IEEE Information Theory Society Newsletter

Vol. 62, No. 8, December 2012 Editor: Tara Javidi ISSN 1059-2362

President's Column

Muriel Médard

Writing my last column as your President coincides with putting the finishing touches on the quinquennial report for the IEEE review of our Society. Both activities naturally lead to retrospection and weighing of our future. Upon reading the last report, which was assembled under the leadership of Bixio Rimoldi for a review in early 2007, I was struck by the fact that the last five years have seen an outstanding number of initiatives and growth of activities. Our Society was lauded in the last report of IEEE thus: "The Society is well managed and well run. It is financially sound, with a successful conference and a prestigious publication". Yet, we have not remained content with our success, but have innovated considerably in the last five years. At our last review, IEEE was encouraging our Society to pursue a Student Committee, which at that time was incipient, having been started by Andrea Goldsmith. Since then, the activities of the Student Committee have touched a great number of our members. The Summer Schools are a constant success and have been so since their inception. I have fond memories of teaching at the first North American School of Information theory at Penn State. The activities of this Committee at ISIT and other of our related conferences, such as Allerton, are of great value to our students and junior members, as is readily evidenced by the heavy attendance they command. The Student Paper Award, which is now a highlight of ISIT, was inaugurated in 2007. Our website, which was also launched in 2007 under the leadership of Nick Laneman, has served as a nexus for information about the Society's activities and become a crucial part of our governance, for instance allowing the agenda and materials for BoG meetings to be made available ahead of time. Other features, such as highlighting of members, easy access to premiated papers, connections to Arxiv papers of interest and announcements of all sorts, make our Society accessible to our members at all times in dynamic, relevant fashion. Initiatives such as Women in the Information Theory Society (WithITS) and the Mentoring Committee have also come into being over the last few years and have provided mentoring, fellowship and professional support to our members. Our Distinguished Lecturers program, which began four years ago, has garnered considerable interest from local chapters and the requests are in clear expansion.

In matters of governance, much also has changed since 2007. We can now report to have an active and effective Conference Committee, whose head is a voting member of the BoG, to consider proposals for conferences, provide advice on their planning and running, as well as to serve as a precious collective memory of best practices. The Conference Committee is able to work with current and would-be organizers in an ongoing fashion. It also provides the BoG with thoroughly vetted recommendations for future conferences, as well as well-documented reports on accepted conferences, from the preparatory stages through the reporting process. We now also have an External Nominations Committee (ENC), which was instituted in February 2012 to promote recognition of our members' contributions. As our report states "The ENC consists of the External Nominations Committee Chair, the Society President and three additional members. The Chair and other members are appointed by the Nominations and Appointments Committee. Typically the members of the ENC will serve for two years, with staggered terms. The ENC is responsible for the solicitation, processing and submission on behalf of the Society of nominations for appropriate IEEE awards (such as, for example, the IEEE W. R. G. Baker Award) and, as applicable, for awards outside of the IEEE. The ENC also identifies worthy individuals who can be nominated for suitable awards – from within as well as without the IEEE – and requests and encourages distinguished appropriate nominators to take action."

continued on page 3

From the Editor

Tara Javidi

Dear IT Society members,

The last issue of 2012, naturally, contains Muriel Medard's last column as the IT society president. Please join me in thanking Muriel for continuing the tradition of excellence and growth as well as preparing such a thorough and detailed report of the work. With sadness, we pay tribute to Professors Irving Reed and Donald Tuft who passed away recently. I would like to thank Solomn Golomb for preparing the tribute for Irving Reed in addition to his regular puzzle contribution. I would also like to acknowledge the extensive effort that Louis Scharf, Leland Jackson and Cyndy Anderson (Don Tufts' daughter) have put in preparing the tribute to Don's work and life. Raymond Yeung has kindly provided us with a summary of his plenary talk at ISIT 2009 (to appear in the special issue of Communications in Information and Systems (CIS) soon). We also have reports from the student committee and 2012 European School of Information Theory. These are all in addition to our popular and regular contribution by our historian Tony Ephremides. Finally, we are experimenting with a new regular column with pointers to interesting blog items around the IT society.

As a reminder, 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 jointly at the IT Society website http://www.itsoc.org/, using the quick links "Share News" and "Announce an Event." Articles and columns also can be e-mailed to me at ITsocietynewsletter@ece.ucsd.edu with a subject line that includes the words "IT newsletter." The next few deadlines are:

Issue	Deadline
March 2013	January 10, 2013
June 2013	April 10, 2013
September 2013	July 10, 2013

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 hear your suggestions (especially regarding the new column) and contributions.

IEEE Information Theory Society Newsletter

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

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

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

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

Table of Contents

President's Column

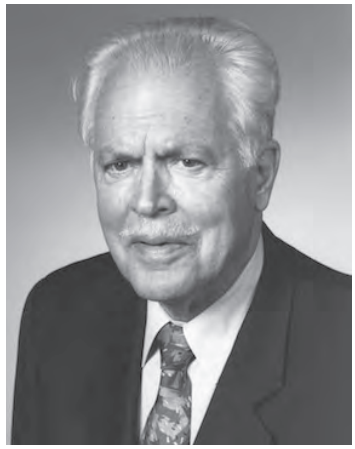
continued from page 1

Considering the future, it is clear that our members are still striving to strengthen our Society. The extensive report of the committee, headed by Abbas El Gamal, on the future of our Transactions, went well beyond its initial scope and shows the many possibilities and choices that lie ahead for us. I expect this report, which occupied a good part of the BoG meeting this past Fall, to furnish inspiration and material for considerable discussion for quite a while. At our last review, our Society was encouraged to "ensure further participation from industry in its activities, highlighting the relevance of its publications to the practitioner, perhaps through articles in its Newsletter, or else, through special issues". The committee, led by Michelle Effros, on education and outreach efforts, has reported once to the Board of Governors, particularly concerning lessons learned from other cognate communities, such as Computer Science, and will continue to guide the BoG's thinking in how to increase our impact as a Society. I look forward to its further reporting at the next BoG. The issue of prizes and recognitions in our Society is currently being considered by a committee, led by Paul Siegel. This committee is tasked with studying and proposing guidelines for named/endowed awards. This committee has a broad strategic chart but also is considering specific matters under discussion. An award that was agreed to in principle at the Board of Governors level, the Tom Cover Dissertation Award, and a proposed renaming of the Student Paper award after Jack Wolf, are being worked on by sub-committees. This arrangement allows us to consider these and other possible awards in a harmonized way and to provide a well-reasoned intellectual and practical framework for our Society's future awards.

It is with pride and pleasure that I shall represent our Society at the upcoming IEEE review. I am very grateful to the many people who have helped me assemble the report, with particular thanks to our Editor- in-Chief Helmut Boelsckei, Treasurer Aylin Yener, Conference Committee Chair Bruce Hajek, Senior Past President Frank Kschischang and Second Vice-President Abbas El Gamal. I am confident my successors, President-elect Gerhard Kramer, First Vice-President-elect Abbas El Gamal and Second Vice-President-elect Michelle Effros will benefit, as I have, from strong help and support from the members of the BoG and great number of volunteers. On a personal note, tinged with unavoidable wistfulness, I would like to thank you again for the immense privilege of being able to serve as your President.

Memorial Tribute for Irving Stoy Reed

(November 12, 1923–September 11, 2012)



Irving Stoy Reed was born on November 12, 1923, in Seattle, WA, and grew up in Fairbanks, AK, where he started college at the University of Alaska. He transferred to the California Institute of Technology (Caltech) in Pasadena, CA, from which he received his bachelor's, master's and Ph.D. degrees, all in Mathematics. He served as an enlisted man in the U.S. Navy during 1945–46, and was on the same ship in the Pacific on which David Huffman was the most junior naval officer. After his Navy service, while still a graduate student at Caltech, he was involved in the development of one of the very first digital computers, the Northrop MADDIDA Magnetic Drum Digital Differential Analyzer, used in aviation guidance systems.

From 1951 to 1960 he worked at MIT's Lincoln Laboratories, where he developed computer programming languages, the theory and analysis of radar systems, and the Reed-Muller and Reed-Solomon codes for protecting the integrity of digital information.

From 1960 to 1963 he was at the Rand Corporation in Santa Monica. He joined USC in 1963, and was a member of the Electrical Engineering faculty until his retirement in 1993 as Powell Chair of Engineering Emeritus.

At USC, Professor Reed was a key faculty member in the departments of Electrical Engineering and Computer Science, and a founding member of both the Communication Sciences Institute and the Signal and Image Processing Institute research groups. He worked with his graduate students on improved decoding algorithms for error-correcting codes, as well as the data compression methods that became the basis for the jpeg image standard that is ubiquitous for image storage and transmission.

He had an extraordinary range of knowledge and interests, including physics, electromagnetics, and aviation. He was a mathematician who realized how finite field theory had practical applications in error correcting codes that preserve the integrity of stored and transmitted digital information. This technology is now everywhere - in CDs, DVDs, disk drives, PDAs, cell phones, iPhones, wired and wireless communications, and computer networks that make up the Internet. It is fair to say that none of these would work without error correcting codes. He was an interdisciplinary research champion before it became necessary or fashionable.

His inquisitiveness and thinking in higher dimensions about different aspects of various issues are qualities that made his colleagues either delighted or exasperated.

He received many major awards in recognition of his technical contributions: member of the U.S. National Academy of Engineering, Fellow of the Institute of Electrical and Electronic Engineers (IEEE), its Hamming Award for Communications and the Shannon Prize, the highest award for Information Theory. In 1995, he shared with the late Gustave Solomon the IEEE Masaru Ibuka Award, and he received the IEEE Golden Jubilee Award for Technological Innovation. He died September 11, 2012, in Santa Monica, California.

The technology that Irving Reed developed has brought important and lasting benefits to society. We honor his memory and legacy as one of the exceptional innovators of the last 100 years.

In Memorium: Donald W. Tufts

Donald Winston Tufts, Emeritus Professor of Electrical and Computer Engineering at the University of Rhode Island, Kingston, passed away on August 9, 2012, at the age of 79. He is survived by his children Cynthia Tufts Anderson, David and John Tufts; two grandchildren, Jay and Katie Anderson; and his companion of 12 years, Sue Ross. Barbara Michelsen Tufts, his wife of 46 years and gracious host to Don's large family of professional friends, predeceased him in 2000.

Don grew up in Briarcliff Manor, NY, and attended the Hotchkiss School. Upon graduation he was awarded the prestigious Tyng Scholarship, which provided for his education at Williams College, where he earned a B.S. in Mathematics in 1955. At MIT he earned his S.B. in Electrical Engineering in 1957, his S.M. in Electrical Engineering in 1958, and his Sc.D. in 1960. From 1960–1967 he served as Harvard University Research Fellow & Lecturer, and Assistant Professor of Applied Mathematics. In 1967 he was appointed Professor of Electrical and Computer Engineering at the University of Rhode Island, where he served for 40 years, until his retirement in 2007. He served as academic advisor for more than 60 M.S. and Ph.D. students, many of whom are luminaries in information theory, communication, and signal processing.

Prof. Tufts dedicated his 47-year engineering career to teaching, research, and service in the fields of digital filtering, communication, and signal processing. He served his profession as a member of the Board of Governors of the Signal Processing Society, as a member of the IEEE Fellow Committee of the SPS, as a Distinguished Lecturer of the SPS Society, as a long-term President of the Providence Section of the IEEE, as Founding Chairman of the IEEE SPS Technical Committee on Sensors and Multichannel Signal Processing (SAM), and as Founder and Organizer of the biennial IEEE Workshop on Underwater Acoustic Signal Processing.

Prof. Tufts was instrumental in building an outstanding program at the University of Rhode Island for teaching and research in signal processing. His long-time colleague, G. Sadasiv, captured the essence of Prof Tufts: "There are some brilliant thinkers who, when you talk to them, make you feel small. But the truly brilliant thinkers make you feel great. Talking to them inspires you to a level where you seem to share understanding with them. Over the years, Don has made his department the kind of place a University department should be, where thinking is what you do and it is fun."

Prof. Tufts was Life Fellow of IEEE. He was elevated to Fellow Grade *"for contributions to communications and digital signal processing."* In 2000 he received an IEEE Millennium Medal and the Technical Achievement Award of the IEEE Signal Processing Society. In 2003 he received the Technical Achievement Award of the IEEE Workshop on Underwater Acoustic Signal Processing, with the citation, *for contributions to sonar, radar, speech, and communication, through his 40 years of research, service, and teaching in signal processing.* In the same year he received an IEEE Award from the Providence Section, *"for 35 years of support and dedication, 1968–2003."* At the University of Rhode Island, he received the College of Engineering Research Excellence Award in 1987, and the University Scholarly Achievement Award in1998.

Prof. Tufts was an active and sought-after consultant to industry and government, consulting to Bell Laboratories, Sanders (now BAE), the National Research Council of the National Academy of Sciences, the Office of Naval Research, and the Institute for Defense Analysis. He held seven patents for speech, digital filtering, computation of the Fourier Transform, and neural networks.

Prof. Tufts' teaching and research interests ranged from the theory and application of communication and signal processing to digital filters and computer architectures for implementing real-time algorithms. He was imaginative, creative, and iconoclastic, often challenging conventional wisdom. His education in mathematics formed the foundation for his research and teaching, but he was always guided by the physics that was revealed by measurements.

In his PhD dissertation, Tufts cracked the Nyquist problem of jointly optimizing transmitters and receivers for transmitting PAM data over ISI channels. This paper, D.W. Tufts, "Nyquist's problem—The joint optimization of transmitter and receiver in pulse amplitude modulation," Proc. IEEE, vol. 53, no. 3, pp 248–259, March 1965, has been reprinted as an IEEE reprint classic, and it may be said to be the antecedent for the modern literature on precoder and equalizer design for communication over MIMO channels. The paper previewed the Tufts style of working fundamental problems, with careful attribution to those who had preceded him.

An example of Tufts' early contributions to digital filtering is the paper, D.W. Tufts and J.T. Francis, "Designing digital low-pass filters—Comparison of some methods and criteria," IEEE Trans

Audio and Electroacoustics, vol. 18, no. 4, pp 487–494, December 1970, on the design of low-pass digital FIR filters. This paper was one of the earliest papers to be published on digital filter design, based on optimization principles.

In D.W. Tufts and J.T. Francis, "Estimation and tracking of parameters of narrowband signals by iterative processing," IEEE Trans Information Theory, vol. 23, no. 6, pp 742–751, November 1977, and D.W. Tufts and R.M. Rao, "Frequency tracking by MAP demodulation and by linear prediction techniques," Proc. IEEE, vol. 65, no. 8, pp 1220–1221, Aug. 1977, Tufts and his collaborators began to look at the problem of amplitude, phase, and frequency estimation, based on the principle of maximum aposteriori probability. Their results dispelled the commonly held belief that the best one can do in approaching optimum demodulation of angle-modulated signals is to use a phase-locked loop.

In 1982, Tufts and Kumaresan began publication of a series of revolutionary papers on phase, frequency, and wavenumber estimation, using modifications of linear prediction (e.g., D.W. Tufts and R. Kumaresan, "Estimation of Frequencies of Multiple Sinusoids: Making Linear Prediction Perform like Maximum Likelihood," Proceedings of the IEEE, vol. 70, no. 9, pp 975–989, September 1982, and R. Kumaresan and D.W. Tufts, "Estimating the Parameters of Exponentially Damped Sinusoids and Pole-Zero Modeling in Noise," IEEE Transactions on Acoustics, Speech, and Signal Processing, vol. 30, no. 6, pp 833–840, December 1982). The key insight was that these problems involved what might be called an impulse or natural response of an AR filter, observed in noise, rather than the response of an AR filter to noise. That is, the noise entered at the output, not the input. These papers, two of the most influential papers ever published in IEEE journals, revolutionized the practice of linear prediction on noisy data and introduced the signal processing community to the power of matrix approximation by singular value decomposition. They produced a flurry of activity in frequency estimation, spectrum analysis and direction-of-arrival estimation in time series analysis and array processing. Moreover, they have influenced subsequent generations of students and researchers, who now think naturally about signal processing in low-dimensional signal subspaces. You have to read the SP Transactions before 1982 and after 1982 to appreciate how profoundly these papers have changed the modeling and processing of radar, sonar, and communication signals.

In D.W. Tufts, A.C. Kot, and R.J. Vaccaro, "The threshold analysis of SVD-based algorithms," Proc. IEEE International Conf on Acoustics, Speech, and Signal Processing, vol. 4, pp 2416–2419, 11–14, April 1988, and J.K. Thomas, L.L. Scharf, and D.W. Tufts, "The probability of a subspace swap in the SVD," IEEE Transactions on Signal Processing, vol. 43, no. 3, pp 730–736, March 1995, Tufts and his collaborators analyzed the threshold effect of signal processing algorithms that use the singular value decomposition (SVD). The method of analysis is applicable to a broad class of parameter estimation methods in which a principal-component technique or low rank approximation is used to approximate the signal component of a matrix. These papers continue to influence work on performance breakdown in parametric methods of signal processing for radar and sonar. In F. Li, R.J. Vaccaro, and D.W. Tufts, "Unified performance analysis of subspace based estimation algorithms," IEEE International Conference on Acoustics, Speech, and Signal Processing, vol. 5, pp 2575–2578, 3–6 April 1990, Tufts and his collaborators presented a unified performance analysis of subspace-based algorithms for direction-of-arrival (DOA) estimation involving multiple signal arrivals in array signal processing. In A. A. Shah and D.W. Tufts: "Determination of the dimension of a signal subspace from short data records," IEEE Trans on Signal Processing, vol 42, no. 9, pp 2531–2535, Sept. 1994, the authors addressed the problem of order determination from short data records, from the point of view of null hypothesis testing.

In G.F. Boudreaux-Bartels, D.W. Tufts, P. Dhir, G. Sadasiv, G. Fischer, "Analysis of errors in the computation of Fourier coefficients using the arithmetic Fourier transform (AFT) and summation by parts (SBP)," Proc. IEEE International Conf on Acoustics, Speech, and Signal Processing, vol. 2, pp 1011–1014, 23–26 May 1989, and I.S. Reed, M.T. Shih, E. Henden, T.K. Truong, D.W. Tufts, "A VLSI architecture for simplified arithmetic Fourier transform algorithm," IEEE Trans Signal Processing, vol. 40, no. 5, pp 1122-1133, May 1992, Tufts and his collaborators reported VSLI architectures for computing the arithmetic Fourier transform. One of the architectures proposed was a butterfly architecture identical to Brun's original 1903 AFT algorithm, a finding that once again revealed Tufts' respect for the historical record.

In D. W. Tufts, E.C. Real, and J.W. Cooley, "Fast Approximate Subspace Tracking (FAST)," Proc. 1997 IEEE Conference on Acoustics, Speech, and Signal Processing, vol. 1, pp 547–550, 21–24 Apr 1997, and James M. Cooley, Timothy M. Toolan and Donald W. Tufts, "A Subspace Tracking Algorithm Using the Fast Fourier Transform," IEEE Signal Processing Letters, vol. 11, no. 1, pp 30–32, January 2004, Tufts and his collaborators published fast algorithms for tracking singular values, singular vectors, and subspace dimension from overlapping sequences of data matrices.

Don balanced his active life of scholarship with a dedication to Community Service, in partnership with his late wife, Barbara. He served two terms as Chairman of the School Committee in East Greenwich, RI, a term as Moderator of the Fire District, and a term on the Town Council. She served as President of the Town Council for East Greenwich and established the Co-operative Preschool subsequently named in her honor. In their frequent travels to Don's technical meetings, Barbara always made it a point to attend the local meeting of her beloved Rotary International.

Don was a sophisticated, intellectual man with charming, courtly manners. He never dwelled on himself or his accomplishments. He is remembered for his intellectual influence, the originality of his contributions to communication, digital filtering, and signal processing; and for his kindness, generosity, and concern for others.

Contributions in memory of Prof. Tufts may be made to the Barbara M. Tufts Cooperative Preschool, 1558 South County Trail, East Greenwich, RI, 02818, or to the Donald W. Tufts Memorial Lecture Fund, University of Rhode Island Foundation, 79 Upper College Road, Kingston, RI 02881.

Facets of Entropy

Plenary Talk at ISIT 2009, Seoul, Korea, June, 2009.

Raymond Yeung
Institute of Network Coding and Department of Information Engineering
Chinese University of Hong Kong
whyeung@ie.cuhk.edu.hk.

Constraints on the entropy function are of fundamental importance in information theory. For a long time, the polymatroidal axioms, or equivalently the nonnegativity of the Shannon information measures, are the only known constraints. Inequalities that are implied by nonnegativity of the Shannon information measures are categorically referred to as Shannon-type inequalities. If the number of random variables is fixed, a Shannon-type inequality can in principle be verified by a software package known as ITIP. A non-Shannon-type inequality is a constraint on the entropy function which is not implied by the nonnegativity of the Shannon information measures. In the late 1990s, the discovery of a few such inequalities revealed that Shannon-type inequalities alone do not constitute a complete set of constraints on the entropy function. In the past decade or so, connections between the entropy function and a number of subjects in information sciences, mathematics, and physics have been established. These subjects include probability theory, network coding, combinatorics, group theory, Kolmogorov complexity, matrix theory, and quantum mechanics. This expository work is an attempt to present a picture for the many facets of the entropy function.

Keywords: Entropy, polymatroid, non-Shannon-type inequalities, positive definite matrix, quasi-uniform array, Kolmogorov complexity, conditional independence, network coding, quantum information theory.

1. Preliminaries

Let $[n] = \{1, \ldots, n\}$, $\mathbf{N} = 2^{[n]}$, and $\overline{\mathbf{N}} = \mathbf{N} \backslash \{\emptyset\}$. Let $\Theta = \{X_i, i \in [n]\}$ be a collection of n discrete random variables. We will not discuss continuous random variables until Section 3.6, so unless otherwise specified, a random variable is assumed to be discrete. Let p_X denote the probability distribution of a random variable X. The entropy (Shannon entropy) [2] of X is defined by

$$H(X) = -\sum_x p_X(x) \log p_X(x).$$

The base of the logarithm is taken to be some convenient positive real number. When it is equal to 2, the unit of entropy is the *bit*. Likewise, the joint entropy of two random variables X and Y is defined by

$$H(X, Y) = -\sum_{x,y} p_{XY}(x, y) \log p_{XY}(x, y).$$

This definition is readily extendible to any finite number of random variables. All summations are assumed to be taken over the support of the underlying distribution. For example, for $H(X, Y)$ above, the summation is taken over all x and y such that $p_{XY}(x, y) > 0$.

Note that the quantity $H(X)$ is defined upon the distribution p_X and does not depend on the actually values taken by X. Therefore, we also write $H(p_X)$ for $H(X)$, $H(p_{XY})$ for $H(X, Y)$, etc.

In information theory, entropy is the measure of the uncertainty contained in a discrete random variable, justified by fundamental coding theorems. For comprehensive treatments of information theory, we refer the reader to [7, 19, 65].

For n random variables, there are $2^n - 1$ joint entropies. For example, for $n = 3$, the 7 joint entropies are

$$H(X_1), H(X_2), H(X_3), H(X_1, X_2), H(X_2, X_3),$$
$$H(X_1, X_3), H(X_1, X_2, X_3).$$

For $\alpha \in \mathbf{N}$, write $X_\alpha = (X_i, i \in \alpha)$, with the convention that $X_\emptyset$ is a constant. For example, $X_{\{1,2,3\}}$, or simply X_{123}, denotes (X_1, X_2, X_3). For a collection Θ of n random variables, define the set function $H_\Theta : \mathbf{N} \to \Re$ by

$$H_\Theta(\alpha) = H(X_\alpha), \quad \alpha \in \mathbf{N},$$

with $H_\Theta(\emptyset) = 0$ because $X_\emptyset$ is a constant. H_Θ is called the *entropy function* of Θ.[1]

In information theory, in addition to entropy, the following information measures are defined:

Conditional Entropy

$$H(X|Y) = H(X, Y) - H(Y)$$

Mutual Information

$$I(X; Y) = H(X) + H(Y) - H(X, Y)$$

Conditional Mutual Information

$$I(X; Y|Z) = H(X, Z) + H(Y, Z) - H(X, Y, Z) - H(Z).$$

Together with entropy, these are called the *Shannon information measures*. Note that all the Shannon information measures are linear combinations of entropies.

*R. W. Yeung's work was partially supported by a grant from the University Grants Committee (Project No. AoE/E-02/08) of the Hong Kong Special Administrative Region, China.

[1] Motivated by the consideration of the capacity of networks, Hassibi and Shadbakht [55] introduced the *normalized* entropy function and studied its properties. In their definition, X_i, $i \in [n]$ are assumed to have the same alphabet size N, and $H_\Theta(\alpha) = (\log N)^{-1} H(X_\alpha)$.

An information expression refers to a function of the Shannon information measures involving a finite number of random variables. Thus an information expression can be written as a function of entropies, called the *canonical form* of the information expression. The uniqueness of the canonical form of a linear information expression was first proved by Han [12] and independently by Csiszár and Körner [16]. The uniqueness of the canonical form of more general information expressions was proved by Yeung [26]. Therefore, to study constraints on the Shannon information measures, it suffices to study constraints on the entropy function.

2. Shannon-Type and Non-Shannon-Type Inequalities

Fujishige [15] showed that for any Θ, H_Θ satisfies the following properties, known as the *polymatroidal axioms*: For any $\alpha, \beta \in \mathbf{N}$,

i) $H_\Theta(\phi) = 0$;

ii) $H_\Theta(\alpha) \le H_\Theta(\beta)$ if $\alpha \subset \beta$;

iii) $H_\Theta(\alpha) + H_\Theta(\beta) \ge H_\Theta(\alpha \cap \beta) + H_\Theta(\alpha \cup \beta)$.

On the other hand, it is well known that all Shannon information measures are nonnegative, i.e.,

$$\begin{aligned} \text{entropy} &\ge 0 \\ \text{conditional entropy} &\ge 0 \\ \text{mutual information} &\ge 0 \\ \text{conditional mutual information} &\ge 0. \end{aligned}$$

These inequalities are referred to as the *basic inequalities* of information theory. Note that the nonnegativity of conditional mutual information implies all the other forms of basic inequalities, and is therefore the most general form of basic inequalities. It can be shown that the polymatriodal axioms on the entropy function are equivalent to the basic inequalities [38, App. 13.A].

When we say that the entropy function satisfies the polymatroidal axioms, it means that for any joint distribution defined for $X_1, X_2, \ldots, X_n$, the corresponding $2^n - 1$ joint entropies satisfy these axioms. The same interpretation applies when we say that a constraint on the entropy function is valid. A constraint can be very general, with inequality and identity being special cases.

Constraints on the entropy function govern the "impossibilities" in information theory. The proofs of most converse coding theorems rely on such constraints. For a long time, the polymatroidal axioms were the only known constraints on the entropy function. In the 1980's, Pippenger [18][2] asked whether these exist constraints on the entropy function other than the polymatroidal axioms. He called constraints on the entropy function the *laws of information theory*. If there are additional constraints on the entropy function, then perhaps new converse coding theorems can be proved.

In the 1990's, Yeung [26] studied constraints on the entropy function and introduced the following geometrical formulation of the problem. First, the number of random variables n is fixed to be some positive integer. Compared with [18], this makes the setting of the problem finite dimensional instead of infinite dimensional, and hence more manageable. Let $\mathcal{H}_n \triangleq \Re^{2^n-1}$, where the coordinates of $\mathcal{H}_n$ are labeled by $h_\alpha, \alpha \in \overline{\mathbf{N}}$. We call $\mathcal{H}_n$ the *entropy space* for n random variables. Then for each collection Θ of n random variables, H_Θ can be represented by a vector $\mathbf{h}^\Theta \in \mathcal{H}_n$, called the *entropy vector* of Θ, whose component corresponding to α is equal to $H_\Theta(\alpha)$ for all $\alpha \in \overline{\mathbf{N}}$. On the other hand, a vector $\mathbf{h} \in \mathcal{H}_n$ is called *entropic* if it is equal to the entropy vector of some collection Θ of n random variables. Define the following region in $\mathcal{H}_n$:

$$\Gamma_n^* = \{\mathbf{h} \in \mathcal{H}_n : \mathbf{h} \text{ is entropic}\}.$$

The region Γ_n^*, or simply Γ^* when n is not specified, is referred to as the region of entropy functions. If Γ_n^* can be determined, then in principle all valid constraints on the entropy function can be determined.

Consider an entropy inequality of the form $f(\mathbf{h}) \ge 0$.[3] For example, the inequality

$$H(X_1) + H(X_2) \ge H(X_1, X_2)$$

corresponds to $f(\mathbf{h}) \ge 0$ with $f(\mathbf{h}) = h_1 + h_2 - h_{12}$. The above setup enables constraints on the entropy function to be interpreted geometrically. Specifically, an entropy inequality $f(\mathbf{h}) \ge 0$ is valid if and only if

$$\Gamma_n^* \subset \{\mathbf{h} \in \mathcal{H}_n : f(\mathbf{h}) \ge 0\}.$$

In fact, $f(\mathbf{h}) \ge 0$ is valid if and only if

$$\overline{\Gamma}_n^* \subset \{\mathbf{h} \in \mathcal{H}_n : f(\mathbf{h}) \ge 0\}$$

because $\{\mathbf{h} \in \mathcal{H}_n : f(\mathbf{h}) \ge 0\}$ is closed. Figure 1(a) and (b) illustrates the two possible scenarios for $f(\mathbf{h}) \ge 0$.

In information theory, we very often deal with information inequalities with certain constraints on the joint distribution of the random variables involved. These are called constrained information inequalities, and the constraints on the joint distribution can

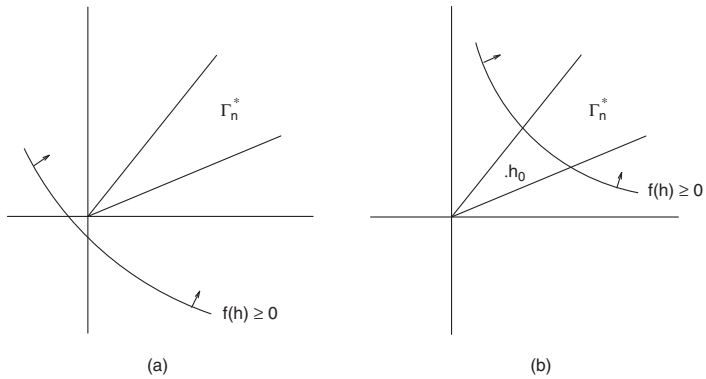


Fig. 1. (a) Γ_n^* is contained in $\{\mathbf{h} \in \mathcal{H}_n : f(\mathbf{h}) \ge 0\}$. (b) Γ_n^* is not contained in $\{\mathbf{h} \in \mathcal{H}_n : f(\mathbf{h}) \ge 0\}$. In this case, there exists an entropy vector $\mathbf{h}_0$ that does not satisfy $f(\mathbf{h}) \ge 0$.

[2]The author would like to thank Prof. Nick Pippenger for pointing out his work.

[3]We consider only non-strict inequalities because these are the inequalities usually used in information theory.

usually be expressed as linear constraints on the entropies. For example, $X_1 \to X_2 \to X_3 \to X_4$ forms a Markov chain if and only if $I(X_1; X_3|X_2) = 0$ and $I(X_1, X_2; X_4|X_3) = 0$. Under this Markov constraint, $I(X_2; X_3) \geq I(X_1; X_4)$, called the *data processing inequality*, is well known.

We now define another region Γ_n in $\mathcal{H}_n$ that corresponds to the basic inequalities (for n random variables):

$$\Gamma_n = \{\mathbf{h} \in \mathcal{H}_n : \mathbf{h} \text{ satisfies the basic inequalities}\}.$$

(The region Γ_n is written as Γ when n is not specified.) Note that Γ_n is a polytope in the positive orthant of $\mathcal{H}_n$ (and so it is computable), and $\Gamma_n^* \subset \Gamma_n$ because the basic inequalities are satisfied by any $X_1, X_2, \ldots, X_n$. An entropy inequality $f(\mathbf{h}) \geq 0$ is called a *Shannon-type inequality* if it is implied by the basic inequalities, or

$$\Gamma_n \subset \{\mathbf{h} \in \mathcal{H}_n : f(\mathbf{h}) \geq 0\}.$$

Constrained Shannon-type inequalities, namely those constrained inequalities that are implied by the basic inequalities, can also be formulated in terms of Γ_n [26].

This formulation of Shannon-type inequalities enables machine proving of such inequalities (both unconstrained and constrained), namely that a Shannon-type inequality can be verified by solving a linear program. See [26] for a detailed discussion. ITIP, a software package for this purpose that runs on MATLAB, was developed by Yeung and Yan [25]. A platform-independent version of ITIP that runs on C, called Xitip, was developed by Pulikkoonattu *et al*. [64]. Another software package for the same purpose that is axiom based was developed by Chung [66].

With ITIP, there is now a way to determine whether an entropy inequality is Shannon-type or not. Specifically, if an inequality can be verified by ITIP, then it is a Shannon-type inequality, otherwise it is not. Thus we are in a position to discuss whether there exist entropy inequalities beyond Shannon-type inequalities. If so, these inequalities would be called non-Shannon-type inequalities.

Let $\bar{\Gamma}_n^*$ denote the closure of Γ_n^*. Zhang and Yeung [27] proved the following fundamental properties of the region Γ_n^*:

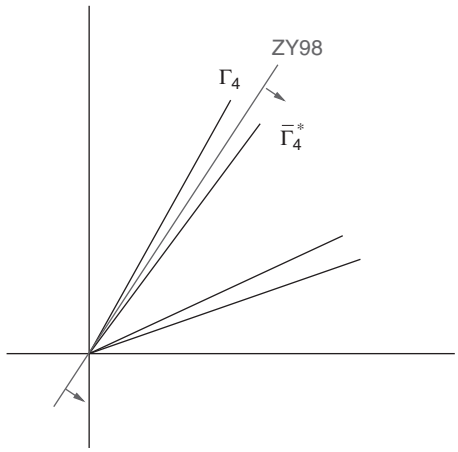


Fig. 2. An illustration of non-Shannon-type inequality ZY98.

i) $\Gamma_2^* = \Gamma_2$;

ii) $\Gamma_3^* \neq \Gamma_3$, but $\bar{\Gamma}_3^* = \Gamma_3$;[4]

iii) For $n \geq 3$, Γ_n^* is neither closed nor convex, but $\bar{\Gamma}_n^*$ is a convex cone.

Therefore, unconstrained non-Shannon-type inequalities can exist only for 4 or more random variables. In the same work, the following constrained non-Shannon-type inequality for 4 random variables was proved.

Theorem 1 (ZY97) *For any four random variables X_1, X_2, X_3, and X_4, if $I(X_1; X_2) = I(X_1; X_2|X_3) = 0$, then*

$$I(X_3; X_4) \leq I(X_3; X_4|X_1) + I(X_3; X_4|X_2).$$

The inequality ZY97 implies the existence of a non-entropic region on the boundary of Γ_4. However, this alone is not sufficient to establish that $\bar{\Gamma}_4^*$ is strictly smaller than Γ_4. Shortly afterwards, Zhang and Yeung [29] proved the following unconstrained non-Shannon-type inequality for 4 random variables, showing that indeed $\bar{\Gamma}_4^* \neq \Gamma_4$.

Theorem 2 (ZY98) *For any four random variables X_1, X_2, X_3, and X_4,*

$$2I(X_3; X_4) \leq I(X_1; X_2) + I(X_1; X_3, X_4) + 3I(X_3; X_4|X_1) + I(X_3; X_4|X_2).$$

The inequality ZY98 cut through the gap between $\bar{\Gamma}_4^*$ and Γ_4. This is illustrated in Figure 2.

This inequality has been further generalized by Makarychev *et al*. [37], Zhang [46], and Matúš [58]. In particular, Matúš showed that $\bar{\Gamma}_n^*$ is not a polyhedral cone, and hence there exist infinitely many linear non-Shannon-type inequalities. On the other hand, by modifying ITIP, Dougherty *et al*. [50] have discovered a number of non-Shannon-type inequalities by a search on a supercomputer.

3. Connections with Information Sciences, Mathematics, and Physics

The study of constraints on the entropy function was originally motivated by information theory, but subsequent to the discovery of the first non-Shannon-type inequalities, fundamental connections have been made between information theory and various branches of information sciences, mathematics, and physics. These connections reveal "non-Shannon-type" inequalities for finite groups, Kolmogorov complexity, and positive definite matrices. Inspired by the existence of non-Shannon-type inequalities for the Shannon entropy, new inequalities have been discovered for the von Neumann entropy. In this section, we give a guided tour for each of these connections. We also refer the reader to Chan [69] for an alternative discussion.

3.1 Combinatorics

Consider a finite alphabet $\mathcal{X}$. For a sequence $\mathbf{x} \in \mathcal{X}^n$, let $N(x; \mathbf{x})$ be the number of occurrences of x in $\mathbf{x}$, and let

[4]Previously, Han [17] proved that Γ_3 is the smallest cone that contains Γ_3^*. The result $\bar{\Gamma}_3^* = \Gamma_3$ was also proved by Golić [20], and is also a consequence of the theorem in Matúš [21].

$q(x) = n^{-1}N(x;\mathbf{x})$. The distribution $q_X = \{q(x)\}$ is called the *empirical distribution* of $\mathbf{x}$.

Central in information theory is the notion of *typical sequences* with respect to a probability distribution defined on some alphabet. Consider any probability distribution p_X on $\mathcal{X}$. Roughly speaking, we say that a sequence $\mathbf{x} \in \mathcal{X}^n$ is typical with respect to p_X if its empirical distribution manifests in some way the distribution p_X. There are different ways to measure the typicality of a sequence. Here we focus on the notion of *strong typicality* [6, 13, 16], and we adopt the definitions in [65].[5] Detailed discussions of the related fundamental results can be found therein.

Definition 1 *The strongly typical set $T^n_{[X]\delta}$ with respect to p_X is the set of sequences $\mathbf{x} \in \mathcal{X}^n$ such that $N(x;\mathbf{x}) = 0$ for all x with $p(x) = 0$, and*

$$\| p_X - q_{\mathbf{x}} \| \le \delta,$$

where $\|\cdot\|$ denotes the L^1-norm, and δ is an arbitrarily small positive real number. The sequences in $T^n_{[X]\delta}$ are called strongly δ-typical sequences.

This definition can readily be extended to the bivariate case. Here we consider a joint alphabet $\mathcal{X} \times \mathcal{Y}$, a joint probability distribution p_{XY} on $\mathcal{X} \times \mathcal{Y}$, and sequences $(\mathbf{x}, \mathbf{y}) \in \mathcal{X}^n \times \mathcal{Y}^n$. The notations we use for the single-variate case are extended naturally. It suffices to say that a pair of sequences $(\mathbf{x}, \mathbf{y}) \in \mathcal{X}^n \times \mathcal{Y}^n$ is jointly δ-typical with respect to p_{XY} if $N(x, y; \mathbf{x}, \mathbf{y}) = 0$ for all (x, y) such that $p(x, y) = 0$ and $\|p_{xy} - q_{xy}\| \le \delta$, and the strongly jointly typical set is denoted by $T^n_{[XY]\delta}$. Further extension to the multivariate case is straightforward.

For convenience, we write $H(X)$ for $H(p_X)$, $H(Y)$ for $H(p_Y)$, and $H(X, Y)$ for $H(p_{XY})$. By the *strong asymptotic equipartition property* (strong AEP), for sufficiently large n, $|T^n_{[X]\delta}| \approx 2^{nH(X)}$, $|T^n_{[Y]\delta}| \approx 2^{nH(Y)}$, and $|T^n_{[XY]\delta}| \approx 2^{nH(XY)}$. By the consistency property of strong typicality, if $(\mathbf{x}, \mathbf{y}) \in T^n_{[XY]\delta}$, then $\mathbf{x} \in T^n_{[X]\delta}$ and $\mathbf{y} \in T^n_{[Y]\delta}$.

Then the following becomes evident. Since there are $\approx 2^{nH(X,Y)}$ typical $(\mathbf{x}, \mathbf{y})$ pairs and $\approx 2^{nH(X)}$ typical $\mathbf{x}$, for a typical $\mathbf{x}$, the number of $\mathbf{y}$ such that $(\mathbf{x}, \mathbf{y})$ is jointly typical is

$$\approx \frac{2^{nH(X,Y)}}{2^{nH(X)}} = 2^{nH(Y|X)}$$

on the average. The conditional strong AEP further asserts that this not only is true on the average, but in fact is true for every typical $\mathbf{x}$ as long as there exists one $\mathbf{y}$ such that $(\mathbf{x}, \mathbf{y})$ is jointly typical. Let $S^n_{[X]\delta}$ be the set of all such typical $\mathbf{x}$ sequences. The set $S^n_{[Y]\delta}$ is defined likewise.

We have established a rich set of structural properties for strong typicality with respect to a bivariate distribution p_{XY}, which is summarized in the two-dimensional *strong joint typicality array* in Figure 3. In this array, the rows and the columns are the typical sequences $\mathbf{x} \in S^n_{[X]\delta}$ and $\mathbf{y} \in S^n_{[Y]\delta}$, respectively. The total number of rows and columns are $\approx 2^{nH(X)}$ and $\approx 2^{nH(Y)}$, respectively. An entry indexed by $(\mathbf{x}, \mathbf{y})$ receives a dot if $(\mathbf{x}, \mathbf{y})$ is strongly jointly typical. The total number of dots is $\approx 2^{nH(X,Y)}$. The number of dots in each row is $\approx 2^{nH(Y|X)}$, while the number of dots in each column is $\approx 2^{nH(X|Y)}$.

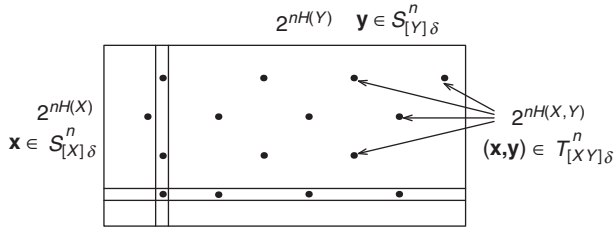


Fig. 3. A two-dimensional strong joint typicality array.

From the strong typicality array, we see that the number of dots in the array is at most equal to the number of entries in the array, i.e.,

$$2^{nH(X,Y)} \le 2^{nH(X)} 2^{nH(Y)}.$$

Upon taking the logarithm in the base 2 and dividing by n, we obtain

$$H(X, Y) \le H(X) + H(Y),$$

or

$$I(X; Y) \ge 0.$$

Thus the nonnegativity of $I(X; Y)$ is about the potentially unfilled entries in the two-dimensional strong typicality array.

We say that the strong joint typicality array in Figure 3 exhibits an *asymptotic quasi-uniform* structure. By a two-dimensional asymptotic quasi-uniform structure, we mean that in the array all the columns have approximately the same number of dots, and all the rows have approximately the same number of dots.

The strong joint typicality array for a multivariate distribution continues to exhibit an asymptotic quasi-uniform structure. Figure 4 shows a three-dimensional strong joint typicality array with respect to a distribution p_{XYZ}. As before, an entry $(\mathbf{x}, \mathbf{y}, \mathbf{z})$ receives a dot if $(\mathbf{x}, \mathbf{y}, \mathbf{z})$ is strongly jointly typical. This is not shown in the figure otherwise it will be very confusing. The total number of dots in the whole array is $\approx 2^{nH(X,Y,Z)}$. These dots are distributed in the array such that all the planes parallel to each other have approximately the same number of dots, and all the cylinders parallel to each other have approximately the same number of dots.

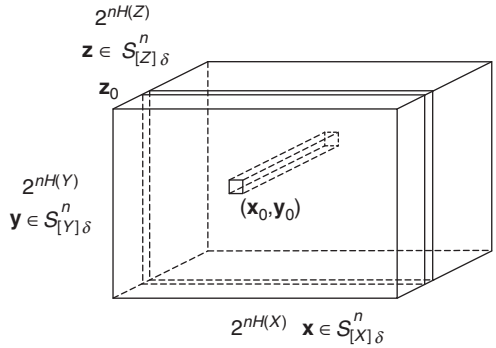


Fig. 4. A three-dimensional strong joint typicality array.

[5]The discussion here is based on strong typicality which applies only to random variables with finite alphabets. Recently, Ho and Yeung [67] introduced the notion of *unified typicality*, with which the same discussion can be applied to random variables with countable alphabets.

More specifically, the total number of dots on the plane for any fixed $\mathbf{z}_0 \in S^n_{[Z]\delta}$ (as shown) is $\approx 2^{nH(X,Y|Z)}$, and the total number of dots in the cylinder for any fixed $(\mathbf{x}_0, \mathbf{y}_0)$ pair in $S^n_{[XY]\delta}$ (as shown) is $\approx 2^{nH(Z|X,Y)}$, so on and so forth. By investigating this array, it is not difficult to show that

$$I(X;Y|Z) \geq 0,$$

which is the most general form of a basic inequality.

The discussion above gives a combinatorial interpretation of the basic inequalities. It is natural to ask whether all constraints on the entropy function, including non-Shannon-type inequalities, can be obtained by using this approach. Ideas along this line were further developed by Chan [35], where a *quasi-uniform array* was formally defined (to be elaborated in Section 3.2) and it was showed that all constraints on the entropy function can indeed be obtained through such arrays, and vice versa. This establishes a one-to-one correspondence between entropy and the combinatorial structure of a quasi-uniform array.

3.2 Group Theory

Let G be a finite group with operation "$\circ$", and $G_1, G_2, \ldots, G_n$ be subgroups of G. Then for any $\alpha \in \overline{\mathbf{N}}$, $G_\alpha = \cap_{i\in\alpha} G_i$ is also a subgroup. For a group element a and a subgroup S, let aS denotes the left coset $a \circ S = \{a \circ s : s \in S\}$. In this section, we explain a one-to-one correspondence between entropy and finite groups established by Chan and Yeung [36]. The following lemma is instrumental.

Lemma 1 *Let G_i be subgroups of a group G and a_i be elements of G, $i \in \alpha$. Then*

$$\Big|\bigcap_{i\in\alpha} a_i G_i\Big| = \begin{cases} |G_\alpha| & \text{if } \cap_{i\in\alpha} a_i G_i \neq \emptyset \\ 0 & \text{otherwise} \end{cases}.$$

The meaning of this lemma can be explained by a simple example. The relation between a finite group G and subgroups G_1 and G_2 is illustrated by the *membership table* in Figure 5. In this table, an element of G is represented by a dot. The first column represents the subgroup G_1, with the dots in the first column being the elements in G_1. The other columns represent the left cosets of G_1. By Lagrange's theorem, all cosets of G_1 have the same order, and so all the columns have the same number of dots. Similarly, the first row represents the subgroup G_2 and the other rows represent the left cosets of G_2. Again, all the rows have the same number of dots.

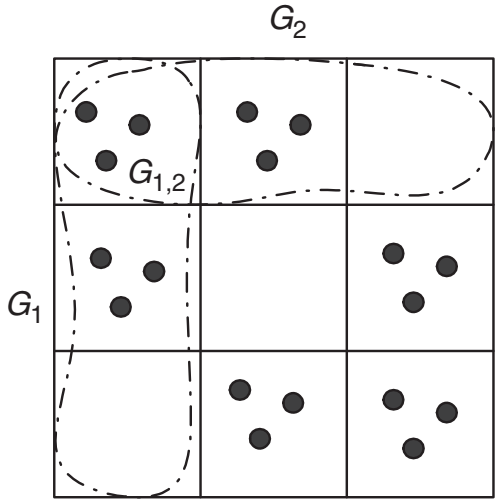


Fig. 5. The membership table for a finite group G and subgroups G_1 and G_2.

The upper left entry in the table represents the subgroup $G_1 \cap G_2$. There are $|G_1 \cap G_2|$ dots in this entry, with one of them representing the identity element. Any other entry represents the intersection between a left coset of G_1 and a left coset of G_2, and by Lemma 1, the number of dots in each of these entries is either equal to $|G_1 \cap G_2|$ or zero.

We have already seen a similar structure in Figure 3 for the two-dimensional strong joint typicality array. In that array, when n is large, all the columns have approximately the same number of dots and all the rows have approximately the same number of dots. In the membership table in Figure 5, all the column have exactly the same numbers of dots and all the rows have exactly the same number of dots. For this reason, we say that the table exhibits a *quasi-uniform* structure. In a membership table, each entry can contain a constant number of dots, while in a strong typicality array, each entry contains only one dot.

Theorem 3 *Let $G_i, i \in [n]$ be subgroups of a group G. Then $\mathbf{h} \in \mathcal{H}_n$ defined by*

$$h_\alpha = \log \frac{|G|}{|G_\alpha|}$$

for all $\alpha \in \overline{\mathbf{N}}$ is entropic, i.e., $\mathbf{h} \in \Gamma^*_n$.

Proof It suffices to show that there exists a collection of random variables $X_1, X_2, \ldots, X_n$ such that

$$H(X)_\alpha = \log \frac{|G|}{|G_\alpha|} \tag{1}$$

for all $\alpha \in \overline{\mathbf{N}}$. We first introduce a uniform random variable Λ defined on the sample space G with probability mass function

$$\Pr\{\Lambda = a\} = \frac{1}{|G|}$$

for all $a \in G$. For any $i \in [n]$, let random variable X_i be a function of Λ such that $X_i = aG_i$ if $\Lambda = a$.

Consider any $\alpha \in \overline{\mathbf{N}}$. Since $X_i = a_i G_i$ for all $i \in \alpha$ if and only if Λ is equal to some $b \in \cap_{i\in\alpha} a_i G_i$,

$$\Pr\{X_i = a_i G_i : i \in \alpha\} = \frac{|\cap_{i\in\alpha} a_i G_i|}{|G|} = \begin{cases} \frac{|G_\alpha|}{|G|} & \text{if } \cap_{i\in\alpha} a_i G_i \neq \emptyset \\ 0 & \text{otherwise} \end{cases}$$

by Lemma 1. In other words, $(X_i, i \in \alpha)$ is distributed uniformly on its support whose cardinality is $\frac{|G|}{|G_\alpha|}$. Then (1) follows and the theorem is proved.

This theorem shows that an entropy function for n random variables $X_1, X_2, \ldots, X_n$ can be constructed from any finite group G and subgroups $G_1, G_2, \ldots, G_n$, with

$$H(X_\alpha) = \log \frac{|G|}{|G_\alpha|}, \quad \alpha \in \overline{\mathbf{N}},$$

which depends only on the orders of G and $G_1, G_2, \ldots, G_n$. Now consider the entropy inequality

$$H(X_1) + H(X_2) \geq H(X_1, X_2)$$

that holds for all random variables X_1 and X_2, in particular for X_1 and X_2 constructed from any finite group G and subgroups G_1 and G_2 by means of Theorem 3. Substituting this entropy function into the inequality, we obtain

$$\log\frac{|G|}{|G_1|} + \log\frac{|G|}{|G_2|} \geq \log\frac{|G|}{|G_1 \cap G_2|}, \tag{2}$$

or

$$|G||G_1 \cap G_2| \geq |G_1||G_2|.$$

This group inequality is well-known in group theory and can be proved by group theoretic means (see for example [38, Sec. 16.4]).

The non-Shannon-type inequality ZY98, expressed in joint entropies, has the form

$$\left.\begin{matrix} H(X_1) + H(X_1,X_2) + 2H(X_3) \\ +2H(X_4) + 4H(X_1,X_3,X_4) \\ +H(X_2,X_3,X_4) \end{matrix}\right\} \leq \left\{\begin{matrix} 3H(X_1,X_3) + 3H(X_1,X_4) \\ +3H(X_3,X_4) + H(X_2,X_3). \\ +H(X_2,X_4) \end{matrix}\right.$$

From this, we can obtain the group inequality

$$\left.\begin{matrix} |G_1 \cap G_3|^3\ |G_1 \cap G_4|^3 \\ \cdot|G_3 \cap G_4|^3\ |G_2 \cap G_3| \\ \cdot|G_2 \cap G_4| \end{matrix}\right\} \leq \left\{\begin{matrix} |G_1|\ |G_1 \cap G_2|\ |G_3|^2 \\ \cdot|G_4|^2\ |G_1 \cap G_3 \cap G_4|^4, \\ \cdot|G_2 \cap G_3 \cap G_4| \end{matrix}\right.$$

which can be called a "non-Shannon-type" group inequality. To our knowledge, there has not been a group theoretic proof of this inequality.

Hence, for any entropy inequality that holds for any n random variables, one can obtain a corresponding inequality that holds for any finite group and any n of its subgroups. It can be shown that for any group inequality of the form (2) that holds for any finite group and any n of its subgroups, the corresponding entropy inequality also holds for any n random variables. This establishes a one-to-one correspondence between entropy and finite groups.

3.3 Probability Theory

In probability theory, a central notion is *conditional independence* of random variables. The relation between conditional independence and constraints on the entropy function is the following: For $\alpha, \beta, \gamma \in \mathbf{N}$, X_α, and X_β are independent conditioning on X_γ if and only if $I(X_\alpha; X_\beta|X_\gamma) = 0$.

We write "$X_\alpha \perp X_\beta|X_\gamma$" for the conditional independency (CI) $I(X_\alpha; X_\beta|X_\gamma) = 0$. Since $I(X_\alpha; X_\beta|X_\gamma) = 0$ is equivalent to

$$H(X_{\alpha\cup\gamma}) + H(X_{\beta\cup\gamma}) - H(X_{\alpha\cup\beta\cup\gamma}) - H(X_\gamma) = 0,$$

"$X_\alpha \perp X_\beta|X_\gamma$" corresponds to the hyperplane

$$\{\mathbf{h} \in \mathcal{H}_n : h_{\alpha\cup\gamma} + h_{\beta\cup\gamma} - h_{\alpha\cup\beta\cup\gamma} - h_\gamma = 0\}.$$

For a CI K, we denote the hyperplane in $\mathcal{H}_n$ corresponding to K by $\mathcal{E}(K)$. For a collection $\Pi = \{K\}$ of CIs, with a slight abuse of notation, let $\mathcal{E}(\Pi) = \cap_{K\in\Pi}\mathcal{E}(K)$. Then a collection of random variables Θ satisfies Π if and only if $\mathbf{h}^\Theta \in \mathcal{E}(\Pi)$. This gives a geometrical interpretation for conditional independence.

The relation between conditional independence and constraints on the entropy function does not stop here. In probability problems, we are often given a set of CI's and we need to determine whether another given CI is implied. This problem, called the *implication problem*, is one of the most basic problems in probability theory. As an example, consider random variables X_1, X_2, and X_3 that satisfy "$X_1 \perp X_3|X_2$" and "$X_1 \perp X_2$". Then we have

$$\begin{aligned} 0 &\leq I(X_1; X_3) \\ &= I(X_1; X_2, X_3) - I(X_1; X_2|X_3) \\ &= I(X_1; X_2) + I(X_1; X_3|X_2) - I(X_1; X_2|X_3) \\ &= 0 + 0 - I(X_1; X_2|X_3) \\ &= -I(X_1; X_2|X_3) \\ &\leq 0, \end{aligned}$$

where we have invoked two basic inequalities. Therefore, we see from the above that $I(X_1; X_3) = 0$, and so we have shown that

$$\left.\begin{matrix} X_1 \perp X_3|X_2 \\ X_1 \perp X_2 \end{matrix}\right\} \Rightarrow X_1 \perp X_3.$$

This example shows that certain structure of conditional independence can be implied by constraints on the entropy functions. In fact, the complete structure of conditional independence is implied by constraints on the entropy functions, namely through the characterization of the region Γ_n^*. To explain this, we first need to explain the building blocks of conditional independence for n random variables $X_i, i \in [n]$. It can be shown that every Shannon information measure involving $X_i, i \in [n]$ can be expressed as the sum of Shannon information measures of the following two *elemental forms:*

i) $H(X_i|X_{[n]-\{i\}}), i \in [n]$;

ii) $I(X_i; X_j|X_K)$, where $i \neq j$ and $K \subset [n] - \{i, j\}$.

For example, it can easily be verified that

$$\begin{aligned} H(X_1, X_2) = {} & H(X_1|X_2, X_3) + I(X_1; X_2) + I(X_1; X_3|X_2) \\ & + H(X_2|X_1, X_3) + I(X_2; X_3|X_1), \end{aligned}$$

where the right hand side consists of elemental Shannon information measures for $n = 3$, Then the basic inequality $H(X_1, X_2) \geq 0$ can be obtained by summing (is implied by) the corresponding elemental inequalities

$$\begin{aligned} H(X_1|X_2, X_3) &\geq 0 \\ I(X_1; X_2) &\geq 0 \\ I(X_1; X_3|X_2) &\geq 0 \\ H(X_2|X_1, X_3) &\geq 0 \\ I(X_2; X_3|X_1) &\geq 0. \end{aligned}$$

This is the reason for the name "elemental inequalities," because for a fixed n, the basic inequalities are implied by this smaller set of inequalities.

For a fixed n, by setting the two forms of elemental Shannon information measures to 0, we obtain the corresponding forms of *elemental conditional independencies*. Note that the first elemental form, namely $H(X_i|X_{[n]-\{i\}})$, can be written as $I(X_i; X_i|X_{[n]-\{i\}})$, and so $H(X_i|X_{[n]-\{i\}}) = 0$ (a functional dependency) is regarded as a special case of conditional independency.

We now explain why it suffices to consider all elemental conditional independencies (ECIs) instead of all conditional independencies (CIs) that involve X_i, $i \in [n]$. As an example, fix $n = 3$ and consider

$$I(X_1, X_2; X_3) = I(X_2; X_3) + I(X_1; X_3|X_2).$$

Since both $I(X_2; X_3)$ and $I(X_1; X_3|X_2)$ are nonnegative, $I(X_1, X_2; X_3)$ vanishes if and only if both $I(X_2; X_3)$ and $I(X_1; X_3|X_2)$ vanish. Therefore, the CI "$(X_1, X_2) \perp X_3$" is equivalent to the ECIs "$X_2 \perp X_3$" and "$X_1 \perp X_3|X_2$". Therefore, ECIs are the building blocks of the structure of conditional independence of random variables.

The compatibility of ECIs has been studied systematically by Matúš and Studený [22] and Matúš [23, 30] (specifically for $n = 4$), in which the p-representability problem was formulated as follows. Let $\mathrm{ECI}(n)$ denote the collection of all ECIs for any collection Θ of n random variables. Let $\{A, A^c\}$ denote a partition of $\mathrm{ECI}(n)$ (either A or A^c may be empty). Then for any $A \subset \mathrm{ECI}(n)$, we ask whether there exists a particular Θ such that Θ satisfies all $K \in A$ but does not satisfy any $K \in A^c$. If so, we say that $\{A, A^c\}$ is p-representable, otherwise we say that $\{A, A^c\}$ is not p-representable.

The problem of characterizing Γ_n^* subsumes the p-representability problem; the latter completely captures the structure of conditional independence of random variables. Specifically, $\{A, A^c\}$ is p-representable if and only if

$$\exists \mathbf{h} \in \Gamma_n^* \,\mathrm{s.t.}\, \mathbf{h} \in \mathcal{E}(A) \setminus \mathcal{E}(A^c),$$

or equivalently,

$$\Gamma_n^* \cap \Big(\bigcap_{K \in A} \mathcal{E}(K)\Big) \setminus \Big(\bigcap_{K \in A^c} \mathcal{E}(K)\Big) \neq \emptyset.$$

Note that it takes more than a characterization of $\bar{\Gamma}_n^*$ to solve the p-representability problem.

The p-representability problem in turn subsumes the implication problem. Specifically, a collection of CIs $\Pi \subset \mathrm{ECI}(n)$ implies a CI $K \in \mathrm{ECI}(n)$ if and only if

$$\forall p\text{-representable partition } \{A, A^c\} \text{ of } \mathrm{ECI}(n),\ \Pi \subset A \Rightarrow K \subset A.$$

The implication problem and hence the p-representability problem are surprising difficult. It was not until the late 1990's that Matúš [30] settled the p-representability problem for $n = 4$ by first establishing a constrained non-Shannon-type inequality which is a variation of ZY97. The general problem is still open. The special case of the problem for any n when all the CIs are *full conditional independencies*[6] (FCIs) was solved by Yeung *et al*. [39]. In particular, a Markov random field can be specified as a collection of FCIs. The characterization of the structure of full conditional independence is purely graph theoretic and is implied by Shannon-type inequalities.

3.4. Kolmogorov Complexity

Kolmogorov complexity, also known as Kolmogorov-Chatin complexity, is a subfield of computer science. The Kolmogorov complexity of a sequence x, denoted by $K(x)$, is the length of the shortest description of the string with respective to a *universal description language*. Without getting into the details, such a universal description language can be based on a computer programming language. Likewise, the Kolmogorov complexity of a pair of sequences x and y is denoted by $K(x, y)$. We refer the reader to [63] for a comprehensive treatment of the subject.

Hammer *et al*. [33] have shown that all linear inequalities that are valid for Kolmogorov complexity are also valid for entropy, and vice versa. For example, the inequality

$$H(X_1) + H(X_2) \geq H(X_1, X_2)$$

for any X_1, X_2 corresponds to the inequality

$$K(x_1) + K(x_2) \geq K(x_1, x_2)$$

for any two sequences x_1 and x_2. This establishes a one-to-one correspondence between entropy and Kolmogorov complexity. Due to this one-to-one correspondence, "non-Shannon-type" inequalities for Kolmogorov complexity can naturally be obtained.

3.5. Network Coding

For a long time, information transmission in a point-to-point network had been by and large regarded as commodity flow in the network, where routing is the only operation performed by the intermediate nodes. In the 1970's, Celebiler and Stette [14] proposed the use of coding in a satellite communication system for the purpose of improving the downlink capacity when the ground stations are considered in pairs.[7] Instead of broadcasting the data streams of the two ground stations separately, the modulo 2 sum of the two data streams are broadcast. This work, inspired by Shannon's work on the two-way channel [5], first proposed the use of coding at an intermediate node of a network.

In the 1990's, Yeung [24] studied a distributed data storage problem and discovered that unlike point-to-point communication, in network communication, joint coding of independent information sources is sometimes necessary in order to achieve the network capacity.[8] This was indeed the case for the satellite communication system studied in [14] although it was not explicitly discussed therein. Subsequently, Yeung and Zhang [31] considered the more general satellite communication problem in which multiple ground stations multicast different information sources to

[6] A CI "$X_\alpha \perp X_\beta|X_\gamma$" is an FCI for a given n if $\{\alpha, \beta, \gamma\}$ is a partition of $[n]$ (α, β, and Υ not necessarily nonempty).

[7] The author would like to thank Prof. Don Towsley for pointing out this reference.

[8] Consider two independent information sources X and Y to be transmitted in a point-to-point communication system. If we compress X and Y jointly, we need to transmit approximately $H(X, Y)$ bits. If we compress X and Y separately, we need to transmit approximately $H(X) + H(Y)$ bits. But since X and Y are independent, we have $H(X, Y) = H(X) + H(Y)$. Roughly speaking, joint coding of independent information sources is not necessary in a point-to-point communication system.

different sets of ground stations. In Ahlswede *et al*. [32], the advantage of network coding over routing was explicitly demonstrated by an example now known as *the butterfly network*,[9] and the term "network coding", which refers to coding at the intermediate nodes of a network, was coined. In this work, they studied *single-source network coding* in which a single information source is multicast from a source node to a set of sink nodes in a general point-to-point network.

It was established in [32] that the network capacity for single-source network coding admits a simple graph theoretic characterization in the form of a max-flow min-cut theorem for information flow that generalizes the corresponding classical theorem for commodity flow [3, 4]. Subsequently, it was proved by Li *et al*. [42] and then by Koetter and Médard [41] that linear network coding suffices to achieve the network capacity.

However, for the more general problem with multiple information sources, characterization of the network capacity is much more difficult. In [31], inner and outer bounds on the network capacity in terms of the region of entropy functions, i.e., Γ^*, were obtained. This work was further developed *into multi-source network coding* by Song *et al*. [51], in which the multi-source multicast problem was considered on general acyclic networks. An exact characterization of the capacity for multi-source network coding (for acyclic networks) in terms of Γ^* was finally obtained by Yan *et al*. [59, 72]. However, this characterization is implicit in the sense that it is not computable, precisely because the determination of Γ^* remains open.

Dougherty *et al*. [54] discovered the first example of multi-source network coding whose capacity characterization requires the use of ZY98. Chan and Grant [61] obtained a duality between entropy functions and network coding which asserts that for every $\mathbf{h} \in \mathcal{H}_n$, there exists a multi-source network coding problem characterized by $\mathbf{h}$, such that the problem has a network solution if and only if $\mathbf{h} \in \bar{\Gamma}_n^*$.

The insufficiency of specific forms of linear coding for multi-source network coding were demonstrated and discussed by Riis [47], Rasala Lehman and Lehman [45], and Médard *et al*. [43]. The insufficiency of very general forms of linear coding has been proved by Dougherty *et al*. [48]. This is also implied by the result of Chan and Grant [61], because compared with the entropy function, the rank function of vector spaces satisfies additional constraints, in particular the Ingleton inequality [9].

The theory of linear network coding has been generalized to *network error correction* by Yeung and Cai [52, 53] and *secure network coding* by Cai and Yeung [68]. Along a related line, Beimel *et al*. [60] have applied ZY98 to obtain new performance bounds in secret sharing, which can be regarded as a special case of secure network coding. An interpretation of secret sharing problems in terms of Γ^* and Γ can be found in [57, Section IV].

In quantum information theory, *quantum network coding* has been studied by Hayashi *et al*. [56].

3.6. Matrix Theory

Let X be a continuous random variable with probability density function (pdf) $f(x)$. The differential entropy of X is defined by

$$h(X) = -\int f(x) \log f(x) dx.$$

Likewise, the joint differential entropy of a random vector $\mathbf{X}$ with joint pdf $f(\mathbf{x})$ is defined by

$$h(\mathbf{X}) = -\int f(\mathbf{x}) \log f(\mathbf{x}) d\mathbf{x}. \tag{3}$$

The integral in the above definitions are assumed to be taken over the support of the underlying pdf.

A linear differential entropy inequality

$$\sum_{\alpha \in \bar{\mathbf{N}}} c_\alpha h(X_\alpha) \geq 0$$

is said to be balanced if for all $i \in [n]$, we have $\sum_{\alpha \in \bar{\mathbf{N}}: i \in \alpha} c_\alpha = 0$. (The same can be defined for an entropy inequality.) Chan [40] showed that the above differential entropy inequality is valid if and only if it is balanced and its discrete analog is valid. For example,

$$h(X|Y) = h(X,Y) - h(Y) \geq 0$$

is not valid because it is not balanced. On the other hand,

$$I(X;Y) = h(X) + h(Y) - h(X,Y) \geq 0$$

is valid because it is balanced and its discrete analog

$$H(X) + H(Y) - H(X,Y) \geq 0$$

is valid. Thus if Γ_n^* can be determined, then in principle all valid differential entropy inequalities can be determined.

Any $n \times n$ symmetric positive definite matrix $K = [k_{ij}]$ defines a Gaussian vector $\mathbf{X} = [X_1\, X_2 \ldots X_n]$ with covariance matrix K. Substituting the corresponding Gaussian distribution into (3), we obtain

$$h(\mathbf{X}) = \frac{1}{2} \log[(2\pi e)^n |K|],$$

where $|K|$ denotes the determinant of K. For $\alpha \in \tilde{\mathbf{N}}$, let K_α be the submatrix of K at the intersection of the rows and the columns of K indexed by α, whose determinant $|K_\alpha|$ is called a *principal minor* of K. Note that K_α is the covariance matrix of the subvector $\mathbf{X}_\alpha = [X_i : i \in \alpha]$. Since $\mathbf{X}_\alpha$ is also Gaussian, it follows that

$$h(\mathbf{X}_\alpha) = \frac{1}{2} \log[(2\pi e)^{|\alpha|} |K_\alpha|]. \tag{4}$$

Now consider the independence bound for differential entropy,

$$h(X_1, X_2, \cdots, X_n) \leq \sum_i h(X_i),$$

which is tight if and only if $X_i, i \in [n]$ are mutually independent. Substituting (4) into the above, we have

$$\frac{1}{2} \log[(2\pi e)^n |K|] \leq \sum_i \frac{1}{2} \log[(2\pi e) K_i],$$

or

$$\frac{n}{2} \log(2\pi e) + \frac{1}{2} \log |K| \leq \frac{n}{2} \log(2\pi e) + \frac{1}{2} \log \prod_i K_i.$$

Note that those terms involving $(1/2)\log(2\pi e)$ are cancelled out, because the independence bound is a valid differential entropy

[9]The name was coined by Michelle Effros.

inequality and so it is balanced. After simplification, we obtain

$$|K| \le \prod_i K_i,$$

namely Hadamard's inequality, which is tight if and only if $X_i, i \in [n]$ are mutually independent, or $k_{ij} = 0$ for all $i \neq j$.

For every valid differential entropy inequality, a corresponding inequality involving the principal minors of a positive definite matrix can be obtained in this fashion. It turns out that all non-Shannon-type inequalities for discrete random variables discovered so far are balanced, and so they are also valid for differential entropy. For example, from ZY98 we can obtain

$$|K_1||K_{12}||K_3|^2|K_4|^2|K_{134}|^4|K_{234}| \le |K_{13}|^3|K_{14}|^3|K_{34}|^3|K_{23}||K_{24}|,$$

which can be called a "non-Shannon-type" inequality for 4×4 positive definite matrices. Recently, Chan *et al*. [70] showed that for 3×3 positive definite matrices, all inequalities involving the principal minors can be obtained through the Gaussian distribution as explained. In a related work, Hassibi and Shadbakht [62] studied the properties of normalized Gaussian (differential) entropy functions.

3.7. Quantum Mechanics

The von Neumann entropy [1] is a generalization of the classical entropy (Shannon entropy) to the field of quantum mechanics.[10] For any quantum state described by a Hermitian positive semi-definite matrix ρ, the von Neumann entropy of ρ is defined as

$$S(\rho) = -\mathrm{Tr}(\rho \log \rho).$$

Consider distinct quantum systems A and B. The joint system is described by a Hermitian positive semi-definite matrix ρ_{AB}. The individual systems are described by ρ_A and ρ_B which are obtained from ρ_{AB} by taking partial trace. Consider a fixed ρ_{AB}. We simply use $S(A)$ to denote the entropy of System A, i.e., $S(\rho_A)$. In the following, the same convention applies to other joint or individual systems. It is well known that

$$|S(A) - S(B)| \le S(AB) \le S(A) + S(B).$$

The second inequality above is called the *subadditivity* for the von Neumann entropy. The first inequality, called the triangular inequality (also known as the Araki-Lieb inequality [8]), is regarded as the quantum analog of the inequality

$$H(X) \le H(X, Y) \tag{5}$$

for the Shannon entropy. It is important to note that although the Shannon entropy of a joint system is always not less than the Shannon entropy of an individual system as shown in (5), this may not be true in quantum systems. It is possible that $S(AB) = 0$ but $S(A) > 0$ and $S(B) > 0$, for example, when AB is a pure entangled state [34]. From this fact, we can see that the quantum world can be quite different from the classical world.

The *strong subadditivity* of the von Neumann entropy proved by Lieb and Ruskai [10, 11] plays the same role as the basic inequalities for the classical entropy. For distinct quantum systems A, B, and C, strong subadditivity can be represented by the following two equivalent forms:

$$S(A) + S(B) \le S(AC) + S(BC)$$
$$S(ABC) + S(B) \le S(AB) + S(BC).$$

These inequalities can be used to show many other interesting inequalities involving conditional entropy and mutual information. Similar to classical information theory, quantum conditional entropy and quantum mutual information are defined as $S(A|B) = S(A, B) - S(B)$ and $S(A{:}B) = S(A) + S(B) - S(A, B)$, respectively. For distinct quantum systems A, B, C and D, we have [34]

i) *Conditioning reduces conditional entropy:*

$$S(A|B, C) \le S(A|B).$$

ii) *Discarding quantum systems never increases mutual information:*

$$S(A{:}B) \le S(A{:}B, C).$$

iii) *Subadditivity of conditional entropy [28]:*

$$S(A, B|C, D) \le S(A|C) + S(B|D)$$
$$S(A, B|C) \le S(A|C) + S(B|C)$$
$$S(A|B, C) \le S(A|B) + S(A|C).$$

Following the discovery of non-Shannon-type inequalities for the classical entropy, it became natural to ask whether there exist constraints on the von Neumann entropy beyond strong subadditivity. Pippenger [44] proved that for a three-party system, there exist no such constraint. Subsequently, Linden and Winter [49] discovered for a four-party system a constrained inequality for the von Neumann entropy which is independent of strong subadditivity. Recently, Cadney *et al*. [71] proved a family of countably infinitely many constrained inequalities that are independent of each other and strong subadditivity.

4. Concluding Remarks

We have presented a comprehensive discussion on the connections between entropy and a number of seemingly unrelated subjects in information sciences, mathematics, and physics. These connections are summarized in the diagram in Figure. 6. In this diagram,

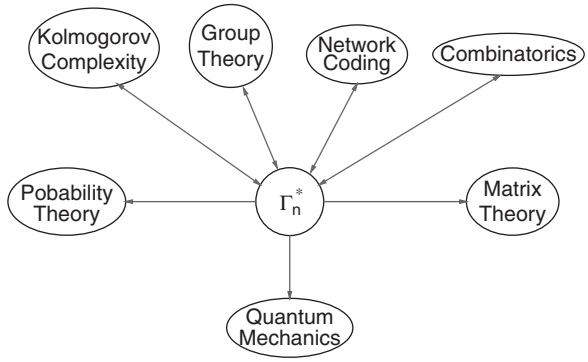


Fig. 6. Connections between entropy and various subjects in information sciences, mathematics, and physics.

[10]We refer the reader to the book by Nielsen and Chuang [34] for quantum information theory.

Γ_n^*, denoting entropy, is connected by double arrows with combinatorics, group theory, Kolmogorov complexity, and network coding, meaning that there is a one-to-one correspondence for each of these pairs. This suggest the existence of a common underlying structure for all these five subjects. The exact relations among these subjects are still highly confounding, although the quasi-uniform array appears to play a central role in these relations.

With the one-to-one correspondence between entropy and finite groups, we have seen how the rich set of tools in information theory can be employed to obtain results in group theory. The other research direction is less explored but is potentially very fertile. Similar can be said for the one-to-one correspondence between entropy and Kolmogorov complexity.

In the same diagram, Γ_n^* is connected by single arrows to probability theory, matrix theory, and quantum mechanics. The studies of entropy have made direct impacts on probability theory and matrix theory. For quantum mechanics, inspirations from classical information theory have borne fruits in quantum information theory.

This expository work does not aim to draw a conclusion on all the findings discussed here. Rather, it serves as a preamble to a series of investigations that will keep researchers from different fields busy for a very long time.

Acknowledgments

The author would like to thank Dr. Siu Wai Ho for contributing Section 3.7 on quantum mechanics, and Dr. Terence Chan, Dr. Fan Cheng, and Mr. Qi Chen for the useful discussions. This work was partially supported by a grant from the University Grants Committee of the Hong Kong Special Administrative Region, China (Project No. AoE/E-02/08).

References

[1] J. von Neumann, *Mathematische Grundlagen der Quantenmechanik*, Springer, Berlin, 1932.

[2] C. E. Shannon, "A Mathematical Theory of Communication," *Bell Sys. Tech. Journal*, 27: 379–423, 623–656, 1948.

[3] P. Elias, A. Feinstein, and C. E. Shannon, "A note on maximum flow through a network," *IRE Trans. Info. Theory*, IT-2: 117–119, 1956.

[4] L. R. Ford, Jr. and D. R. Fulkerson, "Maximal flow through a network," *Canadian J. of Math.*, vol. VIII, 399–404, 1956.

[5] C. E. Shannon, "Two-way communication channels," *Proc. 4th Berkeley Symp. Math. Statist. and Prob.*, vol. 1, 611–644, 1961.

[6] J. Wolfowitz, *Coding Theorems of Information Theory*, Springer, Berlin-Heidelberg, 2nd ed., 1964, 3rd ed., 1978.

[7] R. G. Gallager, *Information Theory and Reliable Communication*, Wiley, New York, 1968.

[8] H. Araki and E. H. Lieb. "Entropy inequalities". *Comm. Math. Phys.*, 18:160–170, 1970.

[9] A. W. Ingleton, "Representation of matroids," in *Combinatorial Mathematics and Its Applications*, D. J. A. Welsh, Ed., 149–167, Academic Press, London, 1971.

[10] E. H. Lieb and M. B. Ruskai, "A fundamental property of quantum-mechanical entropy," *Phys. Rev. Lett.*, 30(10): 434–436, 1973.

[11] E. H. Lieb and M. B. Ruskai, "Proof of the strong subadditivity of quantum mechanical entropy," *J. Math. Phys.*, 14: 1938–1941, 1973.

[12] T. S. Han, "Linear dependence structure of the entropy space," *Info. Contr.*, 29: 337–368, 1975.

[13] T. Berger, "Multiterminal source coding," in *The Information Theory Approach to Communications*, G. Longo, Ed., CISM Courses and Lectures #229, Springer-Verlag, New York, 1978.

[14] M. Celebiler and G. Stette, "On increasing the down-link capacity of a regenerative satellite repeater in point-to-point communications," *Proceedings of the IEEE*, vol. 66, no. 1, 98–100, 1978.

[15] S. Fujishige, "Polymatroidal dependence structure of a set of random variables," *Info. Contr.*, 39: 55–72, 1978.

[16] I. Csiszár and J. Körner, *Information Theory: Coding Theorems for Discrete Memoryless Systems*, Academic Press, New York, 1981.

[17] T. S. Han, "A uniqueness of Shannon's information distance and related non-negativity problems," *J. Comb., Info., and Syst. Sci.*, 6: 320–321, 1981.

[18] N. Pippenger, "What are the laws of information theory?" 1986 Special Problems on Communication and Computation Conference, Palo Alto, CA, Sept. 3–5, 1986.

[19] T. M. Cover and J. A. Thomas, *Elements of Information Theory*, Wiley, 1991, 2nd ed., Wiley-Interscience, 2006.

[20] J. Dj. Golić, "Noiseless coding for multiple channels," 1994 International Symposium on Information Theory and Its Applications, Sydney, Australia, 1994.

[21] F. Matúš, "Probabilistic conditional independence structures and matroid theory: Background," *Int. J. of General Syst.*, 22: 185–196, 1994.

[22] F. Matúš and M. Studený, "Conditional independences among four random variables I," *Combinatorics, Probability and Computing*, 4: 269–278, 1995.

[23] F. Matúš, "Conditional independences among four random variables II," *Combinatorics, Probability and Computing*, 4: 407–417, 1995.

[24] R. W. Yeung, "Multilevel diversity coding with distortion," *IEEE Trans. Info. Theory*, IT-41: 412–422, 1995.

[25] R. W. Yeung and Y.-O. Yan, Information-Theoretic Inequality Prover (ITIP), http://user-www.ie.cuhk.edu.hk/~ITIP/, 1996.

[26] R. W. Yeung, "A framework for linear information inequalities," *IEEE Trans. Info. Theory*, IT-43: 1924–1934, 1997.

[27] Z. Zhang and R. W. Yeung, "A non-Shannon-type conditional inequality of information quantities," *IEEE Trans. Info. Theory*, IT-43: 1982–1986, 1997.

[28] M. A. Nielsen. *Quantum Information Theory.* Ph.D. thesis, University of New Mexico, 1998.

[29] Z. Zhang and R. W. Yeung, "On characterization of entropy function via information inequalities," *IEEE Trans. Info. Theory*, IT-44: 1440–1452, 1998.

[30] F. Matúš, "Conditional independences among four random variables III: Final conclusion," *Combinatorics, Probability and Computing*, 8: 269–276, 1999.

[31] R. W. Yeung and Z. Zhang, "Distributed source coding for satellite communications," *IEEE Trans. Info. Theory*, IT-45: 1111–1120, 1999.

[32] R. Ahlswede, N. Cai, S.-Y. R. Li, and R. W. Yeung, "Network information flow," *IEEE Trans. Info. Theory,* IT-46: 1204–1216, 2000.

[33] D. Hammer, A. Romashchenko, A. Shen, and N. Vereshchagin, "Inequalities for Shannon Entropy and Kolmogorov Complexity," *J. Comp. and Syst. Sci.,* 60: 442–464, 2000.

[34] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quanum Information,* Cambridge University Press, 2000.

[35] T. H. Chan, "A combinatorial approach to information inequalities," *Comm. Info. and Syst.,* 1: 241–253, 2001.

[36] T. H. Chan and R. W. Yeung, "On a relation between information inequalities and group theory," *IEEE Trans. Info. Theory,* IT-48: 1992–1995, 2002.

[37] K. Makarychev, Y. Makarychev, A. Romashchenko, and N. Vereshchagin, "A new class of non-Shannon-type inequalities for entropies," *Comm. Info. and Syst.,* 2: 147–166, 2002.

[38] R. W. Yeung, *A First Course in Information Theory,* Kluwer Academic/Plenum Publishers, New York, 2002.

[39] R. W. Yeung, T. T. Lee and Z. Ye, "Information-theoretic characterization of conditional mutual independence and Markov random fields," *IEEE Trans. Info. Theory,* IT-48: 1996–2011, 2002.

[40] T. H. Chan, "Balanced information inequalities," *IEEE Trans. Info. Theory,* IT-49: 3261–3267, 2003.

[41] R. Koetter and M. Médard, "An algebraic approach to network coding," *IEEE/ACM Trans. Networking,* 11: 782–795, 2003.

[42] S.-Y. R. Li, R. W. Yeung and N. Cai, "Linear network coding," *IEEE Trans. Info. Theory,* IT-49: 371–381, 2003.

[43] M. Médard, M. Effros, T. Ho, and D. Karger, "On coding for nonmulticast networks," 41st Annual Allerton Conference on Communication, Control, and Computing, Monticello, IL, Oct. 2003.

[44] N. Pippenger, "The inequalities of quantum information theory," *IEEE Trans. Info. Theory,* IT-49: 773–789, 2003.

[45] A. Rasala Lehman and E. Lehman, "Complexity classification of network information flow problems," 41st Annual Allerton Conference on Communication, Control, and Computing, Monticello, IL, Oct. 2003.

[46] Z. Zhang, "On a new non-Shannon-type information inequality," *Comm. Info. and Syst.,* 3: 47–60, 2003.

[47] S. Riis, "Linear versus nonlinear boolean functions in network flows," 38th Annual Conference on Information Sciences and Systems (CISS), Princeton, NJ, Mar. 17–19, 2004.

[48] R. Dougherty, C. Freiling, and K. Zeger, "Insufficiency of linear coding in network information flow," *IEEE Trans. Info. Theory,* IT-51: 2745–2759, 2005.

[49] N. Linden and A. Winter, "A new inequality for the von Neumann entropy," *Comm. Math. Phys.,* 259: 129–138, 2005.

[50] R. Dougherty, C. Freiling, and K. Zeger, "Six new non-Shannon information inequalities," 2006 IEEE International Symposium on Information Theory, Seattle, WA, Jul. 9–14, 2006.

[51] L. Song, R. W. Yeung and N. Cai, "A separation theorem for single-source network coding," *IEEE Trans. Info. Theory,* IT-52: 1861–1871, 2006.

[52] R. W. Yeung and N. Cai, "Network error correction, Part I: Basic concepts and upper bounds," *Comm. Info. and Syst.,* 6: 19–36, 2006.

[53] N. Cai and R. W. Yeung, "Network error correction, Part II: Lower bounds," *Comm. Info. and Syst.,* 6: 37–54, 2006.

[54] R. Dougherty, C. Freiling, and K. Zeger, "Networks, matroids, and non-Shannon information inequalities," *IEEE Trans. Info. Theory,* IT-53: 1949–1969, 2007.

[55] B. Hassibi and S. Shadbakht, "Normalized entropy vectors, network information theory and convex optimization," 2007 IEEE Information Theory Workshop on Information Theory for Wireless Networks, Bergen, Norway, Jul 1–6, 2007.

[56] M. Hayashi, K. Iwama, H. Nishimura, R. Raymond, and S. Yamashita, "Quantum network coding," *Lecture Notes in Comp. Sci.,* LNCS 4393: 610–621, 2007.

[57] F. Matúš, "Two constructions on limits of entropy functions," *IEEE Trans. Info. Theory,* IT-53: 320–330, 2007.

[58] F. Matúš, "Infinitely many information inequalities," 2007 IEEE International Symposium on Information Theory, Nice, France, Jun. 24–29, 2007.

[59] X. Yan, R. W. Yeung, and Z. Zhang, "The capacity region for multi-source multi-sink network coding," 2007 IEEE International Symposium on Information Theory, Nice, France, Jun. 24–29, 2007.

[60] A. Beimel, N. Livne, and C. Padro, "Matroids can be far from ideal secret sharing," *Proc. of the Fifth Theory of Cryptography Conference,* New York, NY, Mar 19–21, 2008.

[61] T. Chan and A. Grant, "Dualities between entropy functions and network codes," *IEEE Trans. Info. Theory,* IT-54: 4470–4487, 2008.

[62] B. Hassibi and S. Shadbakht, "The entropy region for three Gaussian random variables," 2008 IEEE International Symposium on Information Theory, Toronto, Canada, Jul 6–11, 2008.

[63] M. Li and P. Vitányi, *An Introduction to Kolmogorov Complexity and Its Applications,* 3rd ed., Springer, New York, 2008.

[64] R. Pulikkoonattu, E. Perron, and S. Diggavi, Xitip, http://http://xitip.epfl.ch, 2008.

[65] R. W. Yeung, *Information Theory and Network Coding,* Spring 2008.

[66] S.-Y. Chung, Information-Theoretic Theorem Prover, http://itl.kaist.ac.kr/ittp.html, 2009.

[67] S. W. Ho and R. W. Yeung, "On information divergence measures and a unified typicality," *IEEE Trans. Info. Theory,* IT-56: 5893–5905, 2010.

[68] N. Cai and R. W. Yeung, "Secure network coding on a wiretap network," IEEE Trans. Info. Theory, IT-57: 424–435, 2011.

[69] T. Chan, "Recent progresses in characterizing information inequalities," Entropy, 13: 379–401, 2011.

[70] T. Chan, D. Guo, and R. Yeung, "Entropy functions and determinant inequalities," 2012 IEEE International Sym. on Info. Theory, Cambridge, MA, USA, Jul 1–6, 2012.

[71] J. Cadney, N. Linden and A. Winter, "Infinitely many constrained inequalities for the von Neumann entropy," *IEEE Trans. Info. Theory,* IT-58: 3657–3663, 2012.

[72] X. Yan, R. W. Yeung, and Z. Zhang, "An Implicit Characterization of the Achievable Rate Region for Acyclic Multi-Source Multi-sink Network Coding," to appear in *IEEE Trans. Info. Theory.*

(Courtesy of Communications in Information and Systems)

Recent Activities of the IEEE IT Student Committee

Galen Reeves and Samantha Summerson

The Student Committee had an active summer and hosted two events at ISIT in Boston. Our first event was a panel which focused on how a training in information theory is useful for careers in both industry and academia. We were fortunate to have Todd Coleman (UCSD), Tim Holliday (Goldman Sachs), Olgica Milenkovic (UIUC), Emre Telatar (EPFL), and Antonia Tulino (Bell Labs), share their experiences with us. The panel was moderated by Lalitha Sankar, and t-shirts were provided for all student attendees.

Our second event at ISIT was an exciting game show titled "Who wants to be an InfoThionaire." In this event, the host (Ninoslav Marina) presented the contestants (Joao Barros, Dan Constello, Rudi Urbanke, and Aylin Yener) with a series of increasingly difficult information theory related questions. Some example questions are[1]:

- ITW in 1997 that was held in Longyearbyen on Svalbard (78° N), was the northern-most IT event held so far. Out of around 50 participants, how many of them were Shannon Award winners:

  A) 1

  B) 3

  C) 5

  D) 7

- The number of citations of Sergio Verdu according to Google scholar is:

  A) 2^12.4

  B) 2^14.4

  C) 2^16.4

  D) 2^18.5

[1]The correct answers to the example questions are 1-C, 2-B, 3-B, 4-A

- "Basic Concepts in information Theory and Coding" is a famous book by 1985 Shannon Award Winner Solomon Golomb. However, the book has a subtitle. What is it?

  A) Roses without thorns

  B) The adventures of Secret Agent 00111

  C) Memories of Saint Helena

  D) Reveries of a Solitary Walker

- Complete the following list of names: Erdal Arikan, Roy Yates, Emre Telatar, David Tse,… With the most logical choice.

  A) Muriel Medard

  B) Abbas El Gamal

  C) Thomas Cover

  D) Emina Soljanin

The competition was very close with all of the contestants tied heading in to the final round. In the end, Aylin Yener was the winner by a single point. After the gameshow, we raffled off five

autographed copies of "Network Information Theory" by Abbas El Gamal and Young-Han Kim. The books were generously donated by Cambridge Press.

These events were organized by the student committee chairs Elza Erkip and Sriram Vishwanath, the co-chairs Mustafa El Halabi and Salim El Rouayheb, and the student members Galen Reeves and Samantha Summerson. Photos at both events were taken by Alex Dytso.

ESIT2012 – 12th IEEE European School of Information Theory

Deniz Gunduz
Gerhard Kramer

The 12th edition of the oldest information theory school, the European School of Information Theory (ESIT), was held in Antalya, Turkey between the 16th and the 20th of April, 2012. The school was organized by Deniz Gunduz (Imperial College, UK) and Gerhard Kramer (TUM, Germany) with local support from Alkan Soysal (Bahcesehir University, Turkey). The main goal of the school is to create an opportunity for doctoral students from Europe and surrounding countries to meet distinguished researchers in information theory, to listen to exceptional lectures on emerging topics and to present their research work while meeting and socializing with their fellow students.

The school followed the usual format of three-hour morning lectures followed by student presentations in the afternoons. The lecturers for this year were Frans Willems (Eindhoven University of Technology) who made an introduction to universal source coding, Gerhard Kramer (TUM) who explained the basics of network flow and network coding, Michael Gastpar (UC Berkeley and EPFL) who talked about how to exploit algebraic structure in network information theory, Sennur Ulukus (University of Maryland) who lectured on information theoretic security, and Alex Dimakis (University of Southern California) who talked about how to exploit network coding for distributed storage. We had an additional short lecture by Amos Lapidoth (ETHZ) who introduced two problems studied by Gelfand and Pinsker and presented some new results. We would like to thank all our lecturers for their valuable time and effort and for the high quality of the lectures.

Student participation is an essential part of the school. Apart from questions and discussions during the morning lectures, many students also presented their own research during the afternoon sessions. Despite the April sun outside, shining on the turquoise waters of the Mediterranean, all sessions were vigorously attended. In addition to the evening games of beach volleyball, football, table tennis and billiards, students had a chance to relax on the Wednesday afternoon during which an excursion was organized to the nearby historical and natural attractions. Owing to the all-inclusive nature of the hotel where the school took place, students had the chance to spend all their meals and free time together with each other and the lecturers.

In the history of information theory schools in Europe, spanning more than two decades, this was both the southernmost and the easternmost location that the school has ever reached. Indeed, it was the first time the school was held in Asia! This helped us to recruit students from Turkey, Iran and even Saudi Arabia. A total of 74 students from 25 institutions in 13 countries attended the school. Moreover, with the growing interest in information theory in and around Europe, the

school has now become an annual event. The high number of participation is even more remarkable considering that the last school was held only a year ago in Barcelona with a similar level of participation.

While the name of the school has varied over the years, it has always been called "the winter school" as it has been mostly held within the winter months. Owing to the shift of the school to the southern countries in recent years, the dates have also shifted first to March and finally to April, in order to enjoy the spring sun, without much complaint from the participants. With the change in the timing of the school and the North American School of Information Theory becoming a regular event, we have decided to name the event the European School of Information Theory (ESIT), which we hope will persist in the coming editions.

The 2012 School website can be accessed at http://www.itsoc.org/european-school-2012, where you can find the lecture abstracts and slides as well as the titles of the student presentations. With the help from Matthieu Bloch, we have started to use the Information Theory (IT) Society webpage to host the European School website. Unfortunately, since the resources from the previous European schools have been hosted on personal websites, they have been lost over time. Thanks to the hosting of the website in the IT Society servers, the lecture materials will be accessible over the years. We are grateful to the IT Society also for its financial support that made the school possible.

With the leadership of Petar Popovski, ESIT 2013 will be held in Ohrid, Republic of Macedonia, a beautiful little city on the banks of a tranquil lake bearing the same name, and famous for its numerous ancient churches, delicious food and hospitable inhabitants, a perfect setting for an information theory school. Follow the IT Society website and this newsletter for further news on ESIT 2013!

IT Society members win "best systems paper" award

Network coding paper, co-authored by IT society members Bella Bose and Thinh Nguyen, is the winner of Jack Neubauer Memorial Award

We are happy to announce that the 2012 Jack Neubauer Memorial Award has been awarded to "Wireless Broadcast Using Network Coding," co-authored by D. Nguyen, T. Tran, T. Nguyen, and B. Bose, published in the IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, VOL. 58, NO. 2, FEBRUARY 2009.

Jack Neubauer Memorial Award is presented annually to recognize the best systems paper published in the *IEEE Transactions on Vehicular Technology.*

The Historian's Column

Anthony Ephremides

In 1997, on the heels of the just completed ISIT in Ulm, Germany, a subset of the participants who proved to be the intrepid core of our Society, ventured towards the North Pole to hold a workshop on Coding and Communications in Svalbard. For those who do not include geography in their favorite subjects, Svalbard, known also as Spitzbergen, lies approximately at 80 degrees of north latitude. To reach its "capital", Longyearbyen, one flies out of Tromso, which is close to the northern tip of Norway. The flight lasts about two hours and heads due north. Svalbard is a piece of mostly ice-covered land that, like Antarctica, is open to all countries of the world for exploitation and development. However, its administration has been ceded by the United Nations to Norway. Upon arrival, at around 2 am, we were impressed by the gloomy picture of snow-covered hills under thick gray clouds. It was middle of July and there was ample daylight around the clock. We were further impressed by the level of development in Longyearbyen. The hotel was a first-class facility with nice meeting rooms, a beautiful dining room with wrap-around glass walls, excellent food (we even found out that there was a Michelin-starred restaurant in the upper reaches of a valley a few kilometers from the town), nice shops, a hospital, a branch of a Norwegian University where artic research was conducted, and, to top it all off, plenty of (rumored) polar bears. We did not see any although the risk of an encounter is taken very seriously by the authorities. If one wanted to succumb to the irresistible urge to venture outside the town for a lovely walk on the arctic tundra, renting a rifle was "de rigueur". Neil Sloane was sighted roaming the nearby hills with a rifle on his shoulder.

The diet at the hotel included whale meat (raw), which was not for the faint hearted. Reindeer, herring, salmon, and other nordic fare complemented the choices. Upon completion of the dinner, around 10 pm, the sun would shine brightly through the ceiling-high windows, creating the uncanny feeling that we just finished breakfast. One day after the sessions ended, an even smaller, and more intrepid subset of the participants headed for the remote slopes for some midnight skiing on cross-county skis. Do not imagine any lifts or other facilities. There was nothing. Just us, our skis, and, thank God, our guide (a most sophisticated outdoor scientists capable of handling all sorts of adversity). Needless to say that the experience was humbling. When we got back safely at around 2 am, with the sun casting long shadows, an eager Jim Massey (with a wiley smile on his face) inquired how the experience was. " It was tough", I volunteered. "I bet it was" was his response, suppressing a chuckle.

We even went for an arctic barbecue by kayaking our way in tandem sea-kayaks across a bay that often fills completely with ice without warning. My wife and I shared one kayak and after narrowly avoiding a capsize, we enjoyed hearty fare cooked on a bonfire in the middle of nowhere. As has been said, "if you are going to be anywhere in no where, you might as well be in the middle of it"! The feeling of bewilderment was intense as we stood on this barren segment of land where explorers first landed a mere century ago.

The last day we went on a hike that started out with 40° F overcast weather and ended with heavy snow showers. We felt like arctic explorers. This feeling was also shared by all when, during the traditional mid-week "excursion", we went on an ice-breaker cruise that brought us to the foot of a glacier; ice cubes from the glacier were used in our drinks to let us taste water that fell on the earth a couple of millennia ago. We visited a bleak iron-ore mine still operated by Russia. The miners, who had not received their wages for several months, seemed to be the unhappiest men I have ever seen.

All of this is not tabloid malarkey. It is true, documented history. One day, I am sure, we will get back there, at least to check the arctic terns as they aggressively protect their nests and force us to fend off their attacks with our umbrellas, like latter-day, sword-wielding musketeers or, worse, poor reincarnations of Don Quixote.

I know I have reported on this fabulous workshop before. Its uniqueness, however, deserved another pass and take. Topics visited twice are intended to assure that no reader escapes unaware of it. How many of you, dear readers, remember that I did? Let me hear from you.

GOLOMB'S PUZZLE COLUMN™

Prime Divisors of $n!$ and of $\binom{2n}{n}$

Solomon W. Golomb

1) What is the highest power of the prime p that divides $n!$? (This is usually expressed as a sum of several terms, each rounded down.)

2) In how many 0's does 1000! end?

3) Find a single expression involving n and p that answers Problem 1. (This is related to writing n in base p.)

4) From Problem 3, what is an expression for the highest power of the prime p that divides the binomial coefficient $\binom{2n}{n}$?

5) Show (by any means) that 2 divides $\binom{2n}{n}$ for all $n \geq 1$.

6) For any odd prime p, what is the condition on the base-p digits of n so that p does *not* divide $\binom{2n}{n}$?

7) It is known that for infinitely many values of n, $\binom{2n}{n}$ is divisible by neither 3 nor 5. Find the first 30 such values of n.

8) It is suspected that for infinitely many values of n, $\binom{2n}{n}$ is divisible by none of 3, 5, or 7. Find 10 such values of n.

9) Find a value of $n > 1$ for which $\binom{2n}{n}$ is divisible by none of 3, 5, 7, or 11.

GOLOMB'S PUZZLE COLUMN™

Some Infinite Sequences Solutions

Solomon W. Golomb

Preamble. In describing a *spanning ruler* R (whether finite or infinite) we call the increasing sequence of integers in R the marks (on the ruler); the difference between any two marks the *measured distances* (on R); and the differences between consecutive marks the *intervals* (of R). Note that every *measured distance* is a sum of consecutive intervals (of R).

Now for the solutions.

Problem 1. To show that $A = \{3^{n-1}\}$ and $B = \{2 \cdot 3^{n-1}\}$ for all $n \geq 1$ form an *infinite spanning biruler,* we note that in base 3 notation, every element of A has the form $100\cdots0$, where the number of 0's is n – 1; and every element of B has the form $200\cdots0$, where the number of 0's is $n-1$. By the uniqueness of the representation of integers in base 3, there can be no duplicates among numbers of the form $3^j - 3^i$, since if $3^j - 3^i = 3^l - 3^k$, then $3^j + 3^k = 3^i + 3^l$. Thus all measured distances in A, the terms of $\triangle A$, are distinct; and in base 3 notation, they all begin with "2". Since $B = 2A$, the measured distances in B, the elements of $\triangle B$, are all distinct from each other; and in base 3 notation, they all begin with "1". Thus also $\triangle A \cap \triangle B = \emptyset$, so that A and B form an infinite spanning biruler.

Problem 2. We defined our Fibonacci sequence $F = \{f_n\}$ by $f_1 = 1$, $f_2 = 2$, and $f_{n+1} = f_n + f_{n-1}$ for all $n > 1$; and then $A = \{a_n\} = \{f_{2n-1}\}$ and $B = \{b_n\} = \{f_{2n}\}$ for all $n \geq 1$. Note that neither A nor B contains any consecutive Fibonacci numbers.

The Lemma of Problem 3 asserts that no positive integer has more than one representation as a sum of non-consecutive Fibonacci numbers. The intervals, $\triangle A$ are the elements of B (since $f_{n+1} - f_{n-1} = f_n$), and the intervals in $\triangle B$ are the elements of A. Since every measured distance is a sum of consecutive intervals, the measured distances of A are sums of elements in B (hence of non-consecutive Fibonacci numbers) and the measured distances of B are sums of elements in A (hence of non-consecutive Fibonacci

numbers). Thus there are no duplicates within $\triangle A$ nor within $\triangle B$; and by the Lemma, $\triangle A \cap \triangle B = \emptyset$. Thus A and B form an infinite spanning biruler.

Problem 3. We will prove that no positive integer has more than one representation as a sum of non-consecutive terms of the Fibonacci sequence $F = \{f_n\} =. \{1, 2, 3, 5, 8, 13, \ldots\}$ Clearly the first few integers have only one such representation: $1 = 1, 2 = 2,. 3 = 3, 4 = 3 + 1, 5 = 5, 6 = 5 + 1, 7 = 5 + 2, 8 = 8, 9 = 8 + 1\ldots$, If there are exceptions, let N be the smallest positive integer with two such representations, e.g. $N = f_{a1} + f_{a2} + \ldots + f_{ar}$ and $N = f_{b1} + f_{b2} + \ldots + f_{bs}$, where $a_1 >> a_2 >> \ldots >> a_r$ and $b_1 >> b_2, >> \ldots >> b_s$ where ">>" means "greater by at least 2". We must have $f_{a_1} \neq f_{b_1}$ for if $f_{a_1} = f_{b_1}$ then $N' = N - f_{a_1}$ is a positive integer smaller than N with two such representations, contrary to the definition of N. Since $f_{a_1} \neq f_{b_1}$, assume $f_{a_1} > f_{b_1}$. But then $N = f_{b_1} + f_{b_2} + \ldots + f_{b_s}$ must at least equal $N \geq f_{a_1} \geq f_{b_1+1}$. However, a sum of non-consecutive Fibonacci terms with largest term f_{b_1} must be *less than* $f_{b_1+1} \leq f_{a_1} \leq N$, and we have the contradiction $N = f_{b_1} + \ldots + f_{b_s} < f_{b_1+1} \leq f_{a_1} \leq N$, and $N < N$ is a contradiction. To prove the assertion that $N = f_{b_1} + f_{b_2} + \cdots + f_{b_s} < f_{a_1}$, we consider the densest possible sequences of non-consecutive Fibonacci numbers, either $U = f_1 + f_3 + f_5 + \cdots + f_{2n-1}$ or $V = f_2 + f_4 + f_6 + \cdots + f_{2n}$. In each case, we show by mathematical induction that $U = f_1 + f_3 + \cdots + f_{2n-1} = f_{2n} - 1 < f_{2n}$, and that $V = f_2 +. \ f_4 + \cdots + f_{2n} = f_{2n+1} - 1 < f_{2n+1}$. To start, $f_1 = 1 = \ f_2 - 1 = 2 - 1$, and $f_2 = 2 = f_3 - 1 = 3 - 1$.Then, the inductive assumption in each case gives us a partial sum up to f_{n-1} equal to $f_n - 1$, and then adding the next term, f_{n+1}, gives $f_n + f_{n+1} - 1 = \ f_{n+2} - 1$, one less than the *next* Fibonacci number.

Problem 4. If $A = \{a_n\}$ and $B = \{b_n\}$, for all $n \geq 1$, form an infinite spanning biruler, where a_n and b_n have the same asymptotic rate of growth, we show that this rate must be at least $O(n^2)$ as follows. Among the first n terms of A, there are $\binom{n}{2}$ differences; among the first n terms of B, there are $\binom{n}{2}$ differences; and all $2\binom{n}{2} = n^2 - n$ of these numbers must be distinct (for a spanning biruler); so $a_n = O(n^2)$ and $b_n = O(n^2)$.

Problem 5. Computer searches indicate that if $A = \{a_n\}$ and $B = \{b_n\}$ form an infinite spanning biruler, both with the same asymptotic growth rate, and if A and B are as dense as possible, this growth rate may be a bit denser than $O(n^3)$, but definitely not as dense as $O(n^2)$.

One attempt to get A and B both as dense as $O(n^3)$ is to start with $A' = \{a_n\} = \{n^3\}$, and $B' = \{b_n\} = \{n^3 + n\}$. Neither $\triangle A'$ nor $\triangle B'$ are fully duplicate free (although the duplicates are infrequent), nor are $\triangle A'$ nor $\triangle B'$ completely disjoint. However, we may form A and B by alternatively adjoining the smallest *eligible* term left in A' to A, and then the smallest *eligible* term left in B' to B, where "eligible" means that it will not cause a repeated difference in A or B, respectively, nor cause an overlap between $\triangle A$ and $\triangle B$. Using this algorithm to compute the first 300 terms of both A and B, it appears that A and B, the "pruned" versions of A' and B', still have growth rate of $O(n^3)$.

Using a similar alternating algorithm, starting with $A' = \{n^4\}$ for all integers $n \geq 1$, and $B' = \{p^3\}$ for all primes $p \geq 3$, extremely few terms of A' or B' need to be discarded to get A and B as an infinite spanning biruler, where it should be provable that the resulting pruned sequences A and B form an infinite spanning biruler with growth rate of $O(n^4)$ for each.

I would like to see specific infinite sequences A and B, each of polynomial growth, that form an infinite spanning biruler (where this is accompanied by a proof).

Problem 6. We seek a non-zero polynomial in two variables, $p(x, y)$, such that $p(f_n, f_{n+1}) = 0$ for all $n \geq 1$, where $F = \{f_n\}$ is our Fibonacci sequence of Problem 2.

We use the well-known Fibonacci identity $f_n^2 - f_{n-1}f_{n+1} = (-1)^n$ for all $n > 1$. Since $f_{n-1} =, f_{n+1} - f_n$, this says $f_n^2 - (f_{n+1} - f_n)f_{n+1} = (-1)^n$, or $x^2 - (y - x)y = (-1)^n$ where $x = f_n$ and $y = f_{n+1}$. Then $(x^2 - xy - y^2)^2 = (-1)^{2n} = +1$, so that $p(x, y) = (x^2 - xy - y^2)^2 - 1 = x^4 + 2x^3y - x^2y^2 - 2xy^3 + y^4 - 1$ satisfies $p(f_n, f_{n+1}) = 0$ for all $n > 1$, where $p(x, y)$ has degree 4. Could anyone find a lower-degree polynomial with this property?

In the Blogosphere...

One of the issues I have been wondering about since I started as the editor of the newsletter is how we can bring in younger voices and capitalize on new forms of communication and social networking. In consultation with various IT society "heavy weights," I have decided to add a column in which I include pointers to some interesting blog items around. I am happy to report that this has coincided with the announcement about a new Princeton-Stanford Information Theory b-log which I am sure will be a good source in the future.

The items, for now, essentially are an indication of my personal taste and limited time but I hope folks will send in their own pointers and their suggested blog posts to add diversity. This issue I would like to bring to your attention the following two items I came across this summer:

An Ergodic Walk

a process whose average over time converges to the true average

Posted by Anand Sarwate under Uncategorized | Tags: mathematics |

William Thurston on proof and progress

William Thurston passed away a little over a month ago, and while I have never had the occasion to read any of his work, this article of his, entitled "On Proof and Progress in Mathematics" has been reposted, and I think it's worth a read for those who think about how mathematical knowledge progresses. For those who do theoretical engineering, I think Thurston offers an interesting outside perspective that is a refreshing antidote to the style of research that we do now. His first point is that we should ask the question:

How do mathematicians advance human understanding of mathematics?

I think we could also ask the question in our own fields, and we can do a similar breakdown to what he does in the article : how do we understand information theory, and how is that communicated to others? Lav Varshney had a nice paper (though I can't seem to find it) about the role of block diagrams as a mode of communicating our models and results to each other — this is a visual way of understanding. By contrast, I find that machine learning papers rarely have block diagrams or schematics to illustrate the geometric intuition behind a proof. Instead, the visual illustrations are plots of experimental results.

Thurston goes through a number of questions that interrogate the motives, methods, and outcomes of mathematical research, but I think it's relevant for everyone, even non-An Ergodic Walk a process whose average over time converges to the true average mathematical researchers. In the end, research is about communication, and understanding the what, how, and why of that is always a valuable exercise.

The Information Structuralist

Posted in Echoes of Cybernetics, Economics, Games and Decisions, Information Theory by Maxim Raginsky

Information theory in economics

Economic activity involves making decisions. In order to make decisions, agents need information. Thus, the problem of acquisition, transmission, and uses of information has been occupying the economists' attention for some time now (there is even a whole subfield of "information economics"). It is not surprising, therefore, that *information* theory, the brainchild of Claude Shannon, would eventually make its way into economics. In this post and the one to follow, I will briefly describe two specific strands of information-theoretic work in economics: the *rational inattention* framework of Christopher Sims and the *robustness* ideas of Thomas Sargent. (As an interesting aside: Sims and Sargent have shared the 2011 Nobel Memorial Prize in Economics, although not directly for their information-theoretic work, but rather for their work related to causality.)

In a nutshell, both Sims and Sargent aim to mitigate a significant shortcoming of the rational expectations hypothesis, namely that (to quote Cosma) "what game theorists [and economists] somewhat disturbingly call rationality is assumed throughout — … game players are assumed to be hedonistic yet infinitely calculating sociopaths endowed with supernatural computing abilities." To put this in more charitable terms, the basic tenet of rational expectations is that all economic agents are continuously optimizing, have access to all relevant information, can react to it instantly, and have unlimited computational capabilities. This is, to put it mildly, a huge oversimplification that does not mesh well with empirical observations. In reality, we see all sorts of "inertia" and delayed reaction effects (what Keynes has referred to as "stickiness" of prices, wages, etc.). Moreover, even disregarding stickiness, there is no reason to believe that the models used by the agents are at all accurate (indeed, if the 2008 financial crisis has taught us anything, quite the opposite is true). Thus, two adjustments are needed to the rational expectations framework: one to account for the fact that economic agents and institutions have only limited resources and capacity for acquiring and processing information, and another to formalize the pervasiveness of model uncertainty…

Max proceeds to summarize the work in simple and elegant terms. The first post, dated June 1, 2012, focused on rational inattention, which seeks to address the first issue. A follow-up post, on July 20, 2012, discussed robustness, which tackles the second issue.

Call for Nominations

IEEE Information Theory Society 2013 Claude E. Shannon Award

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

NOMINATION PROCEDURE: Nominations and letters of endorsement should be submitted by March 1, 2013 to the President of the IEEE Information Theory Society, who in 2013 will be Gerhard Kramer <gerhard.kramer@tum.de>. The nomination form is available at http://www.itsoc.org/honors/claude-e.-shannon-award

IEEE Information Theory Society 2013 Aaron D. Wyner Distinguished Service Award

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

NOMINATION PROCEDURE: Nominations and letters of endorsement should be submitted by March 1, 2013 to the President of the IEEE Information Theory Society, who in 2013 will be Gerhard Kramer <gerhard.kramer@tum.de>. The nomination form is available at http://www.itsoc.org/honors/wyner

IEEE Information Theory Society 2013 Paper Award

The Information Theory Society Paper Award is given annually for an outstanding publication in the fields of interest to the Society appearing anywhere during the preceding two calendar years (2011–2012). The purpose of this Award is to recognize exceptional publications in the field and to stimulate interest in and encourage contributions to fields of interest of the Society.

NOMINATION PROCEDURE: Nominations and letters of endorsement should be submitted by March 15, 2013 to the Awards Committee chair, who in 2013 will be Abbas El Gamal <abbas@ee.stanford.edu>. Please include a statement outlining the paper's contributions.

IEEE Joint ComSoc/ITSoc 2013 Paper Award

The Communications Society/Information Theory Society Joint Paper Award recognizes outstanding papers that lie at the intersection of communications and information theory. Any paper appearing in a ComSoc or ITSoc publication during the preceding three calendar years (2010–2012) is eligible for the 2013 award.

NOMINATION PROCEDURE: Nominations and letters of endorsement should be submitted by February 15, 2013 to the Awards Committee chair, who in 2013 will be Abbas El Gamal <abbas@ee.stanford.edu>. Please include a statement outlining the paper's contributions.

IEEE Fellow Program

Do you have a colleague who is a senior member of IEEE and is deserving of election to IEEE Fellow status? If so, please submit a nomination on his or her behalf to the IEEE Fellows Committee. The deadline for nominations is March 1. IEEE Fellow status is granted to a person with an extraordinary record of accomplishments. The honor is conferred by the IEEE Board of Directors, and the total number of Fellow recommendations in any one year is limited to 0.1% of the IEEE voting membership. For further details on the nomination process please consult: http://www.ieee.org/web/membership/fellows/index.html

IEEE Awards

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

IEEE INTERNATIONAL CONFERENCE ON COMMUNICATIONS

ICC 2013

Bridging the Broadband Divide
9-13 June • Budapest, Hungary

IEEE COMMUNICATIONS SOCIETY

WWW.IEEE-ICC.ORG/2013

The 2013 IEEE International Conference on Communications (ICC) will be held in the vibrant city of Budapest, Hungary from 9 – 13 June 2013. This flagship conference of IEEE Communications Society aims at addressing an essential theme on "Bridging the Broadband Divide." The conference will feature a comprehensive technical program including several Symposia and a number of Tutorials and Workshops. IEEE ICC 2013 will also include an attractive expo program including keynote speakers, various Business, Technology and Industry fora, and vendor exhibits. We invite you to submit your original technical papers, industry forum, workshop, and tutorial proposals to this event. Accepted and presented papers will be published in the IEEE ICC 2013 Conference Proceedings and in IEEE Xplore®. Full details of submission procedures are available at http://www.ieee-icc.org/2013.

To be published in the IEEE ICC 2013 Conference Proceedings and IEEE Xplore®, an author of an accepted paper is required to register for the conference at the full or limited (member or non-member) rate and the paper must be presented at the conference. Non-refundable registration fees must be paid prior to uploading the final IEEE formatted, publication-ready version of the paper. For authors with multiple accepted papers, one full or limited registration is valid for up to 3 papers. Accepted and presented papers will be published in the IEEE ICC 2013 Conference Proceedings and IEEE Xplore®.

PLANNED TECHNICAL SYMPOSIA

Selected Areas in Communications Symposium

E-Health Area
Pradeep Ray, University of New South Wales, Australia

Power Line Communications Area
Andrea Tonello, University of Udine, Italy
Stephan Weiss, University of Strathclyde, UK

Smart Grids Area
Bahram Honary, Lancaster University, UK

Tactical Communications & Operations Area
Gabe Jakobson, Altusys, USA

Satellite & Space Communication Area
Hiromitsu Wakana, NICT, Japan

Data Storage Area
Tiffany Jing Li, Lehigh University, USA

Access Systems and Networks Area
Michael Peeters, Alcatel-Lucent, Belgium

Green Communication Systems and Networks
Athanassios Manikas, Imperial College London, UK

Wireless Communications Symposium

Zhaocheng Wang, Tsinghua University, China
Metha B. Neelesh, Indian Institute of Science, India
Hanna Bogucka, Poznan University of Technology, Poland
Fredrik Tufvesson, Lund University, Sweden

Wireless Networking Symposium

Azzedine Boukerche, University of Ottawa, Canada
Pan Li, Mississippi State University, USA
Min Chen, Seoul National Unversity, Korea

Communication Theory Symposium

David Gesbert, EURECOM, France
Angel Lozano, Universitat Pompeu Fabra, Spain
Velio Tralli, University of Ferrara, Italy
Sennur Ulukus, University of Maryland, USA

Signal Processing for Communications Symposium

Hai Lin, Osaka Prefecture University, Japan
Octavia Dobre, Memorial University, Canada
Saiid Boussakta, Newcastle University, UK
Hongyang Chen, Fujitsu Laboratories, Japan

Optical Networks and Systems Symposium

Xavier Masip-Bruin, Technical University of Catalonia, Spain
Franco Callegati, University of Bologna, Italy
Tibor Cinkler, Budapest University of Technology and Economics, Hungary

Next-Generation Networking Symposium

Malathi "MV" Veeraraghavan, University of Virginia, USA
Joel Rodrigues, University of Beira Interior, Portugal
Wojciech Kabacinski, Poznan University of Technology, Poland

Communication QoS, Reliability & Modeling Symposium

Tetsuya Yokotani, Mitsubishi Electric Corporation, Japan
Harry Skianis, University of the Aegean, Greece
Janos Tapolcai, Budapest University of Technology and Economics, Hungary

Ad-hoc and Sensor Networking Symposium

Guoliang Xue, Arizona State University, USA
Abdallah Shami, University of Western Ontario, Canada
Xinbing Wang, Shanghai Jiaotong University, China

Communication Software and Services Symposium

Jiangtao (Gene) Wen, Tsinghua University, China
Lynda Mokdad, University Paris-Est, France

Communication and Information Systems Security Symposium

Tansu Alpcan, TU Berlin, Germany
Mark Felegyhazi, Budapest University of Technology and Economics, Hungary
Kejie Lu, University of Puerto Rico at Mayagüez, PR

Cognitive Radio and Networks Symposium

Honggang Zhang, Zhejiang University, China
David Grace, University of York, UK
Andrea Giorgetti, University of Bologna, Italy

COMMITTEE

General Chair:
Christopher Mattheisen
CEO, Magyar Telekom, Hungary

Executive Chair:
Lajos Hanzo
University of Southampton, UK

Technical Program Chair:
Andreas F. Molisch
University of Southern California, USA

Technical Program Vice-Chairs:
Andrea Conti
University of Ferrara, Italy
Iain Collings
CSIRO ICT Centre, Australia

Tutorials Co-Chairs:
Marco Chiani
University of Bologna, Italy
Wei Chen
Tsinghua University, China

Workshops Co-Chairs:
Thomas Michael Bohnert
Zurich University of Applied Sciences, Switzerland
Christoph Mecklenbrauker
Vienna University of Technology, Austria
Christina Fragouli
EPFL, Switzerland

Panel Session Co-Chairs:
David Soldani
Huawei, Germany
Peter Rost
NEC Labs Europe, Germany

Publications Co-Chairs:
Dong In Kim
Sungkyunkwan University, Korea
Peter Mueller
IBM Zurich Research Laboratory, Switzerland

Conference Operations Chair:
Rolland Vida
Budapest University of Technology and Economics, Hungary

Keynotes Chair:
Gerhard Bauch
Universität der Bundeswehr München, Germany

Patronage Chair:
Roland Jakab
Ericsson, Hungary

Publicity Chair:
John Vig
IEEE, USA

Student Travel Grant Chair:
Tommaso Melodia
State University of New York, Buffalo, USA

GIMS Advisor:
Klaus D. Kohrt
Germany

GITC Advisor:
John Thompson
University of Edinburgh, UK

ComSoc Project Manager:
June Leach-Barnaby
IEEE ComSoc, USA

Local Arrangements Chair:
Nandor Matrai
Asszisztencia, Hungary

Finance Chair:
Peter Nagy
HTE, Hungary

Treasurer:
Bruce Worthman
IEEE ComSoc, USA

IMPORTANT DATES

Paper Submission	Acceptance Notification	Camera-Ready	Tutorial Proposal	Workshop Proposal	Business Forum Proposal
16 September 2012	27 January 2013	24 February 2013	7 October 2012	25 June 2012	8 April 2012

Photo: Bertil Videt
http://commons.wikimedia.org/wiki/File:Bosphorus.jpg

July 7 – 12, 2013, Istanbul, Turkey

The 2013 IEEE International Symposium on Information Theory will be held in Istanbul, Turkey, from Sunday July 7th through Friday July 12th, 2013. Istanbul is the cultural, economic, and financial center of Turkey and a bridge between two continents as well as between cultures and traditions.

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:

- Coding theory and practice
- Compression
- Detection and estimation
- Information theory in networks
- Pattern recognition and learning
- Sequences and complexity
- Signal processing
- Communication theory
- Cryptography and data security
- Information theory and statistics
- Multi-terminal information theory
- Quantum information theory
- Shannon theory
- Source coding

Researchers working on novel applications of information theory are especially encouraged to submit original findings. Submitted papers should be of sufficient detail for review by experts in the field. Both submitted and final papers will be limited to 5 pages in standard IEEE conference format. The submission deadline is **January 27, 2013,** at midnight, GMT. Authors should refrain from submitting multiple papers on the same topic. Detailed information on paper submission, technical program, tutorials, travel, and social programs will be announced on the ISIT 2013 web site: **http://www.isit2013.org**

General Co-Chairs	Erdal Arıkan Elza Erkip
TPC Co-Chairs	Amos Lapidoth Igal Sason Jossy Sayir Emre Telatar
Finance	Melda Yüksel
Local Arrangements	Ali Emre Pusane
Publications	Stefan M. Moser
Recent Results	Aylin Yener
Tutorials	Şennur Ulukuş
Sponsorships	Elif Uysal Bıyıkoğlu
Student Travel Grants	Defne Aktaş

TURKCELL

IEEE

IEEE INFORMATION THEORY SOCIETY it

ISIT 2013 İSTANBUL

WWW.ISIT2013.ORG

TPC Members

Emmanuel Abbe
Venkat Anantharam
Francois Baccelli
Alexander Barg
Andrew Barron
Yair Beery
Randall Berry
Yitzhak Birk
Ian F. Blake
Helmut Bölcskei
Shraga Bross
Jehoshua Bruck
Joachim Buhmann
David Burshtein
Giuseppe Caire
Yuval Cassuto
Nicolo Cesa-Bianchi
Terence Chan
Asaf Cohen
Giacomo Como
Max Costa
Natasha Devroye
Alex Dimakis
Tolga Duman
Michelle Effros
Abbas El Gamal
Tony Ephremides
Uri Erez
Tuvi Etzion
Robert F. H. Fischer
David Forney
Christina Fragouli
Michael Gastpar
Alex Grant
A. Guillén i Fàbregas
Bruce Hajek
Stephen Hanly
Franz Hlawatsch
Syed Jafar
Nicholas Kalouptsidis
Ashish Khisti
Young-Han Kim
Joerg Kliewer
Kingo Kobayashi
Ioannis Kontoyannis
Frank Kschischang
Gitta Kutyniok
Ingmar Land
Gottfried Lechner
Yingbin Liang
Simon Litsyn
Angel Lozano
Nicolas Macris
Alfonso Martinez
Ueli Maurer
Neri Merhav
Olgica Milenkovic
Ralf Müller
Chandra Nair
Prakash Narayan
Bobak Nazer
Aria Nosratinia
Frédérique Oggier
Erik Ordentlich
Daniel Palomar
Enrico Paolini
Haim Permuter
Henry D. Pfister
Yury Polyanskiy
Vince Poor
Sandeep Pradhan
Bixio Rimoldi
Ronny Roth
Moshe Schwartz
Shlomo Shamai
Paul Siegel
Emina Soljanin
Anelia Somekh-Baruch
Yossi Steinberg
Wojciech Szpankowski
Leandros Tassiulas
Aslan Tchamkerten
Ari Trachtenberg
David Tse
Antonia Tulino
Ertem Tuncel
Daniela Tuninetti
Sennur Ulukus
A. van Wijngaarden
Alexander Vardy
Sergio Verdú
Emanuele Viterbo
Pascal Vontobel
Tadashi Wadayama
Aaron Wagner
Marcelo Weinberger
Tsachy Weissman
Michèle Wigger
Andreas Winter
Gregory Wornell
Roy Yates
Aylin Yener
Raymond Yeung
Ram Zamir

8TH ANNUAL ITA WORKSHOP

Sunday, Feb. 10 - Friday, Feb. 15, 2013
Catamaran Resort, San Diego

The Information Theory and Applications Workshop brings together researchers interested in theory and its many practical applications

TOPICS

Information Theory	Big Data
Signal Processing	Statistics
Communication	Cryptography
Digital Health	Social Networks
Networking	Machine Learning
Control	Computational Biology
Coding	Theoretical Computer Science

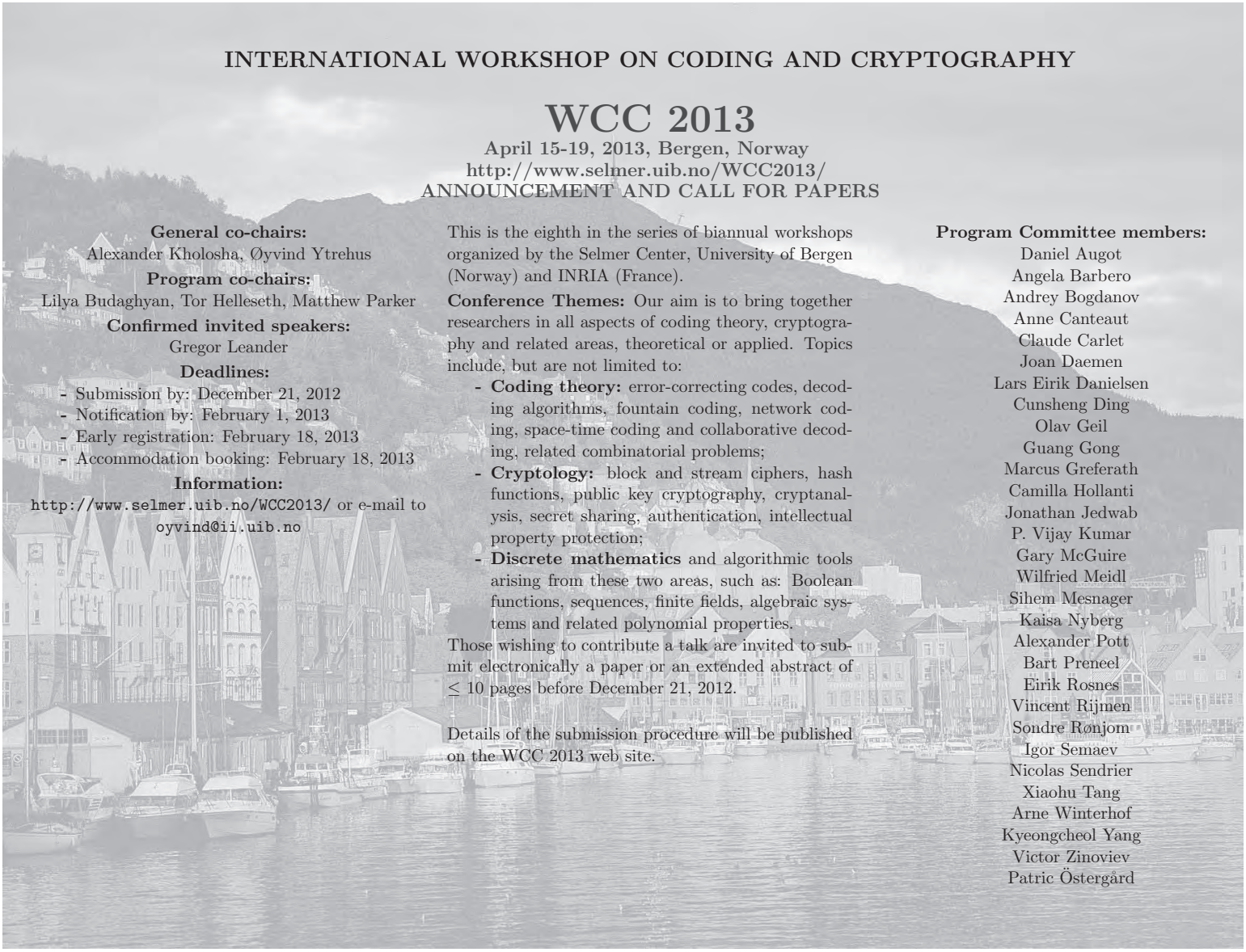
SPECIAL SESSIONS

Plenary presentations on "big data" by Tony Cai, Corinna Cortes, Carlos Guestrin, David Haussler, and Balaji Prabhakar

"Graduation day" presentations by outstanding students and postdocs

Everyone is welcome to attend. Presentations are by invitation only.

ita.ucsd.edu/workshop



INTERNATIONAL WORKSHOP ON CODING AND CRYPTOGRAPHY

WCC 2013

April 15-19, 2013, Bergen, Norway
http://www.selmer.uib.no/WCC2013/
ANNOUNCEMENT AND CALL FOR PAPERS

General co-chairs:
Alexander Kholosha, Øyvind Ytrehus

Program co-chairs:
Lilya Budaghyan, Tor Helleseth, Matthew Parker

Confirmed invited speakers:
Gregor Leander

Deadlines:

- Submission by: December 21, 2012
- Notification by: February 1, 2013
- Early registration: February 18, 2013
- Accommodation booking: February 18, 2013

Information:
`http://www.selmer.uib.no/WCC2013/` or e-mail to `oyvind@ii.uib.no`

This is the eighth in the series of biannual workshops organized by the Selmer Center, University of Bergen (Norway) and INRIA (France).

Conference Themes: Our aim is to bring together researchers in all aspects of coding theory, cryptography and related areas, theoretical or applied. Topics include, but are not limited to:

- **Coding theory:** error-correcting codes, decoding algorithms, fountain coding, network coding, space-time coding and collaborative decoding, related combinatorial problems;
- **Cryptology:** block and stream ciphers, hash functions, public key cryptography, cryptanalysis, secret sharing, authentication, intellectual property protection;
- **Discrete mathematics** and algorithmic tools arising from these two areas, such as: Boolean functions, sequences, finite fields, algebraic systems and related polynomial properties.

Those wishing to contribute a talk are invited to submit electronically a paper or an extended abstract of ≤ 10 pages before December 21, 2012.

Details of the submission procedure will be published on the WCC 2013 web site.

Program Committee members:
Daniel Augot
Angela Barbero
Andrey Bogdanov
Anne Canteaut
Claude Carlet
Joan Daemen
Lars Eirik Danielsen
Cunsheng Ding
Olav Geil
Guang Gong
Marcus Greferath
Camilla Hollanti
Jonathan Jedwab
P. Vijay Kumar
Gary McGuire
Wilfried Meidl
Sihem Mesnager
Kaisa Nyberg
Alexander Pott
Bart Preneel
Eirik Rosnes
Vincent Rijmen
Sondre Rønjom
Igor Semaev
Nicolas Sendrier
Xiaohu Tang
Arne Winterhof
Kyeongcheol Yang
Victor Zinoviev
Patric Östergård

Call for Papers

IWCIT
Iran Workshop on Communication and Information Theory

2013 Iran Workshop on Communication and Information Theory (IWCIT)

8-9 May 2013, Sharif University of Technology, Tehran, Iran

The first Iran Workshop on Communication and Information Theory (IWCIT) will take place at Sharif University of Technology, Tehran, Iran from Wednesday May 8th to Thursday May 9th, 2013. IWCIT will be held annually in Iran to bring together researchers in communication and information theory for exchanging their research results and latest developments.

Prospective authors are invited to submit high-quality, original, and unpublished contributions to IWCIT 2013. All submitted papers will be subject to peer review. This workshop is included in the IEEE Conference Publications Program (CPP). The scope of the workshop includes the following topics:

- Coding theory
- Cognitive radio systems
- Communication theory
- Complexity theory
- Compressed sensing
- Cooperative communications
- Data compression
- Information theoretic learning
- Information theoretic security
- 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
- Multi-terminal information theory
- Network coding
- Network resource sharing and scheduling
- Quantum information theory
- Shannon theory

Important dates:

- Paper Submission: 11 January 2013
- Notification of Acceptance: 15 March 2013
- Camera Ready Submission: 15 April 2013

General Chairs

- Aref, M.R. Sharif University of Technology, Iran
- Marvasti, F. Sharif University of Technology, Iran

Technical Program Chair

- Salehi, J.A. Sharif University of Technology, Iran

Executive Chairs

- Gohari, A.A. Sharif University of Technology, Iran
- Seyfe, B. Shahed University, Iran

Contact: info@iwcit.org, iwcit@sharif.ir
Address: Secretariat of IWCIT 2013, Room 501
Department of Electrical Engineering
Sharif University of Technology
Tehran, Iran
Tel: +98 21 66165908

Technical Program Committee

Aazhang, B.	Rice University, USA
Aghagolzadeh, A.	Babol Noshirvani University of Technology, Iran
Ahmadian, M.	K.N. Toosi University of Technology, Iran
Akhbari, B.	K.N. Toosi University of Technology, Iran
Alishahi , K.	Sharif University of Technology, Iran
Aref, M.R.	Sharif University of Technology, Iran
Avestimehr, S.	Cornell University, USA
Azmi, P.	Tarbiat Modares University, Iran
Banihashemi, A.H.	Carleton University, Canada
Behroozi , H.	Sharif University of Technology, Iran
Esfahani, S.N.	University of Tehran, Iran
Esmaeili, M.	Isfahan University of Technology, Iran
Gohari, A.A.	Sharif University of Technology, Iran
Golestani, S.J.	Sharif University of Technology, Iran
Haddadi, F .	Iran University of Science & Technology, Iran
Hodtani, G.A.	Ferdowsi University of Mashhad, Iran
Jafarkhani, H.	University of California, Irvine, USA
Khandani, A.K.	University of Waterloo, Canada
Lahouti, F.	University of Tehran, Iran
Marvasti, F.	Sharif University of Technology, Iran
Mirmohseni, M.	University of Tehran, Iran
Modarres, M.	Isfahan University of Technology, Iran
Nasiri-Kenari, M.	Sharif University of Technology, Iran
Olfat, A.	University of Tehran, Iran
Sabbaghian, M.	University of Tehran, Iran
Sadeghi, P.	The Australian National University, Australia
Sharafat, A.R.	Tarbiat Modares University, Iran
Shokrollahi, A.	EPFL, Switzerland
Tadaion, A.A.	Yazd University, Iran

www.IWCIT.org www.IWCIT.info

2013 European School of Information Theory (ESIT) Ohrid, Republic of Macedonia, April 22-26, 2013

The 2013 European School of Information Theory will be organized at the beautiful lakeside world-heritage town of Ohrid, Republic of Macedonia, from 22-26th of April 2013. The school is intended to provide an inspiring venue for doctoral and postdoctoral students from all over Europe (and beyond) to learn from leading experts in information theory through short courses/lectures, make friendships and connections with other school participants and present their own research. We especially encourage graduate students from the Balkan Countries to use this opportunity for learning and networking. The school is organized by institutions from Denmark, the Republic of Macedonia, and Serbia, and is supported by the IEEE Information Theory Society.

For this year's European School of Information Theory, we are pleased to announce our distinguished lecturer:

- James Massey

Confirmed course lecturers are:

- Suhas Diggavi (Approximation approach to network information theory)
- Stark Draper (Error exponents & non-asymptotics, feedback)
- Christina Fragouli (Network coding)
- Angel Lozano (Lost in the assumptions)
- Osvaldo Simeone (Source coding with side information)
- Bane Vasic (Error control coding, iterative decoding)

Mornings will be devoted to lectures and afternoons will be reserved for student poster presentations, discussions and problem solving sessions.

The school will be held at the Hotel Metropol in Ohrid http://www.metropol-ohrid.com.mk/. An excursion and sightseeing activities will be included. Transfer between the Skopje International Airport and Ohrid will be organized for school participants.

Organizing Committee

Petar Popovski
Aalborg University, Denmark

Zoran Utkovski
Uni Goce Delcev, R. of Macedonia

Liljana Gavrilovska, University Ss. Cyril and Methodius, R. of Macedonia

Venceslav Kafedziski, University Ss. Cyril and Methodius, R. of Macedonia

Dejan Vukobratovic
Uni Novi Sad, Serbia

Advisory Committee

Gerhard Kramer, TUM, Germany

Deniz Gunduz, Imperial College, UK

Dates

22-26th April 2013

Application/Abstract Deadline

See the web address below

Web

www.itsoc.org/european-school

Contact

Prof. Petar Popovski
Department of Electronic Systems
Aalborg University, Denmark
Tel. +45 99 40 98 97
Email: petarp@es.aau.dk

The 2013 School of Information Theory is organized by **Center for Science of Information (http://soihub.org),** a National Science Foundation science and technology center, and is sponsored by the IEEE Information Theory Society. Hosted at Purdue University from Tuesday, June 4 to Friday, June 7, 2013, the school provides a venue where doctoral and postdoctoral students can meet to learn from distinguished professors in information theory, and form friendships and collaborations. This year the school will introduce several interdisciplinary topics in the emerging field of science of information. Students will present their own research via a poster during the school. Although the focus is on information theory, interdisciplinary topics are welcome, e.g., topics related to mathematics, physics, biology, control, networking, etc.

Important Dates:
Applications: April 1, 2013
Acceptance Decisions: April 15, 2013
Registration: May 1, 2013

Program Overview:

Mornings: Lectures by invited speakers, TBA
Afternoons: Presentations and posters by students
Evening: Special events/activities

Organizing Committee:

- General Chair: Wojciech Szpankowski (Purdue University)
- Andrea Goldsmith (Stanford University)
- Sergio Verdu (Princeton University)
- Deepak Kumar (Bryn Mawr College)
- Olgica Milenkovic (University of Illinois)
- Todd P. Coleman (UC San Diego)
- Mark D. Ward (Purdue University)
- Brent Ladd (Purdue University)
- Barbara Gibson (Purdue University)
- Bob Brown (Purdue University)

Advisor:

- Gerhard Kramer (Technical University of Munich)

For updates, application, and further details: http://www.itsoc.org/north-american-school-2013/

Conference Calendar

DATE	CONFERENCE	LOCATION	WEB PAGE	DUE DATE
December 3–7, 2012	**2012 IEEE Global Communications Conference (GLOBECOM 2012)**	Anaheim, California, USA	http://www.ieee-globecom.org/	Passed
January 21–25, 2013	**16th Workshop on Quantum Information Processing (QIP 2013)**	Beijing, China	http://conference.iiis.tsinghua.edu.cn/QIP2013/index.html	Passed
February 10–15, 2013	**2013 Information Theory and Applications Workshop (ITA 2013)**	San Diego, CA, USA	http://ita.ucsd.edu/workshop.php	By invitation
March 20–22, 2013	**47th Annual Conference on Information Sciences and Systems (CISS 2013)**	Baltimore, MD, USA	http://ciss.jhu.edu/	January 4, 2013
April 14–19, 2013	**32nd IEEE International Conference on Computer Communications (INFOCOM 2013)**	Turin, Italy	http://infocom.di.unimi.it/	Passed
April 15–19. 2013	**International Workshop on Coding and Cryptography (WCC 2013)**	Bergen, Norway	http://www.selmer.uib.no/WCC2013/	December 21, 2012
April 22–26, 2013	**2013 IEEE European School on Information Theory (ESIT 2013)**	Ohrid, Republic of Macedonia	http://www.itsoc.org/european-school-2013	TBD
May 8–9, 2013	**2013 Iran Workshop on Communication and Information Theory (IWCIT)**	Tehran, Iran	www.IWCIT.org	January 11, 2013
May 13–17, 2013	**WiOpt 2013**	Tsukuba Science City, Japan	http://www.wi-opt.org/	December 20, 2012
June 2–5, 2013	**2013 77th Vehicular Technology Conference (VTC2013-Spring)A**	Dresden, Germany	http://www.ieeevtc.org/vtc2013spring/	Passed
June 4–7, 2013	**2013 IEEE North American School of Information Theory**	West Lafayette, Indiana, USA	http://www.itsoc.org/north-american-school-2013/	April 1, 2013
June 9–13, 2013	**IEEE International Conference on Communications (ICC 2013)**	Budapest, Hungary	http://www.ieee-icc.org/	Passed
June 23–26, 2013	**2013 IEEE Communication Theory Workshop**	Phuket, Thailand	http://www.ieee-ctw.org/	April 1, 2013
July 7–12, 2013	**2013 IEEE International Symposium on Information Theory (ISIT 2013)**	Istanbul, Turkey	http://www.isit2013.org/	January 27, 2013

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