n$, each request matrix R_i a standard basis vector and no restriction on the V_i , then determining L of optimal or near-optimal length can be identified with a *low-rank matrix completion* problem. A greedy algorithm for the application to index coding was outlined in [49]. For wireless applications (so for matrices over the reals), the problem has been addressed in [39], [68]. While there are many algorithms for low-rank matrix completion problems

over R , few are known for matrices over finite fields. Even less is known for the most general case.

Open Problem III.5. Find efficient algorithms for low-rank matrix completions arising in the index coding problem over finite fields.

B. The Coded-Caching Problem

The delivery phase of the *canonical coded-caching* problem [52] is the following specialisation of the instance (R, C) . First it is assumed that the n packets of x comprise k blocks x^1, \dots, x^k of size ℓ (so that $n = k\ell$) and that each i th user wants some complete block, say x^j , after delivery. So R_i is an $n \times r_i$ matrix

$$R_i = [O \dots H^T \dots O]^T$$

for some $\ell \times r_i$ matrix H with standard basis vectors of length ℓ as columns. Each user has a subset of some number of packets from each block and the same number of packets v in total. In terms of (R, C) , this imposes the constraints that for each i ,

- V_i is an $n \times v$ matrix,
- R_i and V_i have standard basis vectors as columns,
- the j th block of ℓ rows of V_i has some $\ell - r_i$ standard basis vectors of length ℓ as columns that complete H to a basis of \mathbb{F}_q^ℓ .

For example, if user i has the last $\ell - r_i$ packets of x^j in its cache then R_i and V_i have the form,

$$R_i = \begin{bmatrix} O \\ \vdots \\ O \\ A|0 \\ O \\ \vdots \\ O \end{bmatrix}, V_i = \begin{bmatrix} * & O \\ * & \vdots \\ * & O \\ * & 0|B \\ * & O \\ * & \vdots \\ * & O \end{bmatrix},$$

where $[A|B]$ is an $\ell \times \ell$ permutation matrix. So valid choices of C and R for consideration in the canonical coded caching problem are those satisfying the above. If a subset of users wish to receive the same block, the delivery to that set of users becomes a local multicast problem.

What distinguishes the coded-caching problem from the index coding problem is the role of the sender in the placement phase. If the index coding problem is essentially one of delivery for given (R, C) , central to the coded caching problem is optimal placement of the side-information code C in advance of knowing users' request matrix R . The sender seeks to choose C in such a way that the encoding matrix L can deliver all requests xR_i with a minimal number of transmissions. Thus the problem is to determine C such that $\rho_{\mathcal{R}}(C)$ is minimized, or to minimize this number for all valid choices of C . In [52] the authors use the cut-set bound to derive a lower bound on the optimal storage memory rate trade-off. Furthermore, they devise a scheme that achieves this rate within a constant factor. So asymptotically, the canonical coded caching problem is solved. Moreover, it was shown in [70] that improvements to the scheme presented in [52] can only be achieved by considering caching schemes with coded side-information.

For example, the matrices V_i may have columns that are not standard basis vectors, which corresponds to the cache data (the side-information) being encoded. Then C_i is an arbitrary $n \times v$ -dimensional matrix code for each i . In [66] the authors propose a scheme for

coded-caching with coded side-information using MDS and rank metric codes. Their scheme delivers an improvement in the memory-rate trade-off of several known schemes and are in some cases optimal. However, their scheme requires large field sizes.

Open Problem III.6. *Modify current rank-metric sphere covering bounds to obtain lower bounds on the restricted covering radius for a side-information code C .*

Open Problem III.7. *Obtain good caching schemes for smaller field sizes. Construct codes with low restricted covering radius for the coded caching problem.*

IV. Concluding Remarks

Advances in finite geometry, combinatorics, algebraic coding theory and lattices have been made as a direct result of interest in network coding problems. It is the hope of the author that some small demonstration has been made of the great impact of this field on mathematics. It seems reasonable to expect that rank-metric codes will continue to play a dominant role in network communications theory and many more open problems remain to be solved.

Much of the research described here was conducted by participants in the EU COST Action *Random Network Coding and Designs over $GF(q)$* . A great deal more work than has been mentioned here was carried out as part of that action (see <http://www.network-coding.eu/>), including projects on distributed storage and cryptography and practical schemes for network coding.

References

- [1] N. Alon, A. Hassidim, E. Lubetzky, U. Stav, and A. Weinstein, "Broadcasting with Side Information", in Proc. 49th Annu. IEEE Symp. on Found. of Comput. Sci. (FOCS), pp. 823832, 2008.
- [2] Z. Bar-Yossef, Z. Birk, T. S. Jayram, and T. Kol, "Index Coding with Side Information", in Proc. 47th Annu. IEEE Symp. Found. Comput. Sci., 2006, pp. 197–206.
- [3] Z. Bar-Yossef, Z. Birk, T. S. Jayram, and T. Kol, "Index Coding with Side Information", IEEE Transactions on Information Theory, vol. 57, no. 3, pp. 1479–1494, Mar. 2011.
- [4] E. Byrne and M. Calderini, "Error Correction for Index Coding with Coded Side Information," arXiv preprint, 1506.00785, 2015.
- [5] E. Byrne and M. Calderini, "Bounding the Optimal Rate of the ICSI and ICCSI Problems," arXiv preprint 1604.05991, 2016.
- [6] M. Braun, T. Etzion, P. R. J. Östergård, A. Vardy, A. Wassermann, "Existence of q -Analogues of Steiner Systems," Forum of Mathematics, Pi, to appear (see arXiv:1304.1462).
- [7] M. Bossert, E. Gabidulin, "Codes for network coding," 2008 IEEE International Symposium on Information Theory, pp. 867–870.
- [8] Y. Birk and T. Kol, "Informed Source Coding on Demand (ISCOD) over Broadcast Channels," in Proc. IEEE Conf. Comput. Commun., San Francisco, CA, 1998, pp. 1257–1264.
- [9] A. Blasiak, R. Kleinberg, E. Lubetzky, "Broadcasting With Side Information: Bounding and Approximating the Broadcast Rate," IEEE Transactions on Information Theory, vol. 59, no. 9, 2013, pp. 5811–5823.
- [10] M. Braun, M. Kiermaier, Nakić, "On the Automorphism Group of a Binary q -Analog of the Fano Plane," Eur. J. Comb. 51, 2016.
- [11] M. Braun, A. Kohnert, P. R. J. Östergård, A. Wassermann, "Large Sets of t -Designs over Finite Fields," Journal of Combinatorial Theory, Series A, Vol 124, pp. 195202, 2014.
- [12] T. Berger, P. Loidreau, "How to Mask the Structure of Codes for a Cryptographic Use," Designs, Codes and Cryptography, Volume 35, Issue 1, pp. 6379, 2005.
- [13] C. Bachoc, A. Passuello, and F. Vallentin, "Bounds for Projective Codes from Semidefinite Programming," Advances in Mathematics of Communications 7, pp. 127–145, 2013.
- [14] H. Bartz, V. Siderenko, "Algebraic Decoding of Folded Gabidulin Codes," Des. Codes Crypt., Online First, pp. 1–16 March 2016.
- [15] Z. Chen, "Fundamental limits of caching: Improved bounds for small buffer users," arXiv preprint arXiv:1407.1935v1, Jul. 2014.
- [16] G. Cohen, Honkala, Litsyn, Lobstein, "Covering Codes," Elsevier Science, North-Holland, 1997.
- [17] P. Delsarte, "Four Fundamental Parameters of a Code and Their Combinatorial Significance," Inform. and Contl, 23, pp. 407–438, 1973.
- [18] P. Delsarte, "Bilinear Forms Over a Finite Field with Applications to Coding Theory," Journal of Combinatorial Theory Series A, 1978 25, 3, pp. 226–241.
- [19] J. de la Cruz, E. Gorla, H. H. Lopez, A. Ravagnani, "Rank Distribution of Delsarte Codes," arXiv: 1510.01008, 2015.
- [20] J. de la Cruz, M. Kiermaier, A. Wassermann, W. Willems, "Algebraic Structures of MRD Codes," to appear in Advances in the Mathematics of Communications, arXiv:1502.02711.
- [21] M. Dai, K. W. Shum, C. W. Sung, "Data Dissemination With Side Information and Feedback," IEEE Transactions on Wireless Communications, Vol. 13, 9, pp. 4708–4720, 2014.
- [22] S. H. Dau, V. Skachek, and Y. M. Chee, "On the Security of Index Coding With Side Information," IEEE Transactions on Information Theory, vol. 58, no. 6, June 2012, pp. 3975–3988.
- [23] S. H. Dau, V. Skachek, and Y. M. Chee, "Error Correction for Index Coding With Side Information," IEEE Transactions on Information Theory, Vol. 59, Issue: 3, pp. 1517–1531, 2013.
- [24] T. Etzion, "A New Approach to Examine q -Steiner Systems," arXiv:1507.08503, 2015.
- [25] T. Etzion, "Problems on q -Analogues in Coding Theory," preprint arXiv:1305.6126
- [26] M. Effros, S. El Rouayheb, M. Langberg, "An Equivalence Between Network Coding and Index Coding," IEEE Transactions on Information Theory, (61), No. 5, pp. 2478–2487, 2015.
- [27] T. Etzion, E. Gorla, A. Ravagnani, A. Wachter-Zeh, "Optimal Ferrers Diagram Rank-Metric Codes," IEEE Transactions on Information Theory, Vol. 62, No. 4, 2016, pp. 1616–1631.

- [28] T. Etzion and N. Silberstein, "Error-Correcting Codes in Projective Space Via Rank-Metric Codes and Ferrers Diagrams," *IEEE Trans. Inf. Theory*, vol. 55, no. 7, pp. 2909-2919, 2009.
- [29] T. Etzion and N. Silberstein: "Codes and Designs Related to Lifted MRD Codes Information Theory, *IEEE Transactions on* 59, 2, pp. 1004–1017, 2012.
- [30] T. Etzion, A. Vardy, "Error-Correcting Codes in Projective Space," *IEEE Trans on Inform. Thy*, Volume 57, Issue 2, 2011.
- [31] A. El Rouayheb, A. Sprintson, and C. Georghiades, "On the Index Coding Problem and its Relation to Network Coding and Matroid Theory", *IEEE Transactions on Information Theory*, vol. 56, no. 7, pp. 3187–3195, Jul. 2010.
- [32] A. Fazeli, S. Lovett, A. Vardy, "Nontrivial t -Designs over Finite Fields Exist for all t ," *Journal of Combinatorial Theory, Series A*, Volume 127, Issue 1, pp. 149160, 2014.
- [33] E. Gabidulin, "Theory of Codes with Maximum Rank Distance," *Problems of Information Transmission*, 21:1, pp. 1–12, 1985.
- [34] E. Gorla, A. Ravagnani, "Subspace Codes From Ferrers Diagrams," to appear in *Journal of Algebra and Its Applications* (see arXiv:1405.2736).
- [35] M. Gadouneau, Z. Yan, "Packing and Covering Properties of Rank Metric Codes," *IEEE Trans. Inform. Theory*, 54 (9) 2008.
- [36] M. Gadouneau, Z. Yan, "MacWilliams Identity for Codes with the Rank Metric," *EURASIP Journal on Wireless Communications and Networking*, Volume 2008, Issue 1, 2008.
- [37] M. Gadouneau, Z. Yan, "Packing and Covering Properties of Subspace Codes for Error Control in Random Linear Network Coding," *IEEE Trans. Inform. Theory*, 56 (5), pp. 2097–2108, 2010
- [38] V. Guruswami, C. Wang; C. Xing, "Explicit List-Decodable Rank-Metric and Subspace Codes via Subspace Designs," *IEEE Transactions on Information Theory*, Vol. 62, 5, pp. 2707–2718, 2016.
- [39] X. Huang; S. El Rouayheb, "Index Coding and Network Coding via Rank Minimization," *IEEE Information Theory Workshop (ITW)*, pp.14–18, 2015.
- [40] D. Heinlein, M. Kiermaier, S. Kurz, A. Wassermann, "Tables of Subspace Codes," <http://subspacecodes.uni-bayreuth.de/>, arXiv preprint arXiv:1601.02864, 2016.
- [41] T. Honold, M. Kiermaier, "On Putative q -Analogues of the Fano plane and Related Combinatorial Structures," *Dynamical Systems, Number Theory and Applications*, pp. 141–175, 2016.
- [42] A. Horlemann-Trautmann, K. Marshall, "New Criteria for MRD and Gabidulin Codes and some Rank-Metric Code Constructions," to appear in *Advances in Mathematics of Communications*, 2016 (arXiv: 1507.08641).
- [43] R. Kötter, F. Kschischang, "Coding for Erasures and Errors in Random Network Coding," *IEEE Transactions on Information Theory*, (54), 8, 2008.
- [44] M. Kiermaier, S. Kurz, A. Wassermann, "The Order of the Automorphism Group of a Binary q -Analog of the Fano Plane is at Most Two," *European J. Combin.* 51, pp. 443457, 2016.
- [45] R. Koetter, and M. Medard, "An Algebraic Approach to Network Coding", *IEEE/ACM Trans. Netw.*, 11 (5) pp. 782–795, 2003.
- [46] M. Kiermaier, M. O. Pavcević, "Journal of Combinatorial Designs 23, pp. 463–480, 2015.
- [47] P. Loidreau, "A Welch-Berlekamp Like Algorithm for Decoding Gabidulin Codes," *Lect. Notes in Comp. Sc.*, pp. 36–45, 2006.
- [48] P. Loidreau, "Designing a Rank Metric Based McEliece Cryptosystem," *Post-Quantum Cryptography, Lecture Notes in Computer Science Volume 6061* pp. 142–152, 2010.
- [49] N. Lee, A. G. Dimakis, and R. W. Heath, Jr., "Index Coding With Coded Side-Information," *IEEE Comm. Letters*, 19 (3), 2015.
- [50] R. Lidl, H. Niederreiter, *Finite Fields (Encyclopedia of Mathematics and its Applications)*, 2nd Edition, Cambridge Univ. Press, 1997.
- [51] K. Morrison, "Equivalence for Rank-metric and Matrix Codes and Automorphism Groups of Gabidulin Codes," *IEEE Trans. Inform. Theory* 60 (11), 2014.
- [52] M. Maddah-Ali, U. Niesen. "Fundamental limits of caching," *IEEE Transactions on Information Theory* 60.5 (2014): 2856–2867.
- [53] A. Neri, A. Horlemann-Trautmann, T. Randrianarisoa, J. Rosenthal, "On the Genericity of Maximum Rank Distance and Gabidulin Codes, preprint arxiv, arXiv:1605.05972v1, 2016.
- [54] G. Nebe, W. Willems, "On Self-Dual MRD Codes," arXiv: 1505.07237, 2015.
- [55] O. Ore, "On a Special Class of Polynomials," *Trans. Amer. Math. Soc.* 35 (1933) 559–584.
- [56] A. Ravagnani, "Rank-Metric Codes and Their Duality Theory," *Designs Codes and Cryptography*, Vol. 80, Issue 1, 2016.
- [57] J. Sheekey, "A New Family of MRD Codes," to appear in *Adv. in Math. of Comms* (see arXiv:1504.01581) 2016.
- [58] K. Shanmugan, A. Dimakis, M. Langberg, "Graph Theory versus Minimum-Rank for Index Coding," *Proceedings of the 2014 IEEE International Symposium on Information Theory (ISIT)* (full-paper at arXiv:1402.3898.v1, Feb 2014), pp. 291–295, 2014.
- [59] A. Shishkin, E. Gabidulin and N. Pilipchuk, "On Cardinality of Network Subspace Codes," *Proceeding of the Fourteenth Int. Workshop on Algebraic and Combinatorial Coding Theory (ACCT-XIV)*, 7, 2014.
- [60] D. Silva, F. R. Kschischang, R. Koetter, "Communication Over Finite-Field Matrix Channels," *IEEE Trans. Inf. Theory*, vol. 56, no. 3, pp. 1296–1305, Mar. 2010.

- [61] D. Silva, F. Kschischang, R. Kötter, "A Rank-Metric Approach to Error Control in Random Network Coding," *IEEE Trans. Inform. Th.* (54), 9, 2008.
- [62] K. W. Shum, D. Mingjun, C. Sung, "Broadcasting with Coded Side Information," 2012 IEEE 23rd International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC), vol. 89, no. 94, pp. 9–12, Sept. 2012.
- [63] N. Silberstein, A. Trautmann, "Subspace Codes Based on Graph Matchings, Ferrers Diagrams, and Pending Blocks," *IEEE Trans. Inf. Theory*, vol. 61, no. 7, pp. 3937–3954, 2015.
- [64] S. Thomas, "Designs over Finite Fields," *Geom. Dedicata*, 21, pp. 237242, 1987.
- [65] S. Thomas, "Designs and Partial Geometries over Finite Fields," *Geom. Dedicata*, 63, pp. 247253, 1996.
- [66] C. Tian and J. Chen, "Caching and Delivery via Interference Elimination," arXiv preprint 1604.08600, 2016.
- [67] A. S. Tehrani, A. G. Dimakis, M. J. Neely, "Bipartite Index Coding," *Proceedings of the IEEE 2012 International Symposium on Information Theory (ISIT)*, Boston, Jul 1–6, 2012, pp. 2246–2250.
- [68] J. I. Tamir, E. R. Elenberg, A. Banerjee, S. Vishwanath, "Wireless Index Coding Through Rank Minimization," *IEEE ICC 2014 - Wireless Communications Symposium*, pp. 5209–5214.
- [69] J. H. van Lint and R. M. Wilson, *A Course in Combinatorics*. Cambridge, U.K.: Cambridge Univ. Press, 1992.
- [70] K. Wan, D. Tuninetti, and P. Piantanida, "On the optimality of uncoded cache placement," arXiv preprint arXiv:1511.02256, 2015.
- [71] A. Wachter-Zeh, "Bounds on List Decoding of Rank-Metric Codes," *IEEE Trans. Inf. Theory*, 59 (11) pp. 7268–7278, 2013.
- [72] J. Zumbärgel, "Designs and Codes in Affine Geometry," arXiv preprint arXiv:1605.03789, 2016.

The Historian's Column

This continues to be a year of celebration for Information Theory as we observe the 100th anniversary of C. E. Shannon's birth. No matter how much we say in words of praise for the Founder of the Field, it is never enough. But, it is also appropriate to praise and cherish the Field itself, which is Shannon's foundational creation. We have said a lot about the Man and his inspiring personality. So let us ponder and reflect upon what unites us all, namely our common interest in what Shannon gave us. To talk about anything else in this column during this year would be out of place.

It has often been said that there are two unique characteristics of Information Theory. The first, which is not shared with any other field, is the fact that a single paper has sparked its creation. Truly all of it sprang from that 1948 paper that shook the world like an earthquake. Since then, there have been numerous "aftershocks", created by Shannon's disciples, that linger on and on as the Field keeps its vibrancy and allure. But the Richter scale levels of these aftershocks are at best an order of magnitude separated from the level of that first blast.

The second characteristic that sets Information Theory apart is its intellectual beauty. This beauty is measured on an abstract scale of scientific aesthetics that is difficult to describe. Perhaps an indirect way to partially describe it is that many of the contributions to the Field share a puzzling similarity. They appear as puzzles, or toy problems, that seem to have no relationship to engineering practice. And yet, quite often, unexpected relevance to applications springs up from them and radiates to the proverbial "real world".

It has already been 18 years since we celebrated the golden jubilee of the Field at the ISIT in Cambridge, MA. The "glow" of Information Theory remains unabated. What is the "magic" that appeals to so many of us? We have yet to articulate an authoritative state-

Anthony Ephremides



ment that explains that. Is it because this is the most "theoretical" of the Engineering disciplines? Is it because it is the most applicable branch of Mathematics? Is it because it has tentacles that reach out so effectively to multiple fields (like Physics, Statistics, Economics, and Biology)? Is it, perhaps, because its disciples are "narcissistic" and like to "love" themselves? Is it because it is elitist? It is really hard to say. But there is indeed something unique (like a secret code) that bonds Information Theorists to each other. Often we see in our Symposia and Transactions papers that are not in what we consider "mainstream" Information Theory. Good examples are papers from the areas of Signal Processing, or Networking, or even, Manufacturing. How do they find their way to Information Theory? First of all, if you look carefully at the list of subjects that our Society is "officially" interested in, you see that it is hugely broad. Almost anything that deals with "information" in any shape or form falls within its purview. But, beyond that, it is that mystique of scientific aesthetics that a contribution may or may not possess. It is the "angle" from which a problem is viewed. It is the approach that has a special appeal. It is that elusive and unique element of beauty. Often, I encourage colleagues from other fields to consider submitting their work to our forums, symposia, and journals. Typically they act surprised. "But what we do is not Information Theory", they say. And my response to them is that, yet, their work has Information-theoretic "style". It is that style that remains difficult to define or even describe.

But Information Theorists share some other aspects of working style. To quote Edwin Hubble (the renowned physicist of Hubble telescope fame), "a scientist must possess a healthy skepticism, a suspended

judgment, and a disciplined imagination". And Information Theorists often do possess these special characteristics. We must (and do) have skepticism about what we do or should do. Not only in judging the work of others but also our own. We must (and do) wait till we pass judgment on a piece of work. And we must (and do) let our minds race in unlimited blue sky, but with reins of reason attached.

So, Information Theory is special. But what is the prognosis of its future? How long will the trip last? As mentioned earlier, after the initial earthquake we have been experiencing the thrill of numerous aftershocks. But will there be some more major earthquakes? We do not know. But what we can say is that there are several areas where a new inspirational and powerful viewpoint is needed to cause an earthquake that will prolong significantly the life of our Field.

First of all, as Shannon himself has said, new ideas and techniques are needed to extend the Information theoretic grip to large networks. I would add that what is needed for a true breakthrough in Networking is a brilliant and "different" way of looking at net-

works that will have true "Shannonian proportions". We do not have that at the moment. But beyond that, there is room for possible earthquakes in other fields in which Information Theory in its traditional approaches has encountered brick walls and impenetrable boundaries. The areas of Inference and Sampling are two examples where, as in Networking, we are convinced that Information Theory has an intrinsic thread that ties them together. But we will need, as in Networking, a new "big bang" of an idea to make the "gold" begin to flow in these fields as well. And, of course, there is more. Computing, Biology, and Physics are additional examples.

As we carry on, especially during this year of celebration, we should remind ourselves that like the magma in the earth's guts that is brewing and pushing until it finds the outlet from which to erupt, as we busily study our favorite problems, there may be little "Shannons" amongst us who are silently pushing the envelopes of confinement until they come up with their own explosive, breakthrough ideas that will breathe additional life into the future of Information Theory.

Students' Corner

As you all know, April 30th, 2016, marked the hundredth anniversary of Claude Shannon's birthday. This year is hence referred to as the "Shannon Centenary," and there are a number of exciting events throughout the year which illustrate the importance of Shannon's contributions to electrical engineering and computer science in general, and to information theory in particular. (A list of these events is available at <http://www.itsoc.org/resources/Shannon-Centenary>)

Thus I'm very happy to announce that for the current issue, we have two contributions informing us about these events. The first one is by Onur Günlü, a doctoral candidate at the Technical University of Munich. Onur wrote a report on the two-day event held at the Heinz Nixdorf Museum in Paderborn from May 3-4, 2016. The second is by Jennifer Tang, a graduate student at MIT. Jennifer wrote about her experiences at the Bell Lab and Nokia's "First Shannon Conference on the future of the Information Age" in Murray Hill, New Jersey from April 28 to 29, 2016, where she won first place in the Shannon Centennial Student Competition. I really enjoyed reading these reports and I'm sure you'll enjoy them as much as I did!

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

Parham Noorzad

Celebrating Shannon's 100th Birthday in Paderborn

By Onur Günlü (onur.gunlu@tum.de)

Claude Elwood Shannon would be 100 years old today, and probably still juggling better than most of us. There were many events all over the world to celebrate the 100th birthday of our hero, and I would like to share my experiences from the special event held in early May at the Heinz Nixdorf Museum in Paderborn.

As a doctoral candidate at the Technical University of Munich (TUM), where I work mainly on information-theoretic security, I



was excited to hear that our institute, together with Han Vinck, was organizing a birthday party for Shannon with spectacular speakers. What I expected from this event was to learn whether cryptography came before communications or vice versa. The answer is: communications was first.

The two days of celebration began with a bus ride from Munich to Paderborn with several bachelor's and master's degree students from TUM, as well as doctoral candidates and professors. Once we reached the youth hostel, the doctoral candidates, with a sense of responsibility, made sure that the students ate healthy food by going to an Italian restaurant and then a bar in the old town.

The Shannon event started with a welcome speech by the president of the Heinz Nixdorf Museum, which is the largest computer museum in the world. The talks were amazing and I would like to mention three of them. Guiseppe Durisi showed juggling photos from the 2016 European School of Information Theory. The photos demonstrated that young information theorists have much to learn from Shannon. Second, a unanimous student opinion was that Emre Telatar gave a spectacular talk on Shannon's masterpiece "A Mathematical Theory of Communication". The applause was long-lasting. Finally, Sergio Verdú gave a passionate and in-

spiring talk on Shannon's life. Perhaps such exciting stories should be relayed to our colleagues in other research areas to advertise information theory.

I would like to add that we enjoyed playing with Shannon's "Useless Machine" at the celebration dinner, as shown in the attached picture. I hope that young scientists can attend inspiring events like this more frequently in the future, as they help to trigger curiosity about research. Happy birthday, Claude Shannon, and thank you for making us look smart even when we play with your Useless Machine!

Information Theory in the Broadest Sense

By Jennifer Tang (jstang@mit.edu)

Suppose you have a bipartite graph with the left-side nodes represented by circles and the right-side nodes represented by squares. You want to know which bipartite graphs have the following property: for every coloring of the circles, there exists a coloring of the squares, so that each circle has t or more neighbors with the same color as itself.

This describes the central question of my research. And yes, I do mean my *information theory* research. When I explain this project, I sometimes get asked why my research is considered information theory, since there are no channels, no coding, and not even bits involved. My answer to their question is this: Information theory is constantly reinventing itself and extending its range of applications. What started with entropy and point-to-point coding has expanded to a diverse array of problems in security, distributed storage, DNA and much more.

My graph theory problem is an example of this expansion. It began by studying how we can use insights from IT about adding redundancy to information to see if there are strategic ways we can implement redundancy for objects such as gates in a circuit or look-up tables. This led to the discovery of a class of designs with the best resource usage tradeoffs that turn out also to have desirable properties for practical implementation. We were able to characterize the fundamental limits of the achievable region of these redundancy designs, similar in flavor to how IT has defined achievable regions for many communication problems.

I submitted this project to the Shannon Centennial Student Competition and the researchers at Bell Labs determined my work was indeed novel and interesting enough to be chosen as a finalist. Thus, I had the opportunity to present my work at the centennial event to a wide audience of researchers, among whom were many IT luminaries. With a great amount of luck, my work was selected to be the first place winner of the Shannon Centennial Student Award.

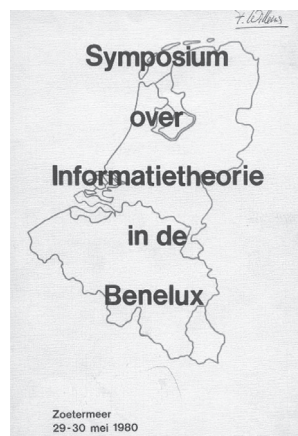
The experience allowed me to see how my research was a part of a program with a number of presentations demonstrating the broad reach of Shannon's ideas. Many of the technical projects were a step outside the normal boundaries, discussing topics like optics, economics, community detection, storing information in DNA and sequencing DNA. My takeaway is that celebrating one hundred years of Shannon is not just about the field he branched but also about the flexibility of the thinking that emerged from his ideas. Despite the fact that my research did not once (yet) mention mutual information, the IT society embraced it anyways. I find this to be pretty cool.

From the Field: 2016 Chapter of the Year Award for the Benelux IT Chapter

In Barcelona, at the 2016 ISIT, the IEEE Benelux Chapter on Information Theory received the 2016 Chapter of the Year Award. The present newsletter item describes the history and some recent activities of the Benelux IT Chapter.

Chapter History

In 1980 the first "Symposium over Informatietheorie in de Benelux" was organised in Zoetermeer, The Netherlands. Four years later the "Werkgemeenschap voor Informatie- en Communicatie theorie in de Benelux" was established by its founding fathers profs. Ijsbrand Boxma (Technische Hogeschool Delft), Willem Gröneveld (Technische Hogeschool Twente), Edward van der Meulen (Katholieke Universiteit Leuven), and Piet Schalkwijk (Technische Hogeschool Eindhoven). In 1990 its IEEE counterpart, the "IEEE Benelux Chapter on Information Theory" became active. Edward van der Meulen founded the Chapter and was the first Chair.

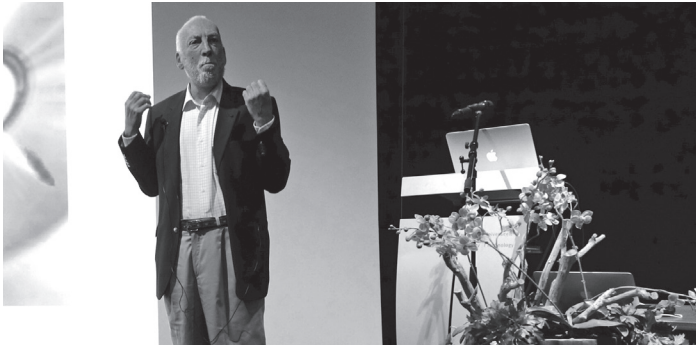


Regular Chapter Activities

The main activity of the Benelux IT Chapter and Werkgemeenschap is an annual two-day symposium which in 2015, took place on May 6–7, at the Université Libre de Bruxelles, Brussels. There were two invited lectures at this "36th WIC Symposium on Information Theory in The Benelux". The number of participants was roughly 40. Two students received an award, Nanang Susyanto for the best paper, and Giel Op 't Veld for the best presentation. The 37th Benelux Symposium on Information Theory was held on May 19–20, 2016, at the Université Catholique de Louvain, Louvain-la-Neuve, Belgium.

The Benelux IT Chapter, together with the Werkgemeenschap, organises every year a Midwinter meeting which focuses on a broad audience. On Feb. 1st, 2016, the topic of the meeting was: "Big Data and Data Analytics". Venue was Eindhoven University of Technology. The program included six invited lectures and there were roughly 80 registered participants.

Typically in the fall the Chapter organises the Van Der Meulen Seminar, on a special topic within Information Theory. Although it was initially scheduled earlier, the 6th Van der Meulen Seminar will be held on September 15, 2016. The topic of the 2016 seminar is "Information Theory and Fiber-Optical Communication". Lectures will be given by Georg Boecherer, Stephan ten Brink, and Gerhard Kramer.



Extra Chapter Activities

In addition to its regular activities, the Benelux IT Chapter organised the 2015 European School of Information Theory in Zandvoort, The Netherlands, from April 20 to 24. Zandvoort is located close to Amsterdam on the North Sea coast. The school hosted 112 participants, including 89 young researchers, in particular PhD students and a number of PostDocs and MSc students. There were six 3-hour tutorials scheduled that were delivered by distinguished speakers. The students presented their own research during one of the three poster sessions. Moreover at ESIT 2015 there were three shorter lectures scheduled that were focusing on applications and entrepreneurial aspects of Information Theory.

An extensive report on the 2015 European school can be found in the September 2015 Newsletter of the Information Theory Society.

On April 13, 2016, the Benelux IT Chapter organised a Symposium celebrating Shannon's 100th birthday. The symposium featured five invited lectures zooming in on innovations inspired by Shannon's ideas, with connections to the Benelux. The lectures were focusing on a broad audience, especially on students. Lecturers were Joan Daemen and Vincent Rijmen (inventors of the Advanced Encryption Standard), Jaap Haartsen (Bluetooth inventor), and Kees Immink (a Philips compact disc inventor, photo on left). Wolter Lemstra described the development of WiFi, which started in the Netherlands, and Jan van der Meer discussed MPEG standardisation, for which he received an Emmy Award. The venue was Eindhoven University of Technology. There were approximately 50 participants.

Website

The webpages of the Benelux IT Chapter were recently brought over to <http://www.itsoc.org/people/chapters/benelux-chapter>. The pages are still under construction.

*Jasper Goseling,
Vincent Rijmen,
Jos Weber,
Frans Willems, and
Peter de With.*

From the Editor *continued from page 2*

Hong Kong; the University of Balamand, Lebanon; UCLA; Ottawa, Canada; the University Ss Cyril and Methodius in Skopje, Republic of Macedonia; the Catholic Institute of Business and Technology in Accra, Ghana; Singapore; and Tarbiat Modares University, Iran. The festivity continues with more events to come and with a collection of fun birthday brainteasers prepared by Aziz Inan in his article "A Numerical Tribute to Claude Shannon".

With sadness, we conclude this issue with tributes to two pillars of the engineering community, Solomon W. Golomb who passed away on May 1st and Rudolf Emil Kalman who passed away on July 2nd. Thanks to Guang Gong, Tor Helleseth, Vijay Kumar, Urbashi Mitra, and Benjamin Paul; and to Tryphon Georgiou, Andrew Kalman, and Pramod Khargonekar for preparing the tributes.

Beyond his extraordinary scholarly contributions, Sol Golomb was a long time newsletter contributor enlightening us all, young and old, with his beautiful puzzles. This issue includes the solution to his final puzzle "Latin Squares". In honor of Sol's immense contribution to the newsletter, a collection of his earlier puzzles dated back to 2001 will appear in 4 compiled parts over the next 4 issues. He will be greatly missed.

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 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:

Oct 10, 2016 for the issue of December 2016.

Jan 10, 2016 for the issue of March 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*

Report on the Munich Workshop on Causal Inference and Information Theory (MCI 2016)

Organizers:

Negar Kiyavash, Gerhard Kramer, Kun Zhang, Bernhard C. Geiger, and Jalal Etesami

The Institute for Communications Engineering (LNT) at the Technical University of Munich (TUM) organized the Munich Workshop on Causal Inference and Information Theory on May 23–24, 2016. The workshop brought together experts from across the world and various scientific disciplines: philosophy (Frederick Eberhardt, Kun Zhang), computer science (Elias Bareinboim), industrial engineering (Christopher Quinn), economics (Michael Eichler), mathematics and statistics (Thomas S. Richardson, Shohei Shimizu), physics (Dominik Janzing), and information theory (Young-Han Kim, Negar Kiyavash, Haim Permuter). The talks ranged over equally diverse approaches to inference of causal

structures: including inference in the presence of confounders or time varying networks and the application of information-theoretic measures such as directed information and Kolmogorov complexity for the inference task. Each workshop day was concluded by a discussion session for the researchers to brainstorm.

The Munich weather cooperated: the constant rain made everyone happy to stay inside, enjoy hot coffee, and continue working. The social program included a pizza lunch and a beer hall, rather than beer garden, event.

The workshop was funded by the TUM Chair for Communications Engineering and the Alexander von Humboldt Foundation. The program, abstracts and speaker biographies, and photos are available at: <https://www.lnt.ei.tum.de/en/events/munich-workshop-on-causal-inference-and-information-theory2016/>

Report on the Bertinoro Workshop on Communications and Coding (BCC 2016)

Organizers:

Enrico Paolini, Roy Timo, and Gerhard Kramer

On the 19th and 20th of May 2016, the Department of Electrical, Electronic, and Information Engineering ‘Guglielmo Marconi’ at the University of Bologna and the Chair for Communications Engineering of the Technical University of Munich organized a Bertinoro Workshop on Communications and Coding (BCC) in Bertinoro, Italy. The workshop venue was the beautiful and historic Centro Residenziale Universitario di Bertinoro. The main purpose of the workshop was to bring together researchers from European institutions to explore topics of information theory and coding. The event further provided a test run for an upcoming IEEE European School of Information Theory bid, and, by all accounts, it was a great success.

The workshop’s technical program included a variety of talks on communications, multi-user information theory, error-control coding and compressive sensing. Participants included:

- Marco Chiani, Ahmed Elzanaty, Andrea Giorgetti, Anna Guerra, Enrico Paolini, Gianni Pasolini (University of Bologna)
- Georg Böcherer, Gerhard Kramer, Roy Timo, Youlong Wu (TUM)
- Luca Barletta (Politecnico di Milano)

- Alexandre Graell i Amat (Chalmers University)
- Gianluigi Liva (DLR, German Aerospace Center)

BCC was funded by the Department of Electrical, Electronic, and Information Engineering ‘Guglielmo Marconi’ of the University of Bologna and by the Alexander von Humboldt Foundation.

The technical program and photos are available at the web address <https://www.lnt.ei.tum.de/en/events/bertinoro-workshop-on-communications-and-coding-2016/>



Luca Barletta, Gianluigi Liva, Gerhard Kramer, Georg Böcherer, Youlong Wu, and the beautiful sight towards the Adriatic Sea from the Bertinoro Castle.

Report on Two Major Events on Information Theory in South Africa

by Han Vinck

Two major events on Information Theory in South Africa, organized by the Center for Telecommunications, University of Johannesburg, at the Protea Hotel Kruger Gate, Skukuza, Kruger National Park from 16 to 21 August, 2015.

The **first IEEE Seminar on Future Directions in Information Theory and Communications** was organized by the Center for Telecommunications, University of Johannesburg, at the Kruger National Park from 16 to 21 August, 2015. Internationally acclaimed researchers in Information Theory and Communications were invited to present seminars. Invited Speakers included: Jeff Andrews, University of Texas at Austin, USA and Chair Future Directions Committee, IEEE Information Theory Society (A Perspective on Future Directions in Information Theory Research); Andrew Jiang (Exploring New Coding Theories for Data Storage); Frans Willems (Combining the Burrows Wheeler Transform and the Context-Tree Weighting Algorithm); Emanuele Viterbo (Lattice Index Coding: An Efficient ARQ Scheme for Wireless Broadcasting); Tadashi Wadayama (Coding and Combinatorial Optimization) and Hirosuke Yamamoto (Efficient Identification Coding Schemes for Multiple Objects).

The organizing committee consisted of the chair: Hendrik C. Ferreira (University of Johannesburg) and the TPC Co-chairs: A. J. Han Vinck (University of Duisburg-Essen) and Hiroyoshi Morita (The University of Electro-Communications)

This event was held in parallel with the 2nd African Winter School on Information Theory and Communications. The goal of holding the two events in parallel is to stimulate interest in Information Theory amongst young academics and researchers as well as to increase cooperation and knowledge sharing between leading international researchers, African students and universities.

The **2nd African Winter School on Information Theory and Communications** was held at the Kruger National Park from 16 to 21 August, 2015. The goal of the African winter school is to increase cooperation and knowledge sharing between African students and universities. Doctoral students and young staff



Participants at the event

members from Africa and other continents presented their ongoing research. Invited speakers at this event included: Jian Song, Tsinghua University, P. R. China, Yuan Luo, Shanghai Jiao Tong University, P. R. China, Jos H. Weber, Delft University of Technology, The Netherlands; Ivan Fair, University of Alberta, Canada; Bella Bose, Oregon State University, USA; Luca Tallini, University of Teramo, Italy; and Fisseha Mekuria, C.S.I.R., South Africa. The Conference Co-Chairs were Theo Swart (University of Johannesburg) and Ling Cheng (University of the Witwatersrand). The TPC Co-chairs were Jos H. Weber (Delft University of Technology); Ulrich Speidel (The University of Auckland) and Ivan Fair (University of Alberta).

The local arrangements committee consisted of Wendy Smith (University of Johannesburg); Allan Emleh (University of Johannesburg) and Lucia Pelsler (University of Johannesburg)

Both events were sponsored by the University of Johannesburg and the IEEE Information Theory Society. The social program included guide tours through the Kruger Park and a traditional evening with tribal dances and an original South African "Braai".

More information can be found on the website of the Center for Telecommunications, <http://telecoms.uj.ac.za/ieee-2015-kruger/>

Report on International Conference on Information Geometry and its Applications IV

Nihat Ay, Paolo Gibilisco and František Matúš

Institute of Information Theory and Automation of the Czech Academy of Sciences organized the International Conference on Information Geometry and its Applications IV on June 12–17, 2016 (<http://igaia.utia.cz>). Information geometry is a quickly growing field which has attracted many scientists from mathematics, physics, neuroscience, cognitive systems, robotics, and machine

learning. The aim was to highlight recent developments within the field and to identify new directions of research.

The conference honored the numerous scientific achievements of Shun-ichi Amari on the occasion of his 80th birthday. The programme committee consisted of Nihat Ay, Paolo Gibilisco and František

Matúš, representing the three sponsoring institutions: Max Planck Institute for Mathematics in the Sciences, Leipzig, Institute of Information Theory and Automation of the Czech Academy of Sciences, and Department of Economics and Finance, Università di Roma Tor Vergata. The event took place in Liblice Castle, Czech Republic, one of the most compact monuments of the Bohemian high Baroque.

Almost sixty participants enjoyed during the week 24 invited lectures, each lasting 50 minutes. Various topics of the field were covered, both theoretical, like foundational geometric structures for information geometry, non-commutative information geometry and statistical inference, and application-oriented, like neural networks, computational and systems biology, mathematical finance, statistical mechanics, quantum information and statistics, and applications to statistical modeling. The list of speakers features most prominent personalities: Shun-ichi Amari, Roman Belavkin, Michel Broniatowski, Imre Csiszar, Shinto Eguchi, Kenji Fukumizu, Davide Girolami, Peter Harremos, Frank Hansen, Shiro Ikeda, Jürgen Jost, Hông Vân Lê, Shunlong Luo, Hiroshi Matsuzoe, Peter Michor, Gerard Misiolek, Guido Montúfar, Hiroshi Nagaoka, Nigel J. Newton, Felix Otto, Giovanni Pistone, Lorenz Schwachhöfer, Flemming Topsøe, and Sumio Watanabe. The poster session consisted of 25 contributions.



The conference programme included a visit of Castle Kokořín and hike in surrounding picturesque landscape formed by various bizarre sandstone rocks, crystal-clear lakes and deep forests.

Thanks go to Václav Kratochvíl for his terrific work with the local organization, and to Antje Vandenberg who managed all the administrative work in Leipzig.

Report on 2016 European School of Information Theory

Fredrik Brännström, Giuseppe Durisi, and Alexandre Graell i Amat

The 2016 edition of the European School of Information Theory (ESIT) was held at Chalmers University of Technology, Gothenburg, Sweden, on April 4–8, 2016. The school was attended by 96 researchers, including 68 students. As in previous editions of ESIT, the school featured six tutorial presentations of three hours each, given by six experts in various fields of information theory. The areas covered this year were lattice index codes, distributed storage systems, fiber-optical systems, modern coding theory, secrecy and stealth, and non-asymptotic Shannon theory.



September 2016

There were two poster sessions, which gave students the opportunity to present their work and interact with fellow students and senior researchers.

The participants came from 16 different countries. Sweden, Germany, and the United Kingdom were the most represented ones. The trip to Sweden was definitely worth it, since the attendees were treated to six terrific tutorials. Emanuele Viterbo opened the school on Monday morning by explaining how to benefit from the



IEEE Information Theory Society Newsletter



availability of side information at the physical layer using lattice index codes. He was followed in the afternoon by Frank R. Kschischang, who gave us a comprehensive introduction to the field of digital communications over optical fibers. Tuesday's tutorial was given by Vijay Kumar and was focused on error correction for distributed storage. On Wednesday, Henry Pfister brought us from the origin of coding theory all the way to spatially-coupled codes, and then back again to the fifties. Thursday's tutorial was given by Gerhard Kramer, who guided us through the fascinating area of secrecy, stealth, and privacy for noisy channels and identifiers. Yury Polyanskiy was Friday's tutorial lecturer. He taught us how to obtain finite-blocklength information-theoretic bounds in source and channel coding.

On Wednesday afternoon, we visited Ericsson Research facilities on the beautiful Göta älv river in Gothenburg. Highlights of the visit included an overview on next generation wireless cellular

networks (5G) and a demonstration of a complete wireless cellular infrastructure.

On Thursday, we celebrated the hundredth anniversary of Claude Elwood Shannon's birth with a panel discussion moderated by Chalmers' professor Erik Ström. The panelist members were Erik Agrell, Tobias Koch, Gerhard Kramer, and Michael Lentmaier. The panel discussion was followed by a surprisingly addictive juggling activity, which was performed with specially designed juggling balls. The social program involved a welcome reception on Monday, which was kindly offered by the city of Gothenburg, and a banquet on Thursday night.

As with its previous editions, the school provided a unique opportunity for students to learn, interact, and network in an informal environment. We are grateful to the guest lecturers for accepting our invitation and for delivering such inspiring presentations. Many thanks must also go to our local student helpers, Sven Jacobsson, Alireza Sheikh, and Johan Östman, who helped enormously with the local arrangement, and to Gerhard Kramer (the soul of ESIT), who supported us in his advisory function.

We are grateful to our financial sponsors Ericsson, Chalmers University of Technology, IEEE Information Theory Society, and the City of Gothenburg. Without their generous support we would not have been able to run this event.

The preparations for ESIT 2017 in Madrid, Spain, are already ongoing. We are looking forward to next year's event.

The 2016 International Zurich Seminar on Communications

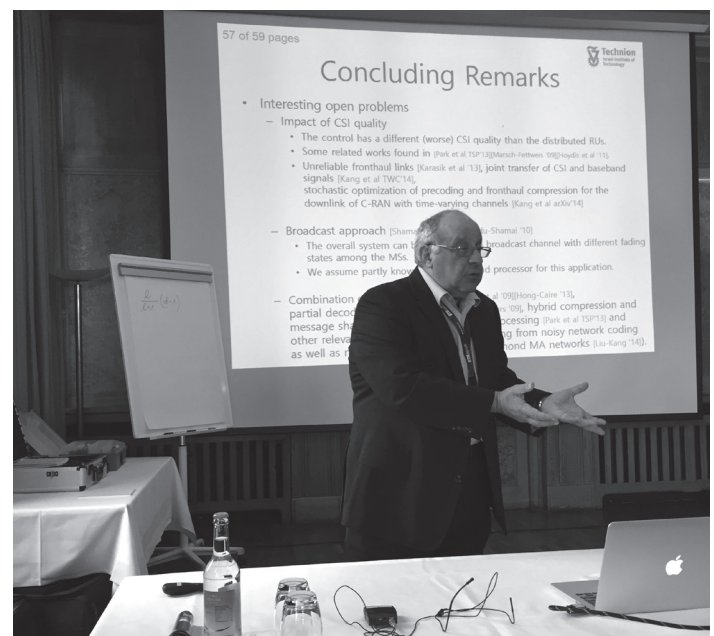
Amos Lapidoth and Stefan M. Moser

Notwithstanding its name, the International Zurich Seminar on Communications (IZS) is not exclusively about communications. With roughly half the sessions being invited, IZS strives to keep abreast of the latest developments in our field.

The conference is a single-track biennial conference, where speakers are encouraged to teach rather than impress. This year's IZS was the twenty-fourth. It was held March 2–4, 2016, at the Hotel Zürichberg overlooking Zurich, and was organized by the IEEE Switzerland Chapter on Digital Communication Systems in collaboration with ETH Zurich.

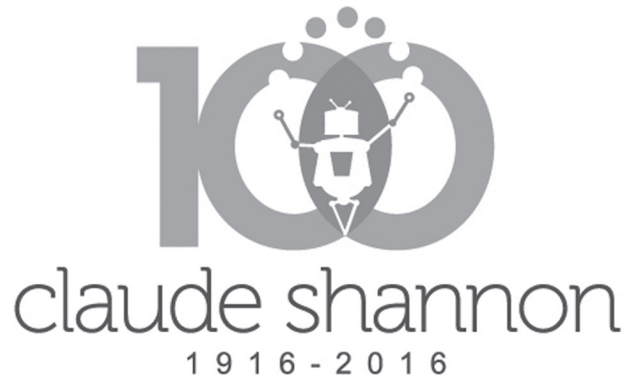
This IZS boasted three superb plenary presentations: Prof. Martin Bossert talked about decoding Reed-Solomon codes beyond half the minimum distance, Prof. Shlomo Shamai gave an information theoretic view of fronthaul-constrained cloud radio access networks, and Prof. Prakash Narayan lectured on common randomness, querying and large probability sets. The detailed program and the proceedings can be found online at the web address <http://www.izs.ethz.ch/>

At the next IZS, which is slated for the winter of 2018, we plan to celebrate its jubilee. Stay tuned!



Shlomo Shamai at his plenary talk

Shannon Centenary Workshop and Celebration Reports



Celebration of Claude Shannon's Centennial Birthday at Bell Labs

Bell Labs, Nokia, celebrated the anniversary of Claude Shannon's 100th birthday at its historic site in Murray Hill, New Jersey, on April 28–29, 2016. The two-day event was entitled the "First Shannon Conference on the Future of the Information Age" and celebrated the critical role that Shannon's information theory has played in advancing the 20th century industrial society to our progressively more information-based economy through digital computing, digital transmission and digital storage, Fig. 1.

After a metaphorical 'turning on' of the innovation engine at Bell Labs (Fig. 2), Marcus Weldon, Bell Labs president, welcomed the more than 250 attendees to the two-day celebration and put in focus the rationale for the henceforth annual event with a broad focus for Day 1 (April 28) on topics related to the unfolding information society and for Day 2 on topics related to information theory and its application.

The talks and the fire-side chat that followed on April 28th not only brought together some of Claude Shannon's top students, collaborators and colleagues – Robert Gallager (MIT), Elwin Ber-

lekamp (UC Berkeley), Leonard Kleinrock (UCLA) and Yakov Sinai (Princeton) – who recounted their experiences and encounters with Claude Shannon, but also included a perceptive and fresh perspective on Shannon's life and work by Sergio Verdú (Princeton), as well as perspectives on the information society by Irwin Jacobs (Founding Chairman and CEO Emeritus of Qualcomm), Eric Schmidt (Executive Chairman of Alphabet Inc. and its holding companies including Google Inc.), Robert Metcalfe (Internet Pioneer credited for inventing Ethernet), Henry Markram (Professor of Neuroscience at the Swiss Federal Institute for Technology – EPFL – and Amber Case (Cyborg Anthropologist). Day 1 program was concluded by a Student Competition with focus on 'Information Theory and Its Application'. Four students made it to finalists from over 40 submissions (<https://www.bell-labs.com/programs/shannon-conference/student-competition/>): Santhosh Kumar and Marco Mondelli, "Capacity via Symmetry", Navid Naderializadeh, "Spectrum sharing in D2D networks", Jennifer Tang, "Redundancy, but not for Information", Min Ye, "Explicit constructions of high-rate regenerating codes". Tang won 1st place, followed by Kumar and Mondelli in the 2nd place and Na-



Figure 1. Bell Labs president unveiling of the Shannon plaque and the IEEE Milestone dedication.



Figure 2. Marcus Weldon, Bell Labs president, turning on the metaphorical 'innovation' switch.

deralizadeh in the 3rd (Ye was unable to attend the final stage of the competition on April 28th). Day 1 was concluded with a gala dinner, an award ceremony for the student competition and an artistic performance of the Human Digital Orchestra™ and Shannon Effect jointly developed by Bell Labs and Stevens Institute of Technology.

The topic of Day 2 (April 29th) was Shannon's information theory and the talks and the concluding panel discussion gradually broadened focus from Shannon's original theory impressively summarized jointly by Vincent Poor (Princeton) and Michelle Effros (Caltech), followed by an overview by Shlomo Shamai (Technion), network coding by Muriel Médard (MIT), optical communication by René Essiambre (Bell Labs), biology by Olga Milenkovic (UIUC), genetics by David Tse (Stanford), economics by Christopher Sims (Princeton), and social network analysis by Emmanuel Abbe (Princeton). The concluding panel discussion led by Tom Marzetta with former Bell Labs researchers Gerhard Kramer (TUM), Emre Telatar (EPFL), Andrea Goldsmith (Stanford), Rüdiger Urbanke (EPFL), and Alon Orlitsky (UCSD) ex-

plored possible directions of information theory in the next few decades.

A web exhibit of selected original versions of Claude Shannon's pre-publication papers and related work at the Bell Labs Math Center into which Shannon was hired in 1941 (through 1957) can be viewed on <https://www.bell-labs.com/claude-shannon/>.

An apt and memorable summary of the two-day event in the context of Shannon's 1948 seminal paper was suggested by Sergio Verdú (Princeton) at the end of the event, "What Jerusalem is to the People of the Book, Murray Hill is to the People of the Article."

*Iraj Saniee
Head
Math & Algorithms Research Group
Bell Labs, Nokia
Murray Hill,
NJ 07974
July 14th, 2016*

Photos from the IEEE Shannon Dedication event that took place at MIT on May 17, 2016.

The event was well attended by IEEE and MIT including President Rafael Reif, Provost Martin Schmidt and both of Claude Shannon's children.



Standing at the plaque which is located on MIT campus outside the elevators on the 4th floor in the Fairchild Building (Bldg 36). This location is between RLE Headquarters and EECS Headquarters where Shannon spent a great deal of time. From left to right - distinguished guests: Provost Martin Schmidt, Claude Shannon's children: Andrew Shannon and Peggy Shannon, IEEE President Dr. Barry Shoop.



Unveiling of the IEEE plaque was done by Provost Martin Schmidt and IEEE President, Dr. Barry Shoop.



A special talk in the Boole-Shannon Lecture Series (the series was hosted by Prof. Muriel Medard and Prof. Richard Milner) was delivered by the distinguished information theorist and Shannon expert, Prof. Sergio Verdú of Princeton University. The beginning of his talk included the life and work of Claude Shannon in great detail.

Report on a Claude Shannon 100th Birthday Celebration at the Heinz Nixdorf Museum in Paderborn, Germany, May 3–4, 2016

Organizers:

Han Vinck, Lars Palzer, and Gerhard Kramer, German Information Theory Society Section Chapter

The German Information Theory Society Section Chapter, together with Prof. Han Vinck and the Institute for Communications Engineering (LNT), organized a Claude Elwood Shannon 100th Birthday Celebration at the Heinz Nixdorf Museum in Paderborn, Germany, on May 3–4, 2016. The technical program included 15 talks on Shannon's life and work. The speakers on May 3 were Frans Willems, Ingo Althöfer, Christof Paar, Jochen Viehoff, Vijay Bhargava, Kees Immink, Rudolf Mathar, Holger Boche, and Stephan ten Brink. The speakers on May 4 were Giuseppe Caire, Petar Popovski, Giuseppe Durisi, Emre Telatar, Joachim Hagenauer, and Sergio Verdú. The technical talks addressed multi-user and quantum information theory, genetics, chess, cryptography, and code design. Two of the talks had a more personal flavor: Emre Telatar's talk on Shannon's 1948 paper and Sergio Verdú's presentation on the life of Shannon. Over 70 persons attended the event, including 30 undergraduate and graduate students.



Six past presidents of the IEEE Information Theory Society celebrating Claude Shannon's work and life in Paderborn, Germany, on May 3

The social program on May 3 included a tour of the Heinz Nixdorf Museum, a reception, a dinner, and a football match. Funding for the workshop was provided by the LNT. The program and photos are available at the web address <http://www.lnt.ei.tum.de/en/events/claude-elwood-shannons-100th-birthday-celebration/>

Workshop on Core and Frontier of Information Theory, Hefei, China, June 11–12, 2016

Wenyi Zhang

A mini-workshop on multiple aspects of information theory and its applications was held on June 11–12, 2016, in Hefei, China, organized by the Department of Electronic Engineering and Information Sciences, University of Science and Technology of China. The workshop aimed at promoting the research interest and activities on information theory in China, during the celebration of 100 years since the birth of Claude Shannon. Around fifty participants attended this workshop, and it featured a number of invited talks as follows:



On the complete monotonicity of Fisher information, by Yanlin Geng (ShanghaiTech University, China)

Many-user information theory, by Dongning Guo (Northwestern University, USA)

A randomized algorithm for the capacity of finite-state channels, by Guangyue Han (University of Hong Kong, Hong Kong SAR, China)

Compressing encrypted data: achieving optimality and strong secrecy via permutations, by Wei Kang (Southeast University, China)

An information-theoretic paradigm for data clustering, by Tie Liu (Texas A&M University, USA)

To prove or to disprove: information inequalities and sparse optimization, by Chee Wei Tan (City University of Hong Kong, Hong Kong SAR, China)

New codes and outer bounds for caching systems, by Chao Tian (University of Tennessee, Knoxville, USA)

Wireless signaling designs and performance guarantees based on results from number theory, by Zhengdao Wang (Iowa State University, USA)

Each speaker presented the material at length and in depth, followed by active discussions from the participants. More details of the workshop including the talk slides can be found at <http://staff.ustc.edu.cn/~wenyizha/workshop.html>.

Report on Shannon Day at IIT Madras

Shannon day was celebrated on June 3, 2016 at the Indian Institute of Technology (IIT) Madras as part of the Shannon centenary celebrations of the IEEE Information Theory Society. The event was aimed at high school students and a general audience. It was organised along with the RSIC, which is a summer residential program for high school students at IIT Madras. More than 150 participants attended the event.

The event began with introductory remarks by Prof. V. Balakrishnan (Physics, IIT Madras). This was followed by two presentations. The first was titled "Shannon and information theory – an audio-visual presentation" and was made by Prof. Andrew Thangaraj (EE, IIT Madras). The second was titled "Error correction and the Shannon blueprint" and was given by Prof. P. Vijay Kumar (ECE, IISc Bangalore). The event concluded with tea/snacks amidst posters of Shannon and his work.



Photos and videos from the event are available at this link: <https://drive.google.com/open?id=0B2XYA8bZ519cN1E5VGxYU3RDckU>

Andrew Thangaraj

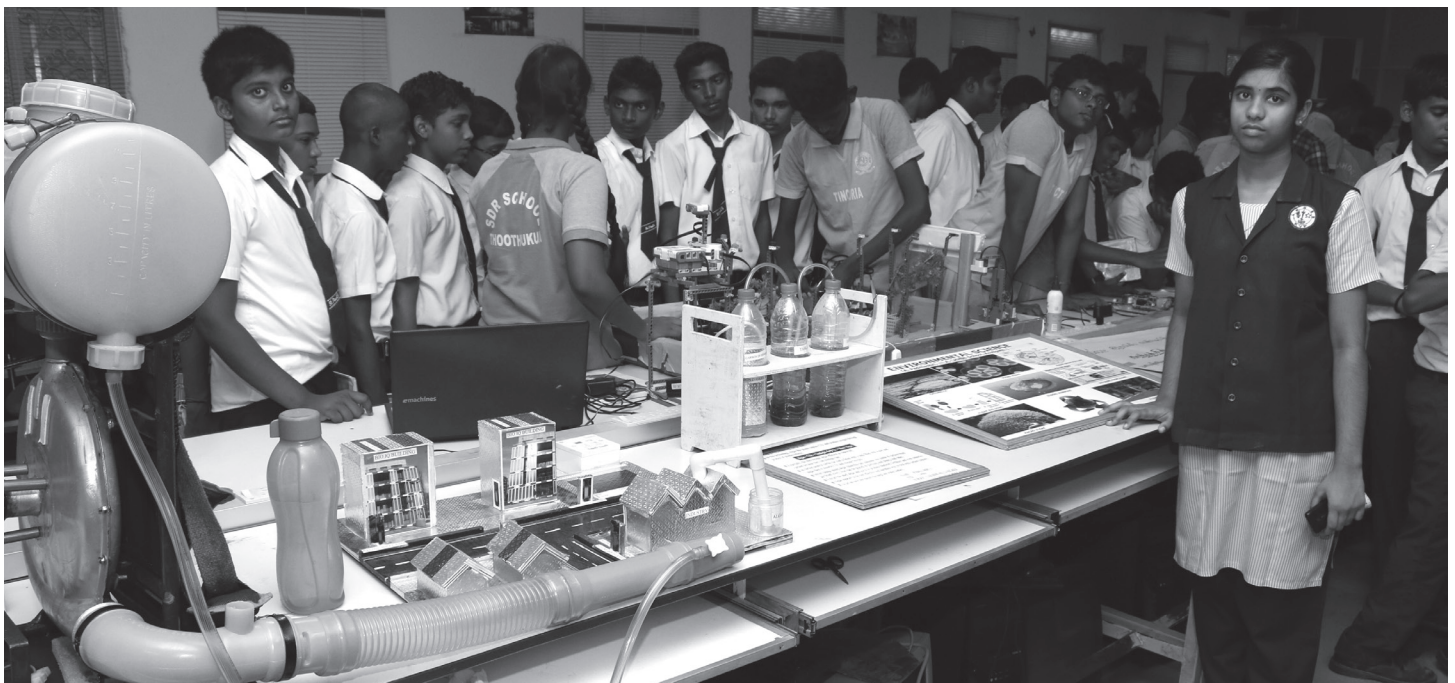
IEEE Information Theory Society Madras Chapter

Shannon Centennial Event – Two Day National Level Project Exhibition for School Students – PROEXPO'16 on 29-06-2016 to 30-06-2016

To celebrate **Cladue E Shannon's** 100th birthday anniversary on behalf of IEEE Information Theory Madras Chapter we have organized the two Day National Level Project Exhibition for School Students – PROEXPO'16 scheduled on 29-06-2016 to 30-06-2016 at National Engineering College, K.R.Nagar, Kovilpatti, Tuticorin, Tamilnadu, India. Chief Guest Mr Pradeep Nair, Head – Engineering Services, Sterlite Copper (A Unit of Vedanta Limited), Thoothukudi, Tamilnadu, India was the chief guest and the special guest Mr. B. Murali, Prof & Head, Dept of CS, PSG College of Arts and Science, Coimbatore, Tamilnadu, India were successfully inaugurated the project exhibition. Thiru. K.R. Arunachalam, Member, Managing Committee,

National Engineering College presides over the function in the august presence of Dr. Kn.K.S.K. Chockalingam, Director, National Engineering College and Dr.S. Shanmugavel, Principal, National Engineering College. 2400 school students (Exhibitors - 200, Visitors – 2200) visited the exhibition and gained a pleasant experience.

*With Kind Regards,
Dr.B.Paramasivan
Chairman-ITS
IEEE Madras Chapter*



Claude Shannon Centenary Celebration at Monash University

The Faculty of Information Technology at Monash University held its own Claude Shannon Centenary Celebration on Friday the 6th of May, 2016. The event consisted of a series of short talks outlining Shannon's work, followed by lunch.

The speakers, and their topics, included:

Professor Jamie Evans	The life and times of Claude Elwood Shannon
Mrs Shampa Shahriyar	How Claude Shannon's master thesis changed our world
Associate Professor Jonathan Keith	Shannon's PhD: An algebra for theoretical genetics
Associate Professor Michael Brand	What is information?
Dr Amin Sakzad	Lossless data compression: a practical example
Dr Yi Hong	Shannon's noisy-channel coding theorem
Dr Kevin Leckey	The fundamental theorem for noisy channels: Shannon's probabilistic proof
Dr Ron Steinfeld	Shannon and cryptography
Dr Reza Haffari	Prediction and entropy of printed English
Associate Professor David Dowe	Shannon's influence on machine learning
Associate Professor Alan Dorin	On automata and chess
Professor Graham Farr	Shannon's switching game
Dr Rebecca Robinson	The Shannon capacity of a graph
Dr Michael Wybrow	Theseus the maze-solving mouse
Associate Professor Burkard Polster	Juggling robots and theorems

The event was very well attended, with around 100 people arriving on the day, including 20 high school students from John Monash Science School, as well as staff and students from the Faculty of IT, the Maths Department and the Department of Electrical and Computer Systems Engineering at Monash.

Informative and enjoyable, the event was a fitting celebration of the significant impact Shannon had on our world.

For more information about Shannon and the Monash celebration, see the following webpage:

<http://www.infotech.monash.edu.au/about/news/archive/2016/shannon-centenary-celebrated-at-monash.html>

We also made the following short videos:

Short clip: <https://www.youtube.com/watch?v=upEUQfbYji0>

Full video: <https://youtu.be/6OnFKMViQMQ>

Professor Jamie Evans <https://youtu.be/lzTIJNiDgW8>
 Mrs Shampa Shahriyar <https://youtu.be/FcGQ4mMTPHI>
 Associate Professor Jonathan Keith <https://youtu.be/pwLdTllhSnA>
 Associate Professor Michael Brand https://youtu.be/zLI_4Hx5y44
 Dr Amin Sakzad <https://youtu.be/yxyx6P0qRwE>
 Dr Yi Hong <https://youtu.be/uXDyaE3epBY>
 Dr Kevin Leckey <https://youtu.be/iM3KuavVQB4>
 Dr Ron Steinfeld <https://youtu.be/rfTMFCRUQv4>
 Professor Graham Farr <https://youtu.be/7Y6fPh-5HJ0>
 Associate Professor David Dowe <https://youtu.be/agku-McFHEI>
 Associate Professor Alan Dorin <https://youtu.be/r9yAylFYZVc>
 Dr Rebecca Robinson <https://youtu.be/LQWh-Ezprqc>
 Dr Michael Wybrow <https://youtu.be/nZe3jHFSDT0>
 Associate Professor Burkard Polster <https://youtu.be/Ndu-nJdZOkU>

Organizers: Prof. Graham Farr and Dr. Amin Sakzad

Claude Shannon Centenary 2016 in Hong Kong

At the Chinese University of Hong Kong's Institute of Network Coding on 19 May 2016 and the Computer Science Challenge at the website <http://cschallenge.io> on 21 May 2016 with its robotic workshop on 30 April 2016 (Shannon Day) at the City University of Hong Kong

The Centenary Workshop was hosted by Prof. Raymond Yeung and consisted of various talks related to information theory with roughly 50 postgraduate students and researchers, with a separate Colloquium seminar on Quantum Information Theory by 2016 Shannon Lecturer Alex Holevo at the City University of Hong Kong. The CS Challenge and workshops are organised by Chee Wei Tan and are meant to reach out to primary and secondary school students with an interest in computer science and getting to know the pioneering work of Claude Shannon. Students learn to code robots to solve mazes and also play computer games to learn computational think-

ing skills and mathematics after watching Shannon's video displaying a myriad of "Game-playing Machines". Educational exhibits of Claude Shannon and his fun and thought-provoking robotic machine replicas such as Rubik Cube manipulators and Shannon's Rubik Cube poem were on display. Altogether 300 primary and secondary school students participated in the events. The educational exhibits and replicas of Shannon are on mobile rotational display at a number of middle schools in Hong Kong for the whole of 2016.

Chee Wei Tan

Knowledge, Information, Theory and Development

A tribute to Claude Shannon in his Centennial Report on April 27, 2016 Event at The University of Balamand, Lebanon

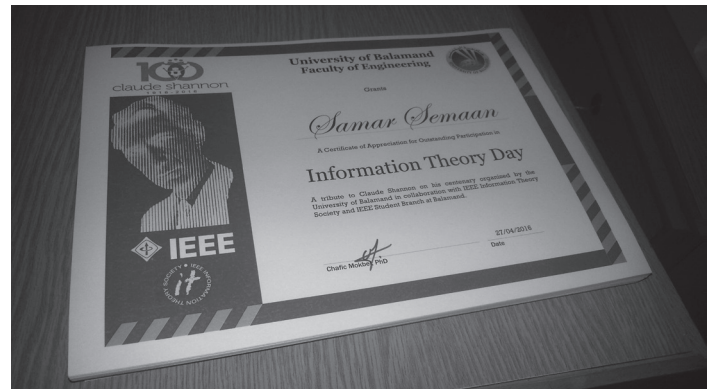
Within the global initiative launched by IEEE Information Theory Society, the University of Balamand commemorated Claude Shannon's centenary on 27 April 2016 in a one day event placed under the title "Knowledge, information, theory and development". More than seventy students from eight surrounding high schools actively participated in this event with their teachers. Several professors from the University and from other universities in Lebanon attended this event. After a welcome note by Vice President Najjar, several professors presented some of Shannon's major achievements highlighting their impact on today's world. The high school students then visited six thematic stands presented by the Information Theory course students. On the stands posters especially prepared for the event illustrated parts of Shannon's scientific productions. The stands also included demonstrators and a few games. After a break, the students were divided into twelve groups supervised by University students.



Six members from different high schools comprised each group. The groups participated in a competition prepared for the occasion. The competition included questions related to Shannon's statements and pathway but also some technical information theory problems. After the evaluation prizes were distributed to the first and second groups' members and certificates were distributed to all participants. All engaged in an excellent spirit and everyone left excited and curious to know more about the genius of Claude Shannon.

It is worth noting that the event was announced by local radio stations and one station dedicated a session where one University student was interviewed about Claude Shannon and how he shaped our knowledge and digital based society.

Chafic Mokbel



Shannon centennial at UCLA

UCLA held the Shannon centennial celebration on May 7th 2016. The event was organized with the participation of the UCLA IEEE students society. The event also featured a video presentation by Prof. Len Kleinrock, who was one of Shannon's students during his graduate studies. There were approximately 60–80 participants in the event, with people from UCLA, as well as various local high-schools visiting. The event featured presentations highlighting the modern influence of Shannon's work as well as demonstration of a self-driving model car, robotic mouse solving a maze as well as 3D printing. A 3D printed key-chain depicting Shannon juggling balls was given as a souvenir to the participants. A puzzle based on the posters presented was designed and the high-school students who completed it were given small prizes. The material, including Kleinrock's video, were shared with the wider Shannon centennial community. The event was jointly sponsored by the IEEE IT society, the department of Electrical Engineering at UCLA as well as the Henry Samueli School of Engineering and Applied Sciences at UCLA.

<http://www.ee.ucla.edu/events/ucla-claude-shannon-centennial-celebration-may-7-2016/>
<http://www.ee.ucla.edu/shannon-centennial/>

Suhas Diggavi



Prof. Fragouli and a middle school student watching a micromouse traverse the maze

Report on Claude Shannon Centenary 2016 Ottawa

In the capital of Canada, a series of Shannon centenary events, Claude Shannon Centenary 2016 Ottawa, was organized jointly by the Canadian Society of Information Theory and the University of Ottawa. On April 15, a mini-conference was held on the campus of the University of Ottawa. Dr Andrew Eckford, a professor at York University and the President of the Canadian Society of Information Theory, gave the opening speech reflecting on the history of communications and information theory in Canada. Six plenary lectures were given by Dr Carlisle Adams (University of Ottawa), Dr Andrew Eckford (York University), Dr Diana Inkpen (University of Ottawa), Dr John Lodge (Communications Research Centre Canada), Dr En-Hui Yang (University of Waterloo), and Dr Halim Yanikomeroglu (Carleton University) on topics in communications, information theory, security and artificial intelligence. On April 23 and April 30, and throughout the month of May, poster exhibitions introducing Shannon and the fields that Shannon impacted were displayed in Indigo Bookstore Barrhaven, Place d'Orleans Shopping Center, and Ottawa Public Library respectively. In these exhibitions reaching out to the general public, student volunteers hosted the "twenty questions" games with prizes. Claude Shannon Centenary 2016 Ottawa was led by Professor Yongyi Mao at the University of Ottawa.

Yongyi Mao



Shannon Day at the Faculty of Electrical Engineering and Information Technologies, University Ss. Cyril and Methodius in Skopje, Republic of Macedonia.

The IEEE Republic of Macedonia Information Theory Chapter, the IEEE Republic of Macedonia Section and the Faculty of Electrical Engineering and Information Technologies (FEEIT) at the University Ss. Cyril and Methodius in Skopje, Republic of Macedonia, organized a Shannon event on April 9th 2016, that coincided with the FEEIT open day intended to promote FEEIT to high school students. The open day was attended by more than one hundred high school students. The Shannon event took place at the premises of the Institute of Telecommunications at FEEIT and consisted of a short presentation of the life and work of Claude Shannon, an exhibition, consisting of ten posters on the life of Claude Shannon and the concepts of Information Theory, and a video describing Shannon's life and achievements, running during the entire event.

The Shannon event was supported by a grant from the IEEE Information Theory Society, from the funds available to support Shannon Centennial outreach events, and by FEEIT.

The high school students were split into groups of around 10–20 persons. There was a short presentation of Shannon's life and contributions for each group by prof. Venceslav Kafedziski, the organizer of the event. The attendees from each group were then guided through the exhibition and were shown the video about Shannon's



life and achievements. The Shannon day event contributed to raising the young public awareness in the Republic of Macedonia of Claude Shannon as the father of the information age.

Event organizer: Prof. Venceslav Kafedziski

IEEE Shannon Centennial Celebration at the Catholic Institute of Business and Technology in Accra, Ghana

The Shannon Centennial was celebrated on the 30th April 2016 at the Catholic Institute of Business and Technology in Accra, Ghana. The celebration brought together mainly academicians, professionals and students to celebrate Shannon's contribution to science and information technology. The celebration was structured around presentations and poster sessions. This allowed participants to enter in to discussions and learn more about Shannon.

The Shannon main speakers were Dr. Anthony Amankwah and Prof. Atma Sahu from Ghana and the United States of America respectively. Dr Amankwah talk was on "Shannon and Information Theory".

Prof. Sahu talked about "Shannon Science and Technology" The topics in the poster session included, the life of Claude Shannon, Information Theory, Cryptography, and Information Technology algorithms. The picture below shows some of the participants.

Below is the Shannon Centennial celebration program in Accra, Ghana.

9.00–9.15 Dr. Anthony Amankwah Amankwah Consult, Accra Ghana

Welcome Address

9.15–10.30 Prof . Atma Sahu , Coppin State University, Maryland, USA
Shannon Science and Technology

11.00–12.00 Dr. Anthony Amankwah Amankwah Consult, Accra Ghana
Shannon Information Theory

13.30–15.00 Dr. Anthony Amankwah Amankwah Consult, Accra Ghana
Information Technology Games



Some of the delegates of the Shannon Centennial.

Mr. George Eduful ECG, Accra, Ghana
Lightning and Electricity

15.00–15.45 **Poster Session**

15.00–16.00 **Closing Remarks**

Feedback from the conference was very positive – participants were informed about the contributions of Claude Shannon (1916–2001).

Anthony Amankwah

The Shannon Centenary in Singapore

The Shannon Centenary in Singapore was held on May 5th 2016 on the campus of the National University of Singapore. It focused on gathering people working in different areas related to information theory, and attracted more than a hundred participants from universities, research centers and schools. The event featured talks by renowned information theorists, and posters from researchers and students, as well as three demos, including Shannon's mind reading machine.

The speakers at the Shannon Centenary included: (i) Mile Gu from NTU who spoke on "Quantum Simplicity - How Complex Systems may be Simplified using Quantum Theory", (ii) Mehul Motani from NUS who spoke on "What we can learn from a bit of information theory", and (iii) Narayana Santhanam from the Univ. of Hawaii who spoke on "A puzzle is worth more than a thousand bits".



Organizers: Rahul Jain, Frederique Oggier, Alex Vardy and Mehul Motani

The poster session consisted of posters that ranged from sequence design to streaming compression of correlated sources to energy harvesting communications. The practical demonstrations included an implementation of Shannon's mind reading machine and software radio implementations of wireless communications and FM radio.

The Shannon Centenary in Singapore was sponsored by the Center for Quantum Technologies, the IEEE, the National University of Singapore, and the Nanyang Technological University.

Website: <https://www.ece.nus.edu.sg/shannon/>

Event Organizers: Mehul Motani, Frederique Oggier, Rahul Jain, and Alex Vardy



Participants enjoying the activities at the Shannon Centenary in Singapore.

A Report on the Shannon Centenary Ceremony at Tarbiat Modares University, Iran

The Shannon centenary ceremony was held on May 8th 2016 at Tarbiat Modares University (TMU), Tehran, Iran. The event was made possible with the help of various stakeholders in TMU, including the Faculty of Electrical and Computer Engineering, the Office of International Affairs, and student volunteers. Partial funding was provided by the organizing committee of the Iran Workshop on Communication and Information Theory. The event chair was Dr. Ahmad R. Sharafat from TMU. The executive chairs were Dr. Hamid Saeedi from TMU, Dr. Babak Seyfe from Shahed University and Dr. Amin A. Gohari from Sharif University of Technology.

The ceremony started with an opening lecture by Dr. Sharafat. This was followed by presenting a short movie about Shannon produced by the IT society. The first keynote speaker of the event was Dr. Jawad Salehi from Sharif University of Technology who delivered an interesting talk entitled "Shannon's Entropy & Physical Reality". The one hour long talk was intended to demonstrate the relationship between Shannon's entropy with the entropy in statistical mechanics. After a short networking break, the second keynote speaker of the event, Dr. Gerhard Kramer from Technical University of Munich presented another interesting talk entitled "Shannon's Information Theory Applied to Fiber Channels". Interestingly, it was the 3rd Shannon event he was attending within a



week (the first 2 were held in Bell Labs, USA and in Germany). Finally, another movie about Shannon was presented in which several pioneer professors in the field talked about Shannon's contributions and achievements. The event ended with closing statements of Dr. Sharafat. There were close to 100 attendees, mainly graduate students from different universities in Tehran and faculty members from TMU, University of Tehran, Sharif University of Technology, KN Toosi University of Technology, and Shahed University.

Future events:

Shannon Centenary Celebration at UC San Diego

UC San Diego will celebrate the 100th anniversary of Claude Shannon's birth with a program of events on Monday–Tuesday, October 10–11, 2016.

The program will center on two invited lectures, the Shannon Memorial Lecture and the Jack Keil Wolf Lecture in Information Theory and Applications. Both lectures are open to the public.

The Shannon Memorial Lectureship was established in 2003 to annually commemorate the accomplishments of Claude Shannon. This year, the Shannon Memorial Lecture will be presented by Dr. A. Robert Calderbank, Professor of Computer Science, Electrical Engineering, and Mathematics and Director of the Information Initiative at Duke University.

The Jack Keil Wolf Lecture Series in Information Theory and Applications, inaugurated in 2014, is named in honor of Prof. Jack

Keil Wolf, who served on the UC San Diego faculty from 1984 to 2011. The Jack Keil Wolf Lecture will be presented by Dr. Ingrid Daubechies, James B. Duke Professor of Mathematics and Professor of Electrical and Computer Engineering at Duke University.

Further details on the lecture schedule and related events will be posted on the IEEE Information Theory Society's Shannon Centenary website <http://www.itsoc.org/resources/Shannon-Centenary>.

IEEE Antennas and Propagation Chapter, IEEE Kerala Section, India

IEEE Antennas and Propagation Chapter, IEEE Kerala Section, India is going to host a technical symposium on "Revisiting Claude Shannon's Contribution" during December 13-14'2016 in Thiruvananthapuram, Kerala, India. The program is technically and financially sponsored by Shannon Centennial Committee, IEEE Information Theory Society and consists of various events which include mass awareness on Shannon's contribution through public lectures by renowned speakers, a poster competition amongst engineering students and technical lectures. Around 100 engineering students and faculty members from various parts of Kerala are

expected to attend the event. Dr. Chinmoy Saha, Dr. CK Vineeth and Dr. B.S. Manoj, faculty members, Indian Institute of Space Science and Technology are the key organizers for this event.

IEEE ITSOC Chicago Chapter

The IEEE ITSOC Chicago Chapter, in conjunction with Motorola – a Lenovo company, is organizing a one day event on September 23, 2016 at the Motorola-Lenovo venue in the Merchandise Mart in downtown Chicago. The event is open to all who register and will feature an opening talk by Dan Costello on "Shannon's Legacy: Coding Theory from 1948–2016", a lunch-time overview of Shannon's life and work by Dongning Guo, and various information theory talks and posters by Chicago-area information theory researchers. Website (under construction) at <http://www.ece.iit.edu/~salim/itsoc.html>

Shannon Symposium, Institute for Advanced Study, Princeton, NJ, USA, 16 Nov 2016

Professor Avi Wigderson of the School of Mathematics of the Institute for Advanced Study is organizing a Claude Shannon Centennial event on November 16, 2016. The event will include a talk given by Sergio Verdú on the Life and Legacy of Claude Shannon.

A Numerical Tribute to Claude Shannon for his Centennial Birthday

*Aziz Inan, Electrical Engineering
University of Portland, Portland,
Oregon July 26, 2016*

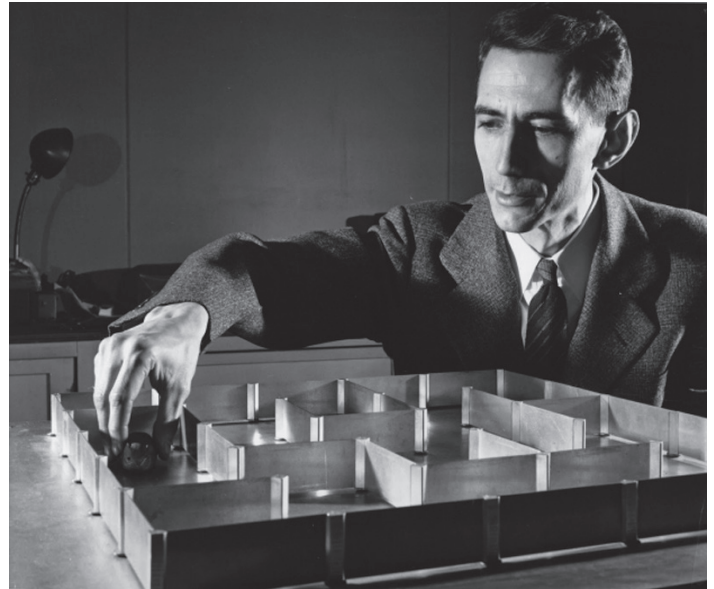
Claude Elwood Shannon, born on April 30, 1916 in Petoskey, Michigan and died on February 24, 2001 at 84, in Medford, Massachusetts, was an American electrical engineer, mathematician, and cryptographer known as "the father of information theory" [1]. Shannon is recognized as the founder of information theory because of a landmark paper he published in 1948. He is perhaps equally well known for founding both digital computer and digital circuit design theory in 1937, when he was a master's degree student at Massachusetts Institute of Technology. At 21, he wrote his thesis demonstrating that electrical applications Period of Boolean algebra could construct any logical, numerical relationship. Shannon's information theorems work most naturally in binary, a base-2 number system involving integer powers of 2.

April 30, 2016 this year marked Shannon's centennial birthday and as a tribute to him, I constructed the following fun birthday brainteasers:

- 1) If Shannon's full birthdate expressed as 4/30/1916, or simply as 4301916 is separated into its odd- and even-numbered digits as 4096 and 311 (4096 and 311 intertwined yields 4301916), these two numbers have a unique numerical connection: 311 is the 64th prime number where 64 is 2^6 and 4096 equals the square of 64, which is 2^{12} . Wow!
- 2) Shannon's birth date 430 (4/30) equals twice 215 where reverse of 215, namely 512, is 2^9 .
- 3) The sum of the digits of Shannon's birthdate 4/30/1916 is 24 where the product of the digits of 24 equals 2^3 . Moreover, 24 is factorial of 4 ($24 = 4!$) where 4 equals 2^2 .
- 4) If numbers 1 to 26 are assigned to the letters of the English alphabet as A being 1, B being 2, C being 3, etc., the sum of the numbers assigned to the letters of Shannon's first name *Claude* is 46, which is the reverse of 64 (2^6).
- 5) The sum of the numbers assigned to *Claude Shannon* equals 131 which is the 32nd prime number where 32 which is half of 64 equals 2^5 . (Also, if number 131 is split into 1 and 31, the sum of these two numbers results in 32.)
- 6) Shannon died at age 84 where the product of the digits of 84 equals 2^5 .
- 7) The sum of the numbers assigned to the letters of *Shannon* equals 85 and interestingly enough, Shannon died during the 85th year of his life. Additionally, the number of calendar dates between 2/24/2001 (the day Shannon died) and what would have been his 85th birthday (4/30/2001) equals 64 (2^6).
- 8) The month, day, and year numbers of Shannon's full birthdate 4/30/1916 have a special numerical connection: the

squares of 4 and 30 add up to 916 which constitute the right-most three digits of 1916.

- 9) Further, the product of 4 and 30 equal 120 and coincidentally, the 120th day of each non-leap year is 4/30 (Shannon's birth date, April 30).
- 10) If Shannon's birthdate expressed in day-month-year date format as 3041916 (30/4/1916) is split into 304, 19, and 16, 19 times 16 yields 304. Additionally, twice the sum of the reverses of 19 and 16, namely 91 and 61, also result in 304. Isn't this magical?
- 11) Shannon died on the 55th day of 2001 (February 24 or 2/24) where the prime factors of 2001, namely 3, 23, and 29, add up to 55. Furthermore, the sum of the prime factors of 55, namely 5 and 11, yields 16 (2^4). Moreover, the sum and the product of the digits of 224 are 2^3 and 2^4 , respectively. Also, 242 representing 24 February equals twice 121 and note that Shannon was born on the 121st day of 1916.
- 12) Shannon's 118th birthday expressed as 4302034 will be a palindrome date. Further, the prime factors of 2034 (2, 3, and 113) add up to 118. Additionally, the sum of the prime multipliers of 2034 (2, 3, 3, and 113) equals 121 and again, Shannon was born on the 121st day of 1916. Also, 2034 equals 18 times 113 where these two numbers add up to 131 (*Claude Shannon*).
- 13) If Shannon's 100th birthday expressed in the day-month-year date format as 30042016 (30/04/2016) is split into 3004 and 2016, these two numbers add up to 5020, and interestingly enough, the reverse of 5020, namely 205, equals the sum of the numbers assigned to the letters of *Claude Elwood Shannon*.
- 14) The sum of the digits of Shannon's 100th birthday expressed as 4/30/2016 equals 16 (2^4).
- 15) The odd-numbered digits of Shannon's 100th birthday, namely 4302016, constitute 4006 which equals twice 2003 where 2003 is the 304th prime number where 304 interpreted as 30/4 coincides with Shannon's birth date, 30 April. Further, the prime factors of reverse of 2003, namely 3002, add up to 100 signifying the 100th birthday of Shannon.
- 16) Also this year, 224 (February 24) marked the 15th anniversary of Shannon's death where 2016 divided by the sum of its digits results in 224.
- 17) Shannon's bicentennial birthday to occur in 2116 in the next century will also be numerically special since 2116 equals square of 46 (*Claude*).
- 18) Lastly, Shannon's 240th birthday expressed as 4/30/2156 will be numerically special since it consists of digits 0 to 6, each digit appearing only once. His 249th birthday written as 4/30/2165 will possess the same property.



Happy 100th birthday to Claude Shannon!

[1] Claude Shannon, Wikipedia https://en.wikipedia.org/wiki/Claude_Shannon

Aziz Inan is an electrical engineering professor at University of Portland. Aziz Inan can be reached at ainan@up.edu.

IEEE Information Theory Society Board of Governors Meeting

Location: Marine Room, La Jolla California

Date: 31 Jan 2016; meeting convened at 1:10 pm PST; meeting adjourned 5:30 pm PST

Meeting Chair: Alon Orlitsky

Minutes taken by: Stark Draper

Meeting Attendees: Krishna Narayan, Pierre Moulin, Alex Vardy, Emanuele Viterbo, Rüdiger Urbanke, Elza Erkip, Aylin Yener, Anand Sarwate, Alon Orlitsky, Michelle Effros, Wei Yu, Jeff Andrews, Abbas El Gamal, Vincent Poor, Suhas Diggavi, Stephen Hanly, Daniela Tuninetti.

Remote Attendees (via Skype): Andrew Barron, Ubli Mitra.

The meeting of the Information Theory Society (ITSoc) Board of Governors (BoG) was called to order at 1:10pm, Pacific Standard Time, by ITSoc President Alon Orlitsky.

Motion: To approve the minutes from the 3 October 2015 BoG meeting in Chicago, Illinois. The motion was tabled to give BoG members more time to review the minutes. The motion was revisited at the end of the meeting.

1) President's Report: President Alon Orlitsky first presented the President's report. Alon welcomed new BoG members: Matthieu Bloch, Suhas Diggavi, Pierre Moulin, Krishna Narayan, and continuing board members Emina Soljanin and Jeff Andrews. He welcomed new officers: Emanuele Viterbo (Conference Committee Chair), Elza Erkip (Second Vice President), and Stark Draper (Secretary). The President extended thanks to retiring board members, committee chairs and officers: Mike Honig, Vijay Kumar, Ram Zamir, Elza Erkip (Conference Committee Chair) and Edmund Yeh (Secretary). Finally, Alon thanked Michelle Effros for her service as ITSoc President in 2015 and Gerhard Kramer for his as Senior Past President.

Alon offered congratulations to a number of Society awardees. Two IEEE Field Awards were awarded: Leandros Tassiulas received the Koji Kobayashi Award and Robert Li, Raymond Young, and Ning Cai received the Eric E. Sumner Award. Three IEEE Medals were awarded to Society members: Roberto Padovani (Bell Medal), Abbas El Gamal (Hamming Medal), David Forney (Medal of Honor). Sergio Verdú received the National Academy of Science Scientific Reviewing Award. Fifteen ITSoc members were elevated to IEEE fellow status: Ozgur Akan, Faramarz Fekri, Christina Fragouli, Erik Larsson, Petar Popovski, Sundeep Rangan, Osvaldo Simeone, John Thompson, Sennur Ulukus, Zhengdao Wang, Kaikit Wong, Liang-Liang Xie, Lie Liang Yang, Jinhong Yuan, and Lizhong Zheng.

Alon provided an update on the position of ITSoc administrator. Matt Lafleur was hired in May 2015. Matt is working 50% for ITSoc and 50% for the RFID council. Matt has been playing important roles in the ITSoc website revision, efforts at creating a movie about Claude Shannon, budgetary work, and generally facilitating interaction with the IEEE.

Alon reported on the State of the Society. The finances are sound. The Transactions are in excellent shape with a record number submissions in 2015. Conference planning is on track and five schools for information theory were held in 2015. A major website revision is in the works.

In terms of Society priorities, Alon raised two. The first is to keep the society vital and important by continually considering how to "branch out" to identify areas in which information theoretic ideas and perspectives can provide insight and impact. Possible initiatives include: (i) organizing a "Bit of information channel" on YouTube or Vimeo, (ii) putting together short videos about information concepts, (iii) a journal of information with a scope broader than that of the Transactions. The second set of priorities surround the Shannon Centennial. Initiatives here include: (i) Shannon Days, and (ii) the Shannon movie. More discussion of the Centennial was to follow later in the meeting.

2) Treasurer's Report: Treasurer Daniela Tuninetti next presented her report on the state of the Society's finances. She first provided the BoG an update on the 2015 budget for which the actual numbers would be finalized by April 2016. She then discussed the 2016 budget.

Regarding the 2015 budget, Daniela first reviewed the three main budget items in terms of percentage revenue/expenses: Publications (60% of revenue / 59% of expenses), conference

(38%/35%), and membership (2%/5%). As of the October 2015 BoG meeting a surplus for 2015 was anticipated, which the BoG approved to donate to the IEEE Foundation Shannon Fund. However, the transfer did not take place as it was too late in the year to get the IEEE Board of Directors' approval to make the transfer. The IEEE Technical Activities Board (TAB) proposed that ITSoc spend the money that would have been donated on the initiatives on which they would have been spent, even through this would mean ITSoc would be in the red for 2016. The projected budget surplus has decreased since the October meeting and the actuals should firm up by early April 2016 by which time all 2015 conference should have closed.

Regarding the 2016 budget, Daniela first discussed the cost of preparation of the Transactions. The switch in 2014 of the Transactions from full-edit to moderate-edit reduced production costs by about 50%. Furthermore, the Transactions page count in 2015 ran about 1000 pages below the estimated page count. Daniela then detailed the income vs. expenses to produce and distribute the Transactions. She presented exact numbers for 2014, but the 2015 numbers are not yet final, pending details on income generated by IEEEExplore. A discussion ensued about the subsidization the Society provides to subscribers of the print edition. This category is decreasing by about 15% per year. It was agreed that the BoG should get a clearer sense of what type of subscribers are receiving the print edition before implementing any changes in pricing. Daniela will work with Matt Lafleur to get such numbers. Finally, Daniela will reach out to the Transactions EiC to get the page count estimated needed to put together the 2017 budget.

Daniela then reviewed the membership situation and fees. There has been a slow decline in overall membership over the past few years, with the exception of 2014 at which time differential pricing was introduced at conferences (for ITSoc vs. non-ITSoc IEEE members). Daniela then reviewed the various product offerings of Society publications to which IEEE members and non-IEEE members can subscribe. Daniela sought guidance from the BoG whether she should formulate a proposal on how to change product pricing and/or product bundling.

Motion: To request the Treasurer to propose a bundling of the Transaction-electronic and Conference-digital-library in a single "Electronic Library" package to sell to IEEE (non-ITSoc) members. After some discussion the motion was tabled.

Daniela reported that in 2015 \$25k was allocated to produce and distribute the Newsletter while actuals were close to \$30k. If a plan is put into motion to grow the Newsletter into a magazine, the additional budget required would need to be planned for.

Regarding conferences, Daniela noted that many schools have occurred sufficiently frequently that they are no longer in the "new initiatives" category (funded through the IEEE "50% rule"), but must be factored into recurrent annual expenses. The 2015 budget aimed for \$268k in net income from conference; through Dec 2015 \$228k had been accrued with some conferences yet to close their books. The 2016 budget is designed to net \$241k in income. The BoG then discussed the possibility of designing budgets to be balanced, to net \$0 in income. Daniela noted that if the BoG decides to aim for such a budget, it will be critical for all conferences to meet their target surpluses.

Daniela then discussed with the BoG administrative fees charged by IEEE, the budgets allocated to the various committees, the salary for the new ITSoc administrator, and the support for the Distinguished Lecturer (DL) series, as well as the budget for new initiatives.

In conclusion Daniela noted two things. First, the draft budget for 2017 is due to the IEEE in July, so if any committee will request an increase in their budget they need to do so before the BoG meeting at ISIT. Second, Daniela provided some guidance regarding reimbursements: (a) submit expenses within one month, (b) email all receipts with the latest expenses form (which Daniela can provide) to her and Matt LaFleur, (c) include a full list of attendees at meals, (d) Distinguished Lecturers should follow same procedure.

- 3) **Nominations and Appointments (N&A) Committee:** N&A Committee Chair Abbas El Gamal next presented his report. He reviewed the composition of the various committees and noted that all are fully staffed except for the External Nominations Committee, which is still missing a committee chair.

Abbas then reviewed two changes in the bylaws that require BoG discussion and votes. The first change was a revision of the current bylaws. It concerned the selection of the James L. Massey Research and Teaching Award. Abbas read the proposed revised bylaw to the board: "A subcommittee of the Awards Committee shall be responsible for selecting the recipient of the IEEE Information Theory Society Thomas M. Cover Dissertation Award, according to Article VII, Section 8. Another subcommittee of the Awards Committee shall be responsible for selecting the recipient of the IEEE Information Theory Society James L. Massey Research & Teaching Award for Young Scholars, according to Article VII, Section 9.... The Cover Dissertation Award and Massey Research & Teaching Award Subcommittees shall be appointed by the Nominations and Appointments Committee by December 31 of the previous year."

Motion: To pass the revision to the bylaws. The motion was passed unanimously.

The second change was an addition to the bylaws requested by the IEEE. The addition deals with possible conflict-of-interest situations wherein a member of the N&A Committee would like to be nominated to a committee for which the N&A Committee handles nominations. In brief, said member would both need to resign prior to the start of the year and cannot be nominated by a (former) fellow member of the N&A Committee. Abbas read the proposed addition: "A member of the N&A Committee may be nominated and run for a position for which the N&A Committee makes nominations only if: (i) the member resigns from the N&A Committee prior to its first meeting of the year in which the nomination shall be made and (ii) the nomination is made by a member of the N&A Committee whose term did not overlap with that of the nominee."

Motion: To pass the addition to the bylaws. The motion was passed unanimously.

- 4) **Online Committee:** Online Committee Chair Anand Sarwate presented his report. Anand reviewed the current

Committee membership and thanked Stefan Moser for his efforts on behalf to the Committee.

Anand reported that ITSoc Administrator Matt Lafleur is taking on the job of updating website content. He gave a tour of the mockup of the revised site. He would like to get a volunteer to manage an ITSoc Twitter feed, as well as other social media links (LinkedIn/Facebook/other). The BoG asked about a YouTube channel. The decision was made to go with Vimeo because there are no ads and because there may be ownership questions once you post content to YouTube. Anand will look into legal issues about ownership on YouTube with the idea that we can perhaps post both to YouTube and to Vimeo, and will report back to the board.

- 5) **Conference Committee:** Conference Committee Chair Emanuele Viterbo first reviewed the current membership of the Committee and made a motion to add two members to the Committee.

Motion: To add Elza Erkip and Brian Kurkoski to the Conference Committee. The motion was passed unanimously.

Emanuele then reviewed the upcoming ISITs. All are on track. Emanuele reviewed the ISIT 2018 (Paris) budget, registration costs, and discussed pessimistic and optimistic revenue scenarios. The target is an 8% surplus. The BoG had a short discussion about how much surplus to target. The ISIT 2018 organizers are requesting a \$60k loan to use for a down-payment for the venue.

Motion: To approve the ISIT 2018 budget and loan. The motion was passed unanimously.

Emanuele then reviewed the ITWs from 2015 (past) through 2017. He also introduced two motions for technical co-sponsorship. A short discussion of the benefits that accrue to ITSoc from technical co-sponsorship ensued. The two conferences requesting technical co-sponsorship are the 9th International Symposium on Turbo Codes (2016) and the 15th International Symposium on Problems of Redundancy in Information and Control Systems (2016). The Committee recommended both symposia be co-sponsored.

Motion: To co-sponsor the 9th International Symposium on Turbo Codes. The motion was passed unanimously.

Motion: To co-sponsor the 15th International Symposium on Problems of Redundancy in Information and Control Systems. The motion was passed unanimously.

- 6) **Schools Committee:** Aylin Yener, Chair of the Schools Committee, then presented the report of the Committee. In 2015 there were five schools. The five school were the North American School held at UCSD, the European School held in the Netherlands, the Indian School, the East Asian School in Hong Kong (funded by the Croucher Foundation), and the African School held in South Africa. The four schools planned for 2016 and previously approved by the BoG are all on track. The Australian School was held already at Monash University in Melbourne in January 2016. The other 2016 schools will be the North American School to be held at

Duke University, the European School to be held at Chalmers University of Technology in Sweden, and the Indian School.

As for future schools, Aylin reported that it is likely that the next Croucher Foundation funded East Asian School will be held in Hong Kong again in 2017. At the moment a biannual event appears more feasible in Asia than an annual event. In 2017 there will be schools in North American and in Europe, these are annual events.

A proposal to hold the 2017 European School in Madrid was presented by Albert Guillén i Fàbregas on behalf of the organizers.

Motion: To support the 2017 European School for Information Theory in the amount of \$20k. The motion passed unanimously.

- 7) **Report on the Transactions:** President Alon Orlitsky presented the report on the Transactions on behalf of EiC Frank Kschischang who could not attend the BoG meeting. A number Associate Editors (AEs) are retiring and were thanked for their service: Michael Langberg, Yingbin Liang, Gerald Matz, B. Sundar Rajan, Rajesh Sundaresan. The number of submissions is up and the page count is down.

Prakash Narayan will become Executive Editor at the beginning of March. The addition of the Executive Editor position was approved by the BoG at the last meeting. The Executive Editor will be responsible for day-to-day paper handling/assignment, dealing with authors and AEs, and interacting with ScholarOne. The EiC retains overall responsibility, and is responsible for producing issues, handling appeals, interacting with IEEE Production Portal, recruiting new AEs (in consultation with EE and EEB), writing reports, chasing delinquent reviewers, making presentations.

Motion: To approve Holger Rauhut as AE for signal processing. The motion was passed unanimously.

- 8) **Membership Committee:** Membership Committee Chair Elza Erkip presented the Committee's report. Elza introduced the new Committee and subcommittee members. Subcommittees include Student, Outreach, and School Committees (the last reported earlier in the meeting). Elza reviewed the major activities of the subcommittees. A point was raised that since the many schools are recurrent rather than new initiatives, the Schools Committee might be shifted to be under the auspices of the Conference Committee. It was recalled that this suggestion had been made in the past, but that the School Committee had not been moved because the Conference Committee is already heavily loaded.
- 9) **Shannon Centennial:** Rüdiger Urbanke presented the Shannon Centennial Committee report on behalf of Committee Chair Christina Fragouli. Rüdiger reviewed three infographics that the Committee had put together with volunteers and a designer of infographic. The three infographics discuss the impact of Shannon's ideas on information compression, storage, and security. The goal is to get 10 posters together. Rüdiger then played a short video (three minutes) about Shannon's life, which could be played, e.g., at Shannon Day celebrations, perhaps in a rolling loop in

poster sessions. Rüdiger discussed how the target of Shannon Days is pre-university students. The Committee has also been in contact with IEEE Spectrum about the centennial, with Khan Academy about the possibility of producing educational videos on information theory, and with Google about getting a Shannon-oriented design for Google's front page on the date of the centennial. There is a website for the centennial that will be updated shortly and a number of Centennial events have already been fixed. The Committee has spent \$10k of its budget for logo design, the short movie, and infographics design.

The BoG discussed various ideas that might prove helpful to publicize the Centennial. One idea was to have the graphics designer make a website banner that departments can use on their websites. Another was to have an array of content that could be shared with news organization that could push that content to local outlets, e.g., text for a newspaper, a one-minute video for TV organizations (we would need to get all rights), something for social media.

Motion: To allocate the Shannon Centennial Committee an additional \$10k budget to complete the infographics, to offer small commemorative gifts, and to create a children's book. The motion passed unanimously

Rüdiger requested \$100k in ITSoc support to support Shannon Centennial events. A discussion ensued regarding the logistics of where the money would come from, the impact on the 2016 budget, the process that would be followed in awarding the money to recipients, and on how to communicate to awardees what sorts of expenses would be reimbursable. Regarding the first two financial items it was noted that the IEEE Technical Activities Board (TAB) has already suggested that ITSoc go into the red for 2016 to support Shannon Centennial events. The money, at least in part, corresponds to monies that in 2015 the BoG approved be transferred to the IEEE Shannon Fund. As noted earlier, this transfer was unable to be completed. Regarding the last point, on reimbursements, the Treasurer would help to determine what sorts of items would be reimbursable and the process for reimbursements. Regarding the process to award funds, the following motion was made:

Motion: To approve expenditure of a budget of up to \$100k to support Shannon Centennial Events. The procedure to allocate funds would be as follows: (i) The Centennial Committee will send out a call for proposals. (ii) The call would include guidelines on items that are likely to be reimbursable, e.g., speaker travel costs, poster printing costs, some small games. (iii) Proposals and accompanying budgets would be submitted to the Shannon Centennial Committee for approval (Chair: Fragouli, Members: Urbanke, Varshney). (iv) The anticipated amount of each award would be on the order of \$4–5k. The motion passed unanimously.

- 10) **Open discussion topics:** In the concluding topic of the meeting President Alon Orlitsky revisited some of the priority topics he had raised in his President's Report.

Alon raised the possibility of a "bit of information channel". This could consist of putting together educational items such as webinars or a YouTube channel. These activities could be

in synchrony with the Centennial celebrations. It was thought that, if needed, the organizers of such content could apply to the Centennial Committee for funding under the auspices of the Shannon Centennial. That was generally thought to be a good idea for this year. The BoG will discuss at a later meeting whether a different funding mechanism is needed in future years.

Alon raised the idea about creating short videos about information theory concepts. Some examples of (successful) short educational videos on extremely technical topics were

mentioned by members of the Board. The Khan Academy was raised as a possible collaborator on such initiatives.

- 11) **Minutes of the last meeting:** The minutes from the previous meeting were briefly discussed.

Motion: To approve minutes from the October 2015 BoG Meeting. The motion was passed unanimously.

The meeting was adjourned at 5:30pm PST.

President's column *continued from page 1*

this philosophy, David made profound theoretical and practical contributions to a variety of topics ranging from MIMO wireless networks, ad-hoc networks, network information theory, scheduling, and most recently bioinformatics. He also co-authored an influential textbook that helped shape the communication-research landscape. David's work was recognized by multiple societies, including ours, Communication, Signal Processing, and Applied Probability, and this year, he received our shiniest trophy.

I was particularly gratified that from student papers to career achievement – all our award recipients were “young”, by the standard “born after me” definition. While you may be tempted to link this concurrence to the author's slightly graying hair, I maintain it is a sign that our society teems with energetic young researchers and engineers who will propel us to the next generation of inventions and technological contributions and serve as role models for years to come.

Success begets submissions – over 1,100 a year lately, roughly 47% of which, accounting for over 7,000 pages, get published in the Transactions. These papers are so popular that IEEE Xplore is now our society's largest and most reliable revenue source, generating \$850K in 2015. The complex operation of handling, reviewing, revising, and publishing this treasure trove of scientific innovation is carried out by a cadre of 53 devoted associate editors, headed by the quintessential researcher and scholar – the Transactions Editor-in-Chief.

Not surprisingly, the EiC position has become all-consuming, and on the advice of current EiC, aka 2016 Wyner Awardee, Frank Kschischang, the society decided to entrust some of the responsibilities to a new Executive Editor position. The EE will interface with ScholarOne, screen new submissions, allocate them to the AE's, and ensure timely reviews. The EiC will retain overall responsibility of the journal and will handle delays, appeals, page setup, production, interaction with IEEE, and AE recruitment. This addition will hopefully also free up some of the EE and EiC time to launch new initiatives and invite papers of strategic importance to the Transactions.

In steady state, the EE will serve for 18 months and then transition and serve as EiC for the same period. Our first EE is Prakash Narayan, one of our most accomplished and respected colleagues, who started in March and will succeed Frank as EiC at the end of the year. I would like to thank Frank for his remarkable service over the past three years and wish Prakash the best of luck with his new responsibilities. Note that Prakash now has the authority to summarily reject any submission, so better be nice to him.

A lion's share of our community's growth and success is due to generous funding agencies that have supported decades of our research and helped educate generations of information scientists and engineers. In particular, here in the US, we were fortunate to have multiple NSF program directors whose dedication, encouragement, and wisdom, have helped guide and foster a wealth of programs, large and small.

The NSF area closest to information theory is the Communication and Information Foundations Cluster. This year, two CIF program directors left their posts. Phil Regalia finished a four-year term and returned to his faculty appointment at the Catholic University of America, and John Cozzens retired after over two decades and is currently serving as a CIF Expert. I would like to thank them both for all they have done (and continue to do) for our community.

In January, Rick Brown took leave from Worcester Polytechnic Institute to succeed Phil in the CIF Cluster. Rick hit Wilson Boulevard running and has proactively engaged our community with a wide range of NSF programs and initiatives. He is particularly interested in helping junior researchers launch their careers, as I discovered when upon visiting him on society business, I found him advising a group of new faculty on applying for their first NSF grant. I asked Rick to write an article about NSF and funding opportunities, and he kindly agreed. You can find his thoughts and several useful resources on page 4.

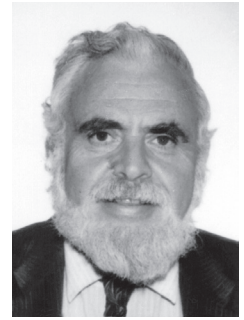
The Shannon documentary we have been working on for the past year is progressing well. Instead of standard “talking head” interviews and voice-over narration, director Mark Levinson plans to bring Shannon to life via an imagined conversation, with a prominent actor portraying Shannon at the Winchester house toy room. Flashbacks, occasional interviews, animation, and graphics will add background, facts, and of course information theory. The main shoot is planned for late Fall and we hope to show you a short excerpt in the next newsletter. Meanwhile, a “teaser” featuring Claude's son Andrew: <https://vimeo.com/180051562>, password ASTeaser.

To conclude, essentially everyone in the world follows a standard solar or lunar, e.g. the Gregorian, calendar. Yet in our unique community, many dance to their own drumbeat and rejoice to a different rhythm and ritual. To all of you I wish,

Happy Academic New Year!

GOLOMB'S PUZZLE COLUMN™

Latin Squares Solutions



Solomon W. Golomb

- 1) Suppose a Latin Square L , of order n has n simultaneous n -over-lapping transversals. Form a new Latin Square, L' again of order n , by putting a "t" wherever there was an element of the t th transversal in L , for each t , $1 \leq t \leq n$. Then L' is a new Latin Square, orthogonal to L .

If a Latin Square of order n is the multiplication table ("Cayley table") of an n -element group, the elements e_k of a transversal have the form $r_i \circ c_j = e_k$, where r_i is the i th row element, c_j is the j th column element, and " \circ " is the group operation. For the $\{e_k\}$ to form a transversal, the $\{r_i\}$, the $\{c_j\}$, and the $\{e_j\}$ must each be permutations of the n elements of the group.

- 2) If the group is Z_p^* , the multiplicative group of the elements $\{1, 2, 3, \dots, p - 1\}$ modulo p , suppose we had a transversal. Then the product, mod p , of the n elements $\{e_k\}$ would be $(p - 1)!$, while the product of all the $r_i \circ c_j$, modulo p , would be $(p - 1)! \circ (p - 1)!$ Wilson's Theorem, in elementary number theory, states that when p is prime, $(p - 1)! \equiv -1 \pmod{p}$. So a transversal of Z_p^* would give $((p - 1)!)^2 \equiv (p - 1)! \pmod{p}$, and $(-1)^2 \equiv -1 \pmod{p}$, so $+1 \equiv -1 \pmod{p}$, which is impossible for prime $p > 2$.
- 3) Suppose we have the Cayley table of an element group G which has a transversal: $r_i \circ c_j = e_k$, where each of $\{r_i\}$, $\{c_j\}$, and $\{e_k\}$ is a permutation of the n elements of G . Take any fixed element g_i in G , and consider $g_i \circ (r_i \circ c_j) = g_i \circ e_k$. By the associate law for group multiplication, this says $(g_i \circ r_i) \circ c_j = g_i \circ e_k$. Here $g_i \circ r_i$ is a permutation of the rows, and $g_i \circ e_k$ is a permutation of the entries, so for each element g_i of G , except the identity element of G , this is a new transversal, and from the n element of G as g_i , we get n simultaneous, disjoint transversals.
- 4) Suppose we have k mutually orthogonal Latin Squares of order n . By renaming the elements of each one, as necessary, we can make the top row of each be: $1, 2, 3, \dots, n$. Then, between any two of them, we see the ordered pairs $(1, 1), (2, 2), (3, 3), \dots, (n, n)$. Let us next consider the left-most element in the second row of each of them. All must be distinct, because if any two were the same, those two Latin Squares would have the ordered pair (r, r) a second time, since the pair (r, r) already occurred from their top rows, for each r , $1 \leq r \leq n$. Moreover, none of the k Latin Squares can have a "1" as their left-most

element in their second row, since that would be a second "1" in the left-most column of that Latin Square. Hence, there are only $n - 1$ elements available for the left-most element in the second row, and there must be a different one of these elements in each of the mutually orthogonal Latin Squares of order n , which limits the maximum number of such squares to $n - 1$.

- 5) Suppose an $n \times n$ Latin Square has $n - 1$ simultaneous non-overlapping transversals. Then what is left over will be one location in each row, one location in each column, and one each of the n -elements – hence, an n th simultaneous non-overlapping transversal.
- 6) The most simultaneous non-overlapping transversals that a Latin Square of order 6 can have is four: because if it had five, then by the previous results it would have six, and hence an orthogonal mate. But we know that there is no pair of orthogonal Latin Squares of order 6.

Here is an example of an order 6 Latin Square with four simultaneous transversals:

①	2	△3	◇4	□5	6
□2	◇3	5	○6	4	△1
3	△4	□6	1	○2	◇5
4	□1	◇2	5	△6	○3
△5	6	○4	□3	◇1	2
◇6	○5	1	△2	3	□4

The elements of the different transversals are enclosed in the symbols ○, △, ◇, □ respectively.

In Memoriam: Professor Rudolf Emil Kalman

Tryphon Georgiou, Andrew Kalman, Pramod Khargonekar

Professor Rudolf E. Kalman, formerly graduate research professor and director of the Center for Mathematical System Theory at the University of Florida in Gainesville, Florida and the chair for Mathematical System Theory at the Swiss Federal Institute of Technology (ETH) in Zürich, Switzerland passed away peacefully on the morning of July 2, 2016, at his home in Gainesville, Florida. He was 86 years old.

Rudolf Kalman was born in Budapest, Hungary, on May 19, 1930. He emigrated to the United States and received his bachelor's (S.B.) and master's (S.M.) degrees in Electrical Engineering from the Massachusetts Institute of Technology in 1953 and 1954, respectively, and his doctoral degree (D. Sci.) from Columbia University in 1957. In 1958 through 1964, as a research mathematician at the Research Institute for Advanced Study (R.I.A.S.) in Baltimore, Maryland he produced a series of groundbreaking contributions that shaped the field of Mathematical Systems Theory and of Control Engineering. Chief amongst those was the "Kalman filter," a mathematical framework and an algorithm that enables navigation and control in virtually all modern-day apparatuses, from airplanes to satellites and from cellphones to magnetic resonance imaging. In particular, in its early days, the Kalman filter proved pivotal in the success of the Apollo program that sent the first humans to the moon. Fifty years since his seminal paper entitled "A new approach to linear filtering and prediction problems," the Kalman filter continues to find new applications in fields as varied as weather forecasting, stock picking, econometrics, GPS, computer vision, autopilots, structural health monitoring, seismology and motor control.

Rudolf Kalman's contributions to the principles of separation between control and estimation, the design of sampled-data systems, optimization, and the structure of dynamical systems perse are timeless. His thought and style of scientific inquiry have educated countless engineers and scientists. His contributions have impacted modern technological and scientific developments across many disciplines.

After R.I.A.S., Rudolf Kalman became a professor at Stanford University (1964–1971). From 1971 to 1992 he was a graduate research professor and director of the Center for Mathematical System Theory at the University of Florida in Gainesville. Simultaneously, he held the chair for Mathematical System Theory at the ETH in Zürich from 1973 until his retirement in 1997. He received numerous awards, including the IEEE Medal



Rudolf Kalman receiving the National Medal of Science from President Barack Obama. Photo credit: <http://www.ams.org/notices/201001/rtx100100056p.pdf>

of Honor (1974), the IEEE Centennial Medal (1984), the Kyoto Prize in High Technology from the Inamori Foundation, Japan (1985), the Steele Prize of the American Mathematical Society (1987), the Bellman Prize (1997), and the Draper Prize (2008). He was elected member of the National Academy of Sciences (USA), the National Academy of Engineering (USA), the American Academy of Arts and Sciences (USA), as well as member of numerous foreign Academies. He received many honorary doctorates and, in 2008, Rudolf Kalman received the National Medal of Science, the highest honor the United States gives for scientific achievement.

Throughout his career, Professor Kalman led and taught by example. He was a purist in pursuing ideas to completion no matter how long or what effort that necessitated. His publications were gems, with no exception, in both elegance and scientific depth. The "Center" (Center for Mathematical System Theory) that he founded at the University of Florida was unique in its scope and reputation. His superb scholarship and magnetic personality was the heart and soul of the Center for over twenty years, attracting the most brilliant colleagues and contributors in Control, Dynamical Systems, as well as many subjects in Mathematics.

Professor Kalman is survived by his wife Constantina née Stavrou, their two children Andrew and Elisabeth, and their families.

In Memoriam: Solomon W. Golomb

The Information Theory Society suffered a great loss earlier this year when Solomon Golomb passed away peacefully on May 1, 2016. Just ten days earlier he was awarded the prestigious Franklin Medal 2016 in Electrical Engineering for his revolutionary work on shift register sequences and their applications to space communications, satellite communications and cellular communications.

Sol was a giant of Information Theory and was responsible for several breakthroughs that changed the nature of the field and helped bring about the era we live in today. Much has been written over the past few months about his accomplishments (Indeed, we will address that ourselves below).

But Sol was more than a mathematical genius. He was a kind and generous man who loved his friends and family, designed math and word-play puzzles, and spoke over 20 languages. While he will certainly be remembered for his contributions to information theory, his impact on the personal lives of those around him should be no less celebrated.

“Sol showed me what an academic advisor should be, taught me how beautiful fundamental research can be, how exciting application research can be, and changed my whole life from the time I was a PhD candidate until today.” Said former student, Professor Hong-Yeop Song.

“During my time as a post-doc, Sol was the Vice Provost. Even still, he always made time for me and his PhD students.” Said Tuvit Etzion. “Just three months after arriving at USC, he invited me to Thanksgiving Dinner – one of many learning experiences I shared with him over a meal.”

Sol was as adventurous as he was academic. Andrew Viterbi, Sol’s close friend of nearly 60 years, recalls a road trip the two of them took to San Francisco with their wives for an IEEE convention in 1957: “All went well on the way up, but returning on pre-Freeway Route 99, perhaps due partly to the heat, the oil cap would come loose and fall off every few miles. This happened half a dozen times, in each case resulting in a feverish but successful search over the last several yards just driven. We finally made it back to Pasadena in one piece.”

In 1963 Sol was highly recruited by some of the best schools in the country. Having his pick of the litter, he chose USC – a school that at the time was not known as an engineering powerhouse. “The question I asked myself was the one I ask my students: ‘Where can you make the most difference?’” Golomb told USC Viterbi magazine in fall 2012.

Over the next half century Sol helped turn USC into a leading center of communications research. An achievement this big does not come from groundbreaking research and genius alone. Sol understood the importance of community, mentorship, and service in building a lasting institution. It is for those qualities, as well as his unique mind, that we celebrate him today. Below, we summarize just a few of Sol’s many contributions.

The start of Feedback Shift Register Sequences

As early as in June 1954, Solomon Golomb worked on a summer job with the Glen L. Martin Company in Baltimore (currently, Lockheed Martin). The leader of the Communications Group,

Thomas Wedge introduced him to a problem that was described as involving a *tapped delay line with feedback*. Sol called it a binary linear shift register with feedback and immediately called on his knowledge of pure mathematics to solve this problem.

An n -stage linear feedback shift register (LFSR) is a circuit consisting of n consecutive 2-state memory cells regulated by a single clock. At each time, the content of each memory cell is shifted to the next cell of line, and a new state is obtained by a feedback loop which computes a new term based on a linear Xor combination of the n previous terms. During that time, the experiments showed that for some combinations of taps of the memory cells, very long binary sequences would be produced, but for other combinations of taps, much shorter output sequences resulted. Sol’s approach was to look at power series generating functions over finite fields, which yielded the correspondence between LFSR sequences and polynomials. The maximal length of those sequences is $2^n - 1$. These are called m -sequences and can be generated by a primitive polynomial over a finite field with order 2.

Sol proposed three criteria to evaluate randomness of those LFSR sequences, known as Golomb’s Three Randomness Postulates: balanced 0–1 distribution, uniformly distributed consecutive 0’s or 1’s (i.e., the runs), and the two valued autocorrelation with all out-of-phase correlation values are equal to $-1/(2^n - 1)$. The m -sequences possess all three randomness properties. Particularly, the autocorrelation of m sequences resembles white Gaussian noise with flat spectrum-like or impulse-like, so it is named pseudo noise (PN) sequences in many textbooks of digital communications.

Applications for Space and Satellite Communications and Radar

The first two applications of the 2-level autocorrelation property of m sequences, discovered by Sol, were in space communications when he worked at the NASA Jet Propulsion Laboratory (JPL). As the Leader of the Information Processing Group in JPL, his lab was tasked to provide a solution to early orbit determination of Explorer I, launched in 1958 after the launch of Sputnik (Russian) in 1957. The signal sent back from Explorer I was the binary phase shift keying (BPSK) pulse modulated by an m -sequence. Another amazing application of this property in 1958 shortly after launching Explorer I, was to prepare to launch a space probe to the vicinity of Venus. Sol was the leader on the Venus Radar detection project. He had designed an interplanetary ranging system at JPL, based on BPSK of an RF carrier using m sequences, that basically counted RF-cycles, and thus potentially provided extreme range accuracy. Venus was successfully detected by JPL in 1961, in a way which was more accurate than before. In their Venus experiment, which directly measured by radar, Sol showed that the distance between Earth and Venus reported before was wrong by far.

Applications in Cellular Communications

The m sequences are used as spreading codes in spread spectrum communications for anti-jamming and low probability interception. His revolutionary book, *Shift Register Sequences* [3], has long been a standard reading requirement for new recruits in many organizations, including the National Security Agency and a variety

of companies that design spread spectrum communication systems for anti-jamming and low probability interception. These technologies, commercialized in cellular communications, are known today as CDMA (code-division multiple access) systems in 2G cellular systems as IS-95, and CDMA 2000 in 3G systems.

Exp-Golomb Code for Lossless Data Compression

Run-Length encoding, a paper Sol published in 1966 [2] became a widely used lossless data compression technique, adopted and termed as Golomb codes or Exponential Golomb (Exp-Golomb) codes. It was used to send back scientific data from the Mars Rover in 1960s. Currently, the Exp-Golomb code has been selected in the standards of multi-media communications such as MPEG-4 (or H.264).

Golomb Ruler

A pattern that Sol observed, originally for coded pulse radar, was a ruler of length L with n marks on it such that any distance d less than or equal to L can be measured in one and only one way as a distance between two of the n marks. This concept was popularized in Martin Gardner's column as *Golomb Rulers*. Since then these have been applied in fields of far ranging for Xray diffraction crystallography, radio antenna placement, and error correction. It is still open whether there exist infinite many shortest Golomb rulers. The latest exhaustive search results have been extended to the length $L = 27$.

Costas Arrays for Radar Detection

John Costas (1984) presented the following problem to Sol: Design an n by n frequency hop pattern for radar or sonar, using n consecutive time intervals and n consecutive frequencies where each frequency corresponds to one time interval and each pair of frequencies with their corresponding time intervals are different, i.e., correspond to an ideal ambiguity function for the frequency hop pattern. Sol discussed this problem with Lloyd Welch and Abraham Lempel and shortly they came up with three systematic constructions to this problem, known as the Welch, Lempel and Golomb constructions, respectively [5]. These constructions remain as general constructions till now. Recently, Sol tackled this problem with a slightly different angle [8]. The latest exhaustive search has been extended to $n = 29$.

Classification of Sequences

In 1958, when he was in JPL, Sol investigated how to generate a sequence with a long period given that the length of each LFSR is bounded. He experimented on using the periods of nonlinear shift register sequences in the radiation detector on Explorer I which discovered what is known as the *van Allen radiation belts*. (James van Allen was a graduate student who worked on this with Sol.) Currently, in cryptology, it is an important method to construct nonlinear generators using multiple LFSRs, called combinatorial generators.

In order to measure randomness of a random sequence with the same period as m -sequences, Sol defined a concept of span n sequences, i.e., any nonzero n -bit string occurs exactly once in a binary sequence with period $2^n - 1$. Then he conjectured that any sequence with 2-level autocorrelation and span n property must be an m -sequence (1980 [4]). Significance of the conjecture in cryptography is that a random sequence with large linear span (or linear complexity) has to compromise one of those two properties.

Golomb's Invariants and Nonlinearity in Cryptography

Most of the properties of nonlinear feedback shift register sequences were unknown until now and the known ones were collected in Sol's book, *Shift Register Sequences*. In cryptographic applications, in order to realize Shannon's concept of a one-time-pad, i.e., stream cipher encryption, m -sequences were used for their long periods in the 1950s and 1960s. However, m -sequences are linear which cannot be directly used in any cryptographic systems since 1968 and should be replaced by nonlinear sequences, generated by filtering single LFSR or multiple LFSRs. The question is then how to measure the cryptographic strength of those filtering functions. Sol (1959 [1]) investigated the invariants of a Boolean function, which measures the distances between the Boolean function and linear combinations of its inputs.

A good filtering function in cryptographic application should be far from or independent from input variables or linear combination of input variables. This can be measured by the invariants and was termed as nonlinearity in modern cryptography. Sol's results, presented in 1959, were rediscovered by Xiao and Massy in 1988. Currently, the nonlinearity of Boolean functions is one of the most important concepts for designing cryptographically strong Boolean functions.

Golomb's Invariants for Correlation Related Attacks

The immediate applications of Sol's invariants of Boolean functions in cryptography are the so-called correlation attacks. In other words, as long as a Boolean function is correlated with some of the input variables, the initial states, loaded as keys, those correlated LFSRs can be recovered individually by computing correlation between the output of the Boolean function and that input. This converts the overall time complexity from the multiplication of the number of states in each LFSR to the addition of the number of states of those correlated LFSRs plus the remaining part from exhaustive search. This is a significant reduction to the size of the exhaustive search. Although Sol did not explicitly mention this application in his 1959's paper, he was awarded a Medal for his contribution to cryptography by the National Security Agency in 1992.

Sol's concept of the invariants is to measure the correlation between a sequence and an m -sequence. However, there are many distinct LFSRs, corresponding to the number of primitive polynomials, which generate distinct m -sequences with the same period. By the end of 1990's, Sol, together with his collaborator, extended this measurement to any LFSRs, called the extended Hadamard transform. The use of the extended Hadamard transform as the measurement of the strength of a cryptographic function gave rise to new cryptographically strong functions, namely hyper-bent functions, which are widely investigated in cryptographic communities today.

Applications in Secure Communications

The field of shift register sequences (or equivalently, pseudorandom sequences), created by Sol is widely used in numerous cryptographic applications including stream cipher, block cipher, pseudorandom sequence generations, key deviation functions, pseudorandom functions, challenge number generations for authentication protocols, public-key cryptographic schemes, hardware test vectors, and

countermeasures for side-channel attacks. Especially due to the simple hardware structure of LFSR based pseudorandom sequence generators, they have been proposed to secure the Internet-of-Things (IoT) where constrained devices will be deployed in extremely large scales, especially, in radio frequency identification systems, for establishing trust among a variety of devices and ensuring confidential transmissions. Those embedded applications and systems have been used for protecting our daily digital world including on-line banking, shopping, health record transfer, medical care, and more future new applications in vision.

Polyominoes

The other branch that Sol investigated is recreational mathematics. Sol generalized a puzzle problem about putting dominoes on a checkerboard from which a pair of opposite corners had been removed, and created the subject of Polyominoes (1954). His book (1965, revised 1994) Polyominoes has a world-wide audience, and has led to the invention of the computer game Tetris.

Inspiring Young Researchers

Sol loved to give talks in various occasions. Each of his talks were full of his intelligent and multi-faced knowledge, especially in the questions periods (e.g [6, 7]). His last talk was given at the Workshop on Shift Register Sequences for Honoring Dr. Solomon W. Golomb Recipient of the 2016 Benjamin Franklin Medal in Electrical Engineering, which was held in Villanova University, Philadelphia, on April 20, 2016.

Over his career, the impact of Sol's contributions were recognized with election into the National Academy of Engineering, the National Academy of Sciences, and a foreign membership in the Russian Academy of Natural Sciences. Within the University of Southern California, Sol was a University Professor and the recipient of the USC Presidential Medallion. He was awarded the National Medal of Science in a White House ceremony in 2011. Sol was a Distinguished Alumnus of Johns Hopkins University and received multiple honorary doctorates. He was a fellow of numerous societies including the IEEE, the American Mathematical Society, the Society for Industrial and Applied Mathematics, the American Association for the Advancement of Science, and the American Academy of Arts and Sciences.

In recent correspondence with a journalist from the New Yorker magazine, Sol recollected some of his experiences with Claude Shannon, "My Shannon Lecture was in Brighton, England, Shannon, who had delivered the first Shannon Lecture (in Ashkelon, Israel) quite a few years earlier, was in my audience – the only Shannon Lecture he attended since his own. I had spent most of the Fall semester of 1959 at MIT (on leave from my position at the Jet Propulsion Laboratory – JPL) where I had lunch three times a week with Claude Shannon and a few other members of the MIT communications faculty. I sat in on Shannon's lectures on his own course on Information Theory. On one occasion, he asked me about a problem in mathematical statistics, and the next day I presented him with a simple solution to it." Sol was also awarded the IEEE Richard W. Hamming Gold Medal.

Sol's passing has been deeply felt by the Information Theory community. Toby Berger wrote, "He is irreplaceable. A genius among our geniuses, he was a man who somehow knew almost

EVERYTHING in an era in which that seems to be impossible, but it was true." Further elaborating on Sol's many talents, "Perhaps less known but equally encyclopedic was Sol's philology. He read more than 120 languages and admitted to speaking over 20 of them; that admission meant that he could converse fluently with native speakers in each of those, which ranged from Ancient Greek, to Mandarin, to Norwegian; he knew three dialects of Norwegian but counted that as only one of his spoken languages."

Abraham Lempel reminisced about when his and Sol's paths first intertwined: "I first met him in 1967, at an IT workshop at the Technion, when I presented him with a proof of one of his conjectures re shift register sequences. At the time I was a fresh PhD at the Technion EE department and Sol invited me for my post-doc at USC which I was happy to accept. I arrived at USC in July 1968, shared an office with Lloyd Welch, and worked very closely with Sol for a year. Under Sol's influence and guidance I have traded my interest in network theory for the rich realm of digital sequences."

Sergio Verdu further adds, "What a towering figure he was. I vividly remember his Shannon lecture in Brighton."

Bob Gray did his PhD at USC under Bob Scholtz; his MS thesis advisor, Irwin Jacobs, strongly urged Bob to take as many courses as he could from Sol Golomb, "regardless of topic," noting that "Sol was a genius." After commenting on how much Bob learned from Sol, he reflected on Sol's human side: "Sol was the archetypal absent minded professor. He forgot to come to my PhD qualifying oral – he was a member of my committee – and wandered off to have tea. Zohrab Kaprielian grabbed Lloyd Welch in the hall and drafted him as a substitute. When Lloyd's turn came out of the blue he asked me prove the Möbius inversion formula, which thanks to Sol, I did easily."

Sol received his bachelor's degree in mathematics from Johns Hopkins in advance of his 19th birthday. He has an MS and PhD from Harvard University in Mathematics. Prior to joining the University of Southern California, he held senior positions at the Jet Propulsion Laboratory in Pasadena. Sol passed away the day after the centennial of Claude Shannon's birth, he was 83. He will be missed by family, friends and the information theory community.

Sol's technical contributions were summarized by Guang Gong and Tor Helleseth; additional memories were put together by Benjamin Paul, Urbashi Mitra and Vijay Kumar.

References

- [1] Solomon W. Golomb. On the classification of Boolean functions. *IEEE Trans. on Inform. Theory*, 5:176–186, May 1959.
- [2] Solomon W. Golomb. Run-length encodings. *IEEE Trans. on Inform. Theory*, 12(3):399–401, 1966.
- [3] Solomon W. Golomb. Shift Register Sequences. Holden-Day, Inc., San Francisco, 1967, Revised edition, Aegean Park Press, Laguna Hills, CA, (1982).
- [4] Solomon W. Golomb. On the classification of balanced binary sequences of period 2^n-1 , *IEEE Trans. on Inform. Theory*, 26(6):730–732, Nov. 1980.

[5] Solomon W. Golomb. Algebraic constructions for costas arrays. *Journal Comb. Theory (A)*, 37:13-21, 1983.

[6] Solomon W. Golomb. Costas arrays – solved and unsolved problems. Keynote Lecture presented at the Symposium on Costas Arrays, at the *CISS Conference*, Princeton, NJ, March 22–26, 2006.

[7] Solomon W. Golomb. A career in technology. Keynote Lecture presented at the *ECE Distinguish Seminar Series*, University of Waterloo, August 12, 2015.

[8] Solomon W. Golomb and Richard Hess. Seating arrangements and Tuscan squares. *Ars Combinatoria*, 2015, to appear.

GOLOMB'S PUZZLE COLUMN™ COLLECTION, Part 1

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 con-

tribution to the newsletter, a collection of his earlier puzzles dated back to 2001 will appear in 4 compiled parts over the next 4 issues. Part 1 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™

SUMS AND PRODUCTS OF DIGITS

Solomon W. Golomb



For every positive integer n , let $S(n)$ be the sum of the decimal digits of n , let $P(n)$ be the product of the decimal digits of n , and let $R(n) = n/S(n)$, the ratio of n to the sum of the digits of n .

1. The equation $S(n) \cdot P(n) = n$ can also be written $P(n) = R(n)$. One solution is $n = 1$, where $S(n) = P(n) = R(n) = n = 1$. There are larger solutions, but only finitely many. Which ones can you find?

2. The ratio $R(n) = n/S(n)$ is sometimes an integer (e.g. when $n = 12$, $R(n) = 12/(1+2) = 4$) and sometimes not (e.g. when $n = 15$, $R(n) = 15/(1+5) = 2.5$). Does every positive integer m occur as $R(n)$ for some positive integer n ? If "yes", give a proof; if "no", find the smallest positive m which is never of the form $R(n)$.

3. For each positive integer k , determine which k -digit number n gives the minimum value (integer or not) of $R(n)$. (While this is a separate problem for each positive integer k , there is an interesting pattern to the solutions.)

4. For how many of the $9 \cdot 10^{k-1}$ k -digit integers is $R(n)$ an integer? (This value has been tabulated for $1 \leq k \leq 7$, but no closed form expression, or even a good asymptotic approximation, has yet been found.)

5. For each positive integer k , which k -digit number gives the smallest integer value of $R(n)$, and what are these values? (This behavior is far less regular than in Problem 3, and the explicit answer has only been found, by exhaustive search, for $1 \leq k \leq 7$.)

Note. Except for Problem 2, due to John H. Conway, the remaining problems are based on an unpublished paper of David Singmaster.

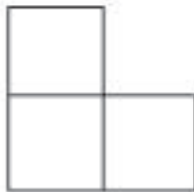
GOLOMB'S PUZZLE COLUMN™

TILINGS WITH RIGHT TROMINOES

—Solomon W. Golomb



A “right tromino” is the shape formed by three quadrants of a 2×2 square:



1. Show that no matter where a single “monomino” (1×1 square) is removed from a $2n \times 2n$ “board”, the rest can be *tiled* (covered exactly, with no gaps and no overlaps) by right trominoes. (*Hint*: Try mathematical induction.)
2. Where can (and where cannot) a monomino be removed from a 5×5 “board” so that the rest can be tiled with right trominoes?
3. Where can (and where cannot) a “domino” (1×2 square) be removed from a 5×7 “board” so that the rest can be tiled with right trominoes?
4. Where can (and where cannot) a monomino be removed from a 7×7 “board” so that the rest can be tiled with right trominoes?
5. Suppose $m > 7$ and m is not a multiple of 3. Show that a monomino can be removed from anywhere on an $m \times m$ board and the rest can then be tiled with right trominoes.
6. What are the values of a and b (both positive integers) such that the entire $a \times b$ board can be tiled with right trominoes?
(Clearly the product ab must be divisible by 3, but this necessary condition is not sufficient.)

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

GOLOMB'S PUZZLE COLUMN™

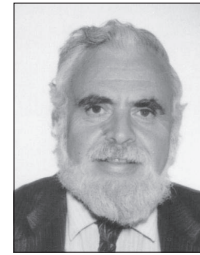
WHAT COLOR IS MY HAT?

Each of the n members of a team will be assigned a hat, either black or white in each case. No team members will see or be told the colors of their own hats, but each will have some information about the colors of the other members' hats. Different sets of rules for this are enumerated below. The team will know in advance what the rules are, and will have an opportunity to agree on a strategy before the contest begins. In general, when asked "What color is your hat?", a team member can answer either "White" or "Black" or "Pass". If any team member gives an incorrect answer ("Black" instead of "White", or "White" instead of "Black") the entire team loses. Also, if **every** team member says "Pass", the entire team loses. The objective is to maximize the probability that the team will *win*, which requires at least one correct answer and no incorrect answers.

Case 1. The n contestants will be lined up single file, and then will be assigned hats. Each will see all the hats in front of him/her, but not his/her own or those behind. They will be given the additional information: "Not all the hats are the same color". The last contestant in line will be the first to be asked "What color is your hat?", then the next-to-last, and so on. What strategy should the team adopt to guarantee a win?

Case 2. The n contestants will be assembled in a room where each one will see the color of every hat but his/her own. They will be asked "What color is your hat?" in random order, and each will hear all the answers. If they are assured that not all the hats are the same color, what winning strategy can the team adopt?

—Solomon W. Golomb



Case 3. Each contestant will be in a different hotel room (rooms numbered 1 to n), and will be told the colors of the hats of the contestants in each of the other $n - 1$ rooms, but not the color of his/her own hat. There will be no communication of any sort (verbal, visual, auditory, etc.) among the contestants once the hat colors are assigned, and no contestant will hear the answer of any other contestant to the question "What color is your hat?"

The n hat colors will be assigned independently and at random. Thus, all hats *might* be the same color, though this is unlikely if n is large. The objective, in the team's planning session, is to develop a strategy which will maximize the probability that the team will win. What strategy should they adopt, and what probability of winning will it achieve?

Notes and Hints.

1. The team could agree in advance that all but one of them will say "Pass", and the designated guesser will guess randomly (or could even specifically guess "White"), to give the team a 50% chance of winning. This strategy gives a lower bound, but surprisingly it can be improved upon for $n \geq 3$.
2. There is a non-trivial connection between this problem and a major topic in Information Theory.
3. Given any $\epsilon > 0$, there is an integer $N = N_\epsilon$ such that the optimum strategy will win with probability $\geq 1 - \epsilon$ provided that the number of team members n exceeds N_ϵ . (If $\epsilon = 2^{-k}$, then N_ϵ is easily calculated!)

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

GOLOMB'S PUZZLE COLUMN™

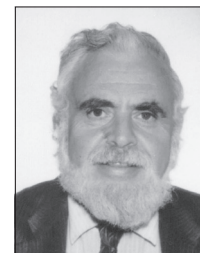
Some Combinatorial Questions

1. 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. [Thus, if the first ball to go had the number 4, the next must be either number 3 or number 5. If the first ball to go had the number 15, the next to go would have to be number 14.] How many possible sequences are there for the order in which all 15 balls go off the table?

2. 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 , $0 \leq \alpha \leq \pi$. What happens if $\pi < \alpha < 2\pi$?

3. Every permutation on n symbols $\{a_1, a_2, \dots, a_n\}$ can be written as a product of disjoint cycles whose cycle lengths

—Solomon W. Golomb



sum to n . Let L_n be the expected length of the longest cycle in a random permutation on n symbols, and let $\lim_{n \rightarrow \infty} \frac{L_n}{n} = \lambda$. 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 $\lim_{n \rightarrow \infty} P_n^{(1)}$ in terms of λ .

(To obtain probabilities and expected values for a "random" permutation on n symbols, simply take the average over all $n!$ permutations.)

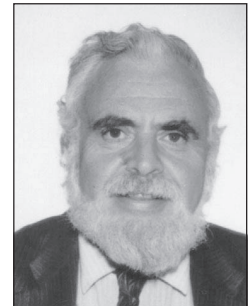
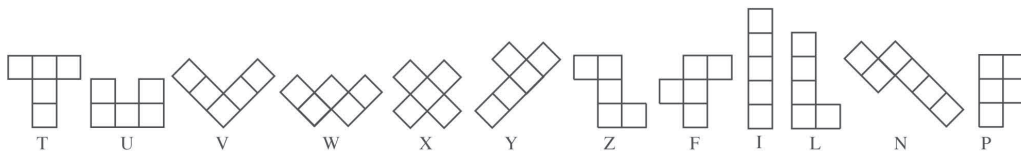
4. If n black beads and $n + 1$ white beads are placed on a string, and the ends of the string are joined to form a necklace, how many cyclically distinct necklaces can result?


GOLOMB'S PUZZLE COLUMN™

Placing Pentominoes on Boards

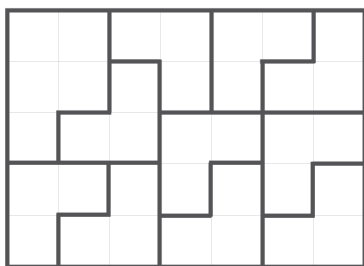
Solomon W. Golomb

The twelve pentominoes are the figures made of five edge-adjacent squares of equal size:



1. Your first assignment is to find all the distinct locations on a 5×7 board (distinct relative to the group of rotations and reflections of the 5×7 rectangle) where each one of the twelve pentominoes can be placed so that the rest of the 5×7 rectangle can be tiled with ten "right trominoes" ().

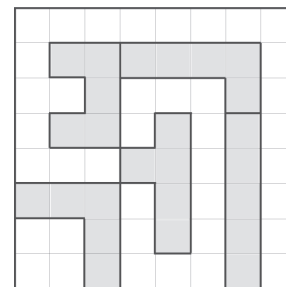
(A pentomino can be rotated and reflected at will, but its placement on the 5×7 board must match the grid lines.) We only care about distinct locations for the pentomino, and not about possible rearrangements of the ten right trominoes. Here is one solution for the P-pentomino:



There are at least three different locations for each pentomino, and as many as eight (in the cases of the P and Y). See how many you can find. (I have a total of 50. Can you improve on this?)

While this is largely trial and error, there are some guiding principles which greatly reduce the number of locations that need to be tried.

2. As shown in my book *Polyominoes* (in Figure 16), it is possible to place five pentominoes on the 8×8 board in such a way that none of the other seven pentominoes will fit, e.g.



On the 7×7 board, it is possible to place four pentominoes (following the grid lines) in such a way that none of the other eight pentominoes will fit. In particular, the I, L, and V pentominoes can be used with any one of the other nine pentominoes to prevent any of the remaining pentominoes from fitting on the board. Find an example for each of these nine cases. Finally, there is a set of four pentominoes which includes neither the I nor the V which can be placed on the 7×7 board to preclude the placement of any additional pentominoes. Can you find an example of this configuration?

It is quite common that there is more than one way to place the same four pentominoes on the 7×7 board to keep all the others off. You are asked to find only one placement for each set of four pentominoes, for a total of ten configurations. Among the 495 four-element subsets of the twelve pentominoes, this indicates that ten of them can be used to keep the remaining pentominoes off the 7×7 board. Is there an eleventh subset with this property? Or a twelfth?

3. The five pentominoes shown above (I, L, U, V, Y) can be rearranged in several ways and still succeed in preventing any of the other seven pentominoes from being placed on the 8×8 board. Find a *different* subset containing five of the twelve pentominoes which can be placed on the 8×8 board so as to exclude the remaining seven. (It may overlap, but not coincide, with the previous five-pentomino subset.)

GOLOMB'S PUZZLE COLUMN™

On a Problem of Richard Epstein

Solomon W. Golomb

I received the following letter from Bulgaria, dated 6 April, 2002:

Dear Prof. Golomb:

Recently, I attended a lecture by Dr. Richard Epstein here at the University of Sofia.

Seeking a number-theoretic problem for my master's thesis, Dr. Epstein kindly offered the hypothesis that "there is a closed [i.e. *finite*] set of numbers n such that the last digit(s) of n^2 is (are) the number n itself."

He gave the following examples:

n	n^2
5	25
6	36
25	625
76	5776
376	141,376
625	390,625

(ignoring the trivial $n = 1$).

Object: prove that no other examples exist.

Dr. Epstein suggested that if I should become stuck, I write to you for helpful hints. I am stuck. So would appreciate much your insights on this matter.

Sincerely,

Georghe Costello

One of the "hints" I sent him was that the hypothesis might be false. Here are some specific questions.

1. Are there more examples than the six listed? If so, exhibit the next one.

2. What is the general procedure for finding additional examples? (There is a Main Theorem for this.)

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

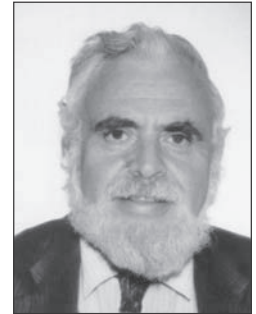
We generalize the problem from base 10 to base b as follows:

Let E_b be the "Epstein set" of positive integers $n > 1$ for which n^2 "ends in n " when both are written in base b .

4. Show that for prime values of b , E_b is empty.

5. Show that if $b = 2p$, where $p > 2$ is prime, then E_b contains p and $p + 1$.

6. For the case in problem 5., show how the complete solution for E_b parallels the special case when $b = 10$.



GOLOMB'S PUZZLE COLUMN™

EARLY BIRD NUMBERS

Solomon W. Golomb

Consider the sequence (*) consisting of the consecutive positive integers, written in decimal notation, with no intervening spaces or punctuation:

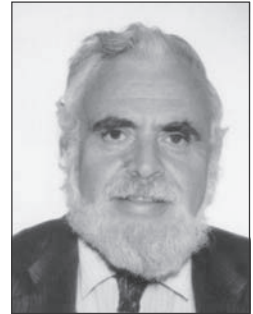
(*) 12345678910111213141516171819202122232425...

It is easy to show that if this sequence is preceded by a decimal point, the resulting real number is irrational and is "normal, to the base ten" (i.e. every sequence of k consecutive digits occurs in this sequence, asymptotically, with a frequency of 10^{-k}). It has also been shown that this real number is transcendental.

Martin Gardner has defined a positive integer to be an *early bird number* (e.b. no., for short), if it can be found in the sequence (*) earlier than its guaranteed place in the counting sequence. Thus, **12** is an e.b. no., since the sequence (*) begins with 12. So too is **718**, since we find it in (*) in the overlap of 17 and 18: (17)(18). On the other hand, the numbers from 1 to 11, inclusive, are *not* e.b. nos., nor are any two-digit numbers ending in "0". Here are some questions.

1. There are 90 two-digit integers from 10 through 99. Exactly half of these (i.e. 45) are e.b. nos. Can you describe which ones these are?
2. Suppose that n is a k -digit positive integer ($k > 1$) such that there is a cyclic permutation n' of the digits of n , where n' begins in a digit other than 0 and ends in a digit other than 9, and $n' < n$. Prove that n must be an e.b. no.

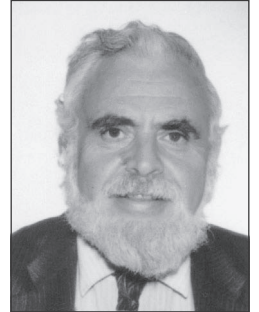
3. Is the previous statement still true if n' , the cyclic permutation of n with $n' < n$, is allowed to end with the digit 9? (Prove or disprove.)
4.
 - a. Show that every integer from 91 to 99 (inclusive) is an e.b. no.
 - b. Show that every integer from 901 to 999 is an e.b. no.
 - c. Prove or disprove: "Every integer from $9 \cdot 10^d + 1$ to $10^{d+1} - 1$ (inclusive) is an e.b. no., for all $d \geq 1$." (If true, give a proof. If false, exhibit counter-examples.)
5. Martin Gardner observed that "31415" (the first five digits of π) is an "early" e.b. no., occurring in the sequence (*) at (13)(14)(15). By the theorem in Problem 2, we can also get 31415 as an e.b. no. using either $n' = 14153$ or $n' = 15314$. (That is, n appears in the overlap of the consecutive integers (14153)(14154) and of (15314)(15315).) Find a 5-digit integer that has *six* different representations as an e.b. number.
6. Asymptotically, what percentage of all positive integers are e.b. numbers?



GOLOMB'S PUZZLE COLUMN™

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

Solomon W. Golomb



This time we will look at properties of the "central binomial coefficient", $\binom{2n}{n} = \frac{(2n)!}{(n!)^2}$. (Most of these are well-known.)

1. Prove these approximations:

a. $2^n < \binom{2n}{n} < 4^n$, all $n > 1$.

b. $\binom{2n}{n} \sim \frac{1}{\sqrt{\pi n}} 4^n$ as $n \rightarrow \infty$.

2. Prove these identities, for all $n \geq 1$.

a. $\binom{2n}{n} = \sum_{k=0}^n \binom{n}{k}^2$.

b. $\binom{2n}{n} = (-1)^n \sum_{k=0}^{2n} (-1)^k \binom{2n}{k}^2$.

c. $\binom{2n}{n} = 2(-1)^n \sum_{k=1}^{2n-1} (-1)^k \binom{2n-1}{k} \binom{2n-1}{k-1}$.

d. $\binom{2n}{n} = \prod_{j=1}^n \left(4 - \frac{2}{j}\right)$

3. Prove that each of the following must be an integer, for all $n \geq 1$.

a. $\frac{1}{n+1} \binom{2n}{n}$.

b. $\frac{1}{p} \binom{2n}{n}$, for each prime p , n , $p \leq 2n$.

c. $\frac{1}{R} \binom{2n}{n}$, where $R = 2 \prod_{n < p_j \leq 2n} p_j$

where p_j runs through all primes in $(n, 2n]$.

4. Let $L(n) = \text{l.c.m. } \{1, 2, 3, \dots, n\}$, let $L(x) = L(\lfloor x \rfloor)$ for real x , and set $L(x) = 1$ for $0 < x < 1$.

a. Show that $\binom{2n}{n}$ divides $L(2n)$.

b. Show that $\binom{2n}{n} = \prod_{k=0}^n \left\{ L\left(\frac{2n}{k}\right) \right\}^{(-1)^k}$, for all $n \geq 1$.

GOLOMB'S PUZZLE COLUMN™

Latin Squares and Transversals

– Solomon W. Golomb



A Latin Square of order n is an $n \times n$ array of n symbols (we will use $1, 2, \dots, n$ as the symbols), such that each symbol occurs once in each row and once in each column.

A Latin Square of order n is in standard form if the top row and the left-most column each contain the symbols $1, 2, \dots, n$ in sequential order.

A transversal of a Latin Square of order n is a set of n of the positions ("cells") of the square with one in each row, one in each column, and containing each of the n entries exactly once.

Here is an example of a Latin Square of order 5 in standard form in which the members of a transversal are circled.

1	2	3	4	5
2	5	1	3	4
3	4	5	1	2
4	1	2	5	3
5	3	4	2	1

The "multiplication table" (or "Cayley table") of a finite group is always a Latin Square; but Latin Squares, in general, are not "group tables". (They can be viewed as quasi-groups, which lack the associative law of groups, and are far more numerous than groups, as a function of the order n .)

Two Latin Squares of order n (not necessarily in standard form) are called orthogonal if the n^2 ordered pairs of corresponding elements are all distinct. An example with $n = 3$ is:

1	2	3
2	3	1
3	1	2

,

1	2	3
3	1	2
2	3	1

 with ordered pairs

11	22	33
23	31	12
32	13	21

Try to prove each of the following results.

1. If L is a Latin Square of order n , there is a second Latin Square L' of order n orthogonal to L if and only if L has n disjoint transversals.
 2. If L is the "Cayley table" of a group of order n , then there is a second Latin Square L' of order n orthogonal to L if and only if L has (at least) one transversal.
 3. If $p = n + 1$ is prime, $n > 1$, then the multiplicative group modulo p , viewed (from its Cayley table) as a Latin Square of order n , has no transversals.
 4. The number of Latin Squares of order n such that any two of them are orthogonal cannot exceed $n - 1$. ("The maximum number of Mutually Orthogonal Latin Squares – MOLS – of order n cannot exceed $n - 1$.")
 5. If a Latin Square of order n has $n - 1$ disjoint transversals, then it has n disjoint transversals (and therefore, in view of 1., an "orthogonal mate").
- Euler conjectured, and it was eventually proved, that a pair of orthogonal Latin Squares of order 6 does not exist.
6. Find a Latin Square of order 6 with 4 disjoint transversals.

GOLOMB 'S PUZZLE COLUMN™

Irreducible Divisors of Trinomials

Solomon W. Golomb



We consider trinomials over $GF(2)$ of the form $x^n + x^a + 1$, $0 < a < n$, and consider which irreducible polynomials $f(x)$ over $GF(2)$ may be divisors of trinomials and which ones may not.

If $f(x)$ is an irreducible polynomial of degree n over $GF(2)$, we define the *primitivity* t of $f(x)$ to be the smallest positive integer such that $f(x)$ divides $x^t - 1$, in

$GF(2)$ arithmetic. It is well known that t must be a factor of $2^n - 1$, and if $t = 2^n - 1$ we say that $f(x)$ is a *primitive* irreducible polynomial over $GF(2)$. Letting $r = (2^n - 1)/t$ this can be restated as " $f(x)$ is primitive iff $r = 1$ ". It is also well known that the primitivity t of $f(x)$ is the small-

est positive integer such that $\alpha^t = 1$, where α is any root of $f(x)$.

See which of the following statements you can prove. In all cases we take $f(x)$ to be an irreducible polynomial of degree n , $n > 1$ over $GF(2)$.

1. If $f(x)$ is primitive, then $f(x)$ divides infinitely many trinomials.
2. If $f(x)$ has primitivity t and $f(x)$ divides no trinomials of degree $< t$, then $f(x)$ divides no trinomials.
3. If $p \geq 5$ is a prime such that 2 is "primitive" modulo p (i.e. the powers $2^1, 2^2, 2^3, \dots, 2^{p-1} = 1$ are all distinct modulo p) then the polynomial $f(x) = 1 + x + x^2 + \dots + x^{p-1} = (x^p - 1)/(x - 1)$ is irreducible, and divides no trinomials.



GOLOMB'S PUZZLE COLUMN™

Overlapping Subsets

– Solomon W. Golomb

A former student in my undergraduate course in combinatorial analysis recently wrote to me with a question. The 900 students in the graduate program he is now attending are partitioned into 90-student sections (for manageable class sizes) in each of several courses. These partitionings are supposedly performed randomly, and independently from one course to another. Yet he estimates an overlap of about 25 students between “his” sections in two of these courses, which seemed highly improbable to him. He sought my assistance in addressing this issue.

1. Let's generalize to the following problem: From a set S of N elements, subsets A and B are formed, independently and at random, with a elements in A and b elements in B .

- What is the expected number M of overlaps between set A and set B ?
- What is the probability $pr(k)$ of exactly k overlaps between sets A and B ? (Use binomial coefficients in your answer.)
- From your answer to 1.b., obtain a fairly simple expression for the ratio $\frac{pr(k+1)}{pr(k)}$.

2. For the case $N = 900$, $a = b = 90$,

- What is the value of M ?
- Evaluate $\frac{pr(k+1)}{pr(k)}$ for each k , $0 \leq k \leq M + 2$.
- From your answer to 2.b., what is the *mode* of the distribution $\{pr(k)\}$? (That is, for what value of k is $pr(k)$ biggest?)

3. Stirling's approximation formula for $n!$ says $n! \sim \sqrt{2\pi n} \left(\frac{n}{e}\right)^n$, as $n \rightarrow \infty$, where $e = 2.718 \dots$ is the base of natural logarithms, and $\pi = 3.14159 \dots$

- In your answer to 1.b., substitute $N = 900$, $a = b = 90$, and then substitute Stirling's approximation for each of the factorials (in each of the binomial coefficients) for the case $k = M$.
- Simplify the expression in 3.a., by cancellation between numerator and denominator.
- What numerical value does 3.b. yield for $pr(M)$?

4. The Poisson Distribution with parameter λ , given by $Pr(k) = e^{-\lambda} \cdot \frac{\lambda^k}{k!}$ for integers $k \geq 0$, is often used to approximate other distributions with mean equal to λ .

- Using the value of M from problem 1.a., what value does the Poisson Distribution give at $\lambda = k = M$?
- The value of $pr(M)$ in 3.c. used the Stirling approximation to $n!$ Which approximation to the “true” value of $pr(M)$, from 3.c. or from 4.a., do you believe is closer?
- How does $\frac{Pr(k+1)}{Pr(k)}$ with $\lambda = M$ compare with $\frac{pr(k+1)}{pr(k)}$ in 2.b., for k in the interval $[M - 2, M + 2]$?

5. Use any approximation method to evaluate $pr(25)$ for the case in Problem 2. Was the student's intuition correct?

ITW 2016 CAMBRIDGE

Information Theory Workshop Call for Papers

11 - 14 September 2016

The 2016 IEEE Information Theory Workshop will take place from the 11th to the 14th September 2016 at Robinson College, Cambridge, United Kingdom.

Founded in 1209, the University of Cambridge is a collegiate university consisting of 31 constituent colleges. ITW 2016 will take place at Robinson College, the youngest of the Cambridge colleges founded in 1979, offering modern dedicated conference facilities in a cosy residential setup and easy access to the sights and attractions in central Cambridge that lie within a 10 minutes walk of the college.

Plenary Speakers

Yonina Eldar, *Technion—Israel Institute of Technology*
Andrew Blake, *Microsoft Research Cambridge*
Thomas Strohmer, *University of California, Davis*

Call for Papers

The 2016 IEEE Information Theory Workshop welcomes original technical contributions in all areas of information theory. The agenda includes both invited and contributed sessions, with a particular emphasis on the interface between:

- Information Theory, Statistics and Machine Learning
- Information Theory and Compressed Sensing
- Information Theory and Radar

Paper Submission

Authors are invited to submit previously unpublished papers, not exceeding five pages, according to the directions that will appear on the conference website: <http://sigproc.eng.cam.ac.uk/ITW2016>
The ITW proceedings will be published by the IEEE and will be available on IEEE Xplore.

Schedule

Paper Submission Deadline: 13th March 2016
Acceptance Notification: 12th June 2016
Final Paper Submission: 31st July 2016

General Co-Chairs

Deniz Gündüz, *Imperial College London*
David MacKay, *University of Cambridge*
Jossy Sayir, *University of Cambridge*

TPC Co-Chairs

Helmut Bölcskei, *ETH Zurich*
Robert Calderbank, *Duke University*
Miguel Rodrigues, *University College London*

Financial Chair

Ramji Venkataramanan, *University of Cambridge*

Publications Chair

Iñaki Esnaola, *University of Sheffield*

Publicity Chair

Michèle Wigger, *Telecom ParisTech*





The **Fifty-Fourth Annual Allerton Conference on Communication, Control, and Computing** will kick off with Opening Tutorials being held on Tuesday, September 27, 2016 at the Coordinated Science Laboratory. The conference sessions will start on Wednesday, September 28, 2016 through Friday, September 30, 2016, at the Allerton Park and Retreat Center. The Allerton House is located twenty-six miles southwest of the Urbana-Champaign campus of the University of Illinois in a wooded area on the Sangamon River. It is part of the fifteen-hundred acre Robert Allerton Park, a complex of natural and man-made beauty designated as a National natural landmark. Allerton Park has twenty miles of well-maintained trails and a living gallery of formal gardens, studded with sculptures collected from around the world.

Papers presenting original research are solicited in the broad areas of control, communication and computing, including but not limited to biological information systems; coding techniques and applications; coding theory; data storage; information theory; multiuser detection and estimation; network information theory; sensor networks in communications; wireless communication systems; intrusion/anomaly detection and diagnosis; network coding; network games and algorithms; performance analysis; pricing and congestion control; reliability, security and trust; decentralized control systems; robust and nonlinear control; adaptive control and automation; robotics; distributed and large-scale systems; complex networked systems; optimization; dynamic games; machine learning and learning theory; signal models and representations; signal acquisition, coding, and retrieval; detection and estimation; learning and inference; statistical signal processing; sensor networks; and data analytics.

Final versions of papers to be presented at the conference are required to be submitted electronically

Conference Co-Chairs: Minh Do and Naira Hovakimyan

Email: allerton-conf@illinois.edu

URL: www.csl.illinois.edu/allerton/

**COORDINATED SCIENCE LABORATORY AND THE
DEPARTMENT OF ELECTRICAL AND COMPUTER ENGINEERING
University of Illinois at Urbana-Champaign**

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

September 27, 2016 – Opening Tutorials
September 28 - 30, 2016 – Conference Sessions

CALL FOR PAPERS

by October 2, 2016 in order to appear in the Conference Proceedings and IEEE Xplore.

PLENARY LECTURE: Professor **Naomi Leonard** from the Mechanical and Aerospace Engineering, Princeton University, will deliver this year's plenary lecture. It is scheduled for Friday, September 30, 2016 at the Allerton Park and Retreat Center.

OPENING TUTORIAL LECTURES: Professor **Panagiotis Tsiotras**, Georgia Institute of Technology, and Professor **Emmanuel Abbe**, Princeton University, will both present tutorial lectures on Tuesday, September 27, 2016 at the Coordinated Science Laboratory, University of Illinois at Urbana-Champaign.

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

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

Manuscripts can be submitted during **June 15-July 8, 2016** with the submission deadline of July 8th being firm. Please follow the instructions at the Conference website: <http://www.csl.illinois.edu/allerton/>.

Authors will be notified of acceptance via e-mail by August 8, 2016, at which time they will also be sent detailed instructions for the preparation of their papers for the Proceedings.



Symposium Committee

General Co-Chairs

Toshiyasu Matsushima Waseda Univ
Robert Morelos-Zaragoza San Jose State Univ

General Secretaries

Tetsuya Sakai Waseda Univ
Ryo Nomura Senshu Univ

Finance

Yuichi Kaji NAIST
Tota Suko Waseda Univ

Publicity

Brian M. Kurkoski JAIST
Manabu Kobayashi Shonan Inst of Tech

Publications

Tetsunao Matsuta Tokyo Inst of Tech
Jun Muramatsu NTT
Hideki Yagi Univ of Electro-Comm

Registration

Shigeaki Kuzuoka Wakayama Univ
Takahiro Yoshida Yokohama College of Commerce

Local Arrangement

Tetsuya Kojima NIT, Tokyo College
Yoshifumi Ukita Yokohama College of Commerce

International Advisory Committee Co-Chairs

Toru Fujiwara Osaka Univ
Bin Yu Univ of California, Berkeley
Jos H. Weber Delft Univ of Tech

Technical Program Committee

TPC Co-Chairs

Hiroki Koga Univ. of Tsukuba
Christian Schlegel Dalhousie Univ

Secretary

Ken-ichi Iwata Univ. of Fukui

ISITA2016

October 30–November 2, 2016
Monterey, California, USA

The International Symposium on Information Theory and Its Applications (ISITA) is a leading conference on information theory. Since its inception in 1990, ISITA has been an exciting forum for interdisciplinary interaction, gathering leading researchers to discuss topics of common interest in the field of information theory. In 2016, the biennial ISITA will be held October 30–November 2 at the Hyatt Regency Monterey Hotel in Monterey, California, USA.

Call for Papers

Interested authors are invited to submit papers describing novel and previously unpublished results on topics in information theory and its applications, including, but not limited to:

- Error Control Coding
- Coded Modulation
- Communication Systems
- Detection and Estimation
- Signal Processing
- Rate-Distortion Theory
- Stochastic Processes
- Network Coding
- Shannon Theory
- Coding Theory and Practice
- Data Compression and Source Coding
- Data Storage
- Mobile Communications
- Pattern Recognition and Learning
- Multi-Terminal Information Theory
- Cryptography and Data Security
- Applications of Information Theory
- Quantum Information Theory

Paper Submission

Authors should submit papers according to the guidelines which will later appear on the conference website:

<http://www.isita2016.org/>

This link points to the permanent site <http://www.isita.ieice.org/2016/>. Accepted papers will appear in the symposium proceedings. To be published in *IEEE Xplore*, an author of an accepted paper must register and present the paper. IEEE does not guarantee inclusion in *IEEE Xplore*.

Schedule

Paper submission deadline April 7, 2016

Acceptance notification June 30, 2016

Further information on the technical program, plenary talks, social events and registration will be posted on the symposium web site as it becomes available.

The Asilomar Conference on Signals, Systems, and Computers will be held from November 6 to 9, 2016 in nearby Pacific Grove, California.

Financial Support
The Telecommunications
Advancement Foundation



Sponsor
Research Society of Information Theory and Its Applications,
Engineering Sciences Society, IEICE



Technical Co-Sponsor
IEEE Information Theory Society



Photo: Flickr/Raghuvara Ravikumar

IWCIT 2017

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

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

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

3-4 May 2017

Call for Papers

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

Shannon Theory

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

Communication Theory

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

Coding Theory

- Compressed sensing
- Data compression
- Network coding

Applications of Information Theory

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

Important Dates:

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

General Chairs:

- Aref, M. R.

Sharif University of Technology

- Salehi, J. A.

Sharif University of Technology

Technical Program Chair:

- Sharafat, A. R.

Tarbiat Modares University

Executive Chairs:

- Gohari, A.

Sharif University of Technology

- Seyfe, B.

Shahed University



IEEE
IRAN SECTION

Contact Us :

• Emails:

iwcit@sharif.ir

• Address:

Secretariat of IWCIT 2017 Rom 503 Dept. of Electrical Engineering

Sharif University of Technology Tehran, Iran

Tel : +98 21 66165910

WWW . IWCIT . COM



Call for Papers

RWTHAACHEN
UNIVERSITY

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 welcoming you to ISIT 2017 in Aachen.

General Co-Chairs
Rudolf Mathar
Gerhard Kramer

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

Finance Chairs
Meik Dörpinghaus
Volker Schanz

Publications Chairs
Giuseppe Durisi
Christoph Studer

Tutorial Chairs
Eduard Jorswieck
Jörg Kliewer



www.isit2017.org

VDE

ITG

Conference Calendar

DATE	CONFERENCE	LOCATION	WEB PAGE	DUE DATE
September 11–14, 2016	2016 IEEE Information Theory Workshop.	Cambridge, United Kingdom.	http://sigproc.eng.cam.ac.uk/ITW2016	Passed
September 27–30, 2016	54th Annual Allerton Conference on Communication, Control, and Computing.	Allerton Retreat Center, Monticello, Illinois, USA.	http://allerton.csl.illinois.edu	Passed
October 9–11, 2016	57th Annual IEEE Symposium on Foundations of Computer Science (FOCS 2015).	New Brunswick, New Jersey, USA.	http://www.wisdom.weizmann.ac.il/~dinuri/focs16/CFP.html	Passed
October 17–19, 2016	IEEE CNS 2016 3rd Workshop on Physical-Layer Methods for Wireless Security.	Philadelphia, PA, USA.	http://cns2016.ieee-cns.org	Passed
Oct. 30–Nov. 2, 2016	The International Symposium on Information Theory and Its Applications (ISITA).	Monterey, California	http://www.isita2016.org/	Passed
Nov. 16–18, 2016	International Conference on the Science of Electrical Engineering (ICSEE).	Eilat, Israel	http://www.ieee.org.il/icsee-2016/	Passed
December 4–8, 2016	IEEE GLOBECOM.	Washington DC, USA	http://globecom2016.ieee-globecom.org/	Passed
December 4–8, 2016 December 4, 2016	Workshop on Network Coding and Applications (IEEE Globcom NetCod 2016).	Washington DC, USA	http://www.netcod16.org/	Passed
December 4–8, 2016	Signal Processing for Big Data in Wireless Network (Globcom'16 workshop)	Washington DC, USA	http://comp.uark.edu/~wuj/spbd	Passed
December 7–9, 2016	IEEE Global Conference on Signal and Information Processing (GlobalSIP). Symposium on Information Theoretic Approaches to Security and Privacy	Washington DC, USA	http://www.ieeeglobalsip.org/	Passed
May 3–4, 2017	Iran Workshop on Communication and Information Theory.	Tehran, Iran	http://www.iwcit.com	January 11, 2017
June 25–30, 2017	2017 IEEE International Symposium on Information Theory.	Aachen, Germany	http://www.isit2017.org	January 16, 2017

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