IEEE Information Theory Society Newsletter

Vol. 48, No. 4, December 1998 Editor: Michelle Effros ISSN 1059-2362

Symposium Report ISIT '98

The 1998 IEEE International Symposium on Information Theory was held on the MIT campus in Cambridge, MA, USA, from Sunday afternoon, 16 August, through Friday evening, 21 August. The special theme of ISIT 98 was the 50th anniversary of the founding of the field of information theory in Claude Shannon's classic 1948 paper, "A mathematical theory of communication." Attendance was over 900, greatly exceeding the previous record of 701 (Ulm, ISIT'97). About 500 registrants were from the U.S., and 400 from 45 other countries (with ten or more from Japan (55), Germany (33), Sweden (32), Canada (31), Israel (29), France (25), Australia (19), Russia (18), Italy (16), Switzerland (15), the Netherlands (13), the United Kingdom (13), and Denmark (11)). All registrants received an extraordinary gift of a set of 11 CD-ROMs containing the entire contents of the *IEEE Transactions on Information Theory* from inception through 1997, courtesy of a special project of the IT Society and the efforts of Steve McLaughlin and Ramesh Rao. Other favors were a special edition of Shannon's paper edited by Emre Telatar and kindly furnished by Lucent Bell Laboratories, and a souvenir ISIT'98 mouse pad designed and produced by Amos Lapidoth and Frank Kschischang.

On Sunday afternoon, Peter Elias chaired a special History and Reminiscences session in Kresge Auditorium, featuring reminiscences by Peter Elias, David Huffman, Jim Massey and David Slepian, and a panel including Tom Cover, Imre Csiszar, Robert Fano, Sol Golomb, Brockway McMillan, Mark Pinsker, Andy Viterbi, Jack Wolf and Jacob Ziv. An animated reception followed on the lawn outside. The Technical Program included 475 technical papers presented in six parallel sessions extending through late Friday afternoon. Plenary lectures were given by a distinguished group of invited speakers:

Monday: Leonard Kleinrock (UCLA)
Tuesday: Thomas Kailath (Stanford)
Wednesday: Irwin Jacobs (Qualcomm)
Friday: Richard Karp (U. Washington)

Neil Sloane (AT&T Labs) gave the Shannon Lecture, "Codes and Lattices," on Thursday morning, where it was announced that AT&T Laboratories would shortly be renamed the "Shannon Laboratories."

On Monday evening, Sergio Verdú hosted a special award ceremony in Kresge Auditorium. In addition to awards for IT Society service and 9 new IEEE Fellows, special Golden Jubilee Paper Awards and Awards for Technological Innovations were announced (see the special issue of the IT Newsletter). IEEE President Joseph Bordogna congratulated Jack Wolf, for the IEEE Kobayashi Award, Oliver Collins, for the IEEE Resnik Award, and Dick Blahut, for the IEEE Bell Medal. There has surely never been such a gathering of distinguished information theorists on one stage.

A champagne reception followed in the Kresge foyer, with a special edition of the IT Newsletter guest edited by Tony Ephremides and Jim Massey hot off the presses. Recent Results sessions, organized by Amos Lapidoth, were held Tuesday evening. In addition several hundred people attended a special concert / lecture by Diana Dabby, "A dynamic music for our time."

On Wednesday afternoon, a gorgeous sparkling day, nearly 1000 registrants and guests boarded the ferry M.V. Provinceton in the Charlestown Navy Yard for a whale-watching cruise on the Stellwagen Bank, an hour outside Boston Harbor. Dozens of whales cooperated in putting on a memorable show.

Continued on page 3

From the Editor

Michelle Effros

As promised in the last issue, this issue spotlights ISIT'98 — the International Symposium on Information Theory for this year of Golden Jubilee celebrations. The issue begins with a look at the symposium itself — a report on symposium activities, a look at some images from ISIT'98, and a collection of signatures gathered from many of the award recipients after the ISIT'98 awards ceremony. The issue continues with important announcements from ISIT'98: the winner of the 1999 Shannon Award, the 1998 IT Society Paper Award, and the winning logo from the Information Theory Society logo contest were all announced at ISIT'98 and are all reported in this issue. Following the announcements come more detailed reports on some of the highlights from the symposium. Neil Sloane writes about the 1998 Shannon Lecture, Tom Kailath reports on his ISIT'98 plenary lecture (look for more plenary lecture reports in upcoming issues of the Newsletter), and some Shannon Award winners reflect on Shannon and the field of information theory. Later in the issue you will find reports on some of the other activities that took place around the world in celebration of Claude E. Shannon and the field that his work created and continues to inspire.

Michelle Effros

Also in this issue are Thomas Ericson's final column as 1998 president of the Information Theory Society, a fascinating look at a little-known chapter in the history of spread-spectrum technology, and, of course, another clever puzzle from the inexhaustible pen of Sol Golomb. Finally, we note the sad passing of Dwight O. North, inventor of the matched filter and recipient of an IT Society Golden Jubilee Award for Technological Innovation.

This issue marks the end of my three year term as editor of the *IEEE Information Theory Society Newsletter*. I have enjoyed my term as editor and owe many thanks to all of the people who have made the creation of this Newsletter possible and pleasurable. While I can't name all of the people who have been involved in this

Continued on page 22

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.

© 1998 IEEE. Information contained in this newsletter may be copied without permission provided that the copies are not made or distributed for direct commercial advantage, and the title of the publication and its date appear.

Table of Contents

Symposium Report . . .

continued from front cover

An elegant reception and banquet was held Thursday evening at the Boston Park Plaza Hotel, with entertainment by the Northeastern University Ballroom Dance Team and a Boston string quartet. Special recognition was given to Mrs. Betty Shannon, and also to four guests representing Gaylord, MI (Claude Shannon's birthplace). Neil Sloane received the Shannon Award, and the new IT Paper Prize and Shannon Award winners were announced (see elsewhere in this issue).

A final highlight for the several hundred registrants who stayed through Friday evening was a closing reception organized by Tony Ephremides and Ezio Biglieri, featuring excellent Italian antipasti and wines. Under a banner inviting the world to come to ISIT 2000 in Sorrento, a number of remarkable musical events took place:

- A series of five Italian opera arias by soprano Barbara Quintiliani;
- Five tenured tenors (E. Biglieri, A. Ephremides, T. Ericson, K. Vastola, and S. Verdú) joined in the famous aria "Torna a Sorriento" — an Italian romantic song about the locus of the next ISIT.;
- A reprise of "Ob-La-Di P-Log-P" (San Diego, ISIT'90), Bob McEliece's IT version of "Obladi, oblada;"
- As a grand finale, Ms. Quintiliani and Tony E sang the world premiere of the well-known baseball story poem "Casey at the Bat" that Tony set to music.

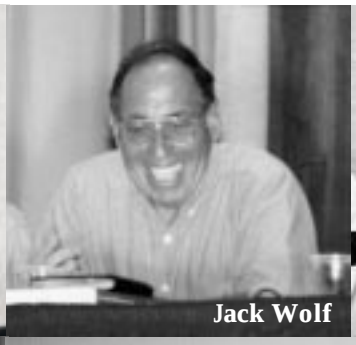
Those who were there say they will never forget it, and those who missed it are still kicking themselves.

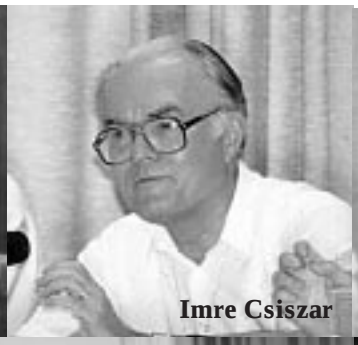
Generous financial support for this commemorative symposium was provided by the National Science Foundation, the National Aeronautics and Space Administration, and the Office of Naval Research, and also by AT&T, Lucent, Motorola and Qualcomm. Travel support was provided to 87 U.S. and non-U.S. registrants. In addition, 10 publishers exhibited (another all-time record): Cambridge Univ. Press, IEEE Press, Kluwer, McGraw-Hill, MIT Press, Morgan Kaufman, Plenum, Prentice-Hall, Springer and Wiley.

Signatures of Some Golden Jubilee Award Recipients

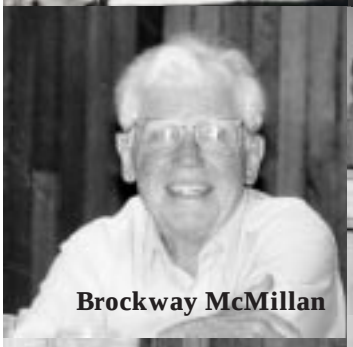
Images from ISIT '98


Tom Cover

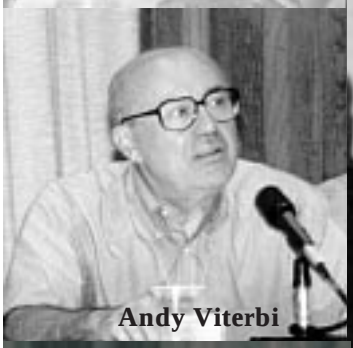

Jack Wolf


Imre Csiszar

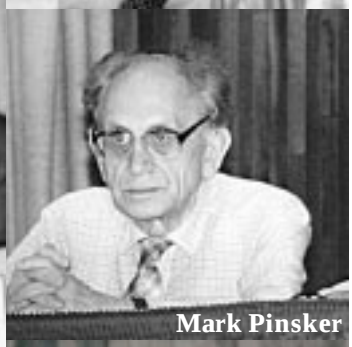

Jacob Ziv

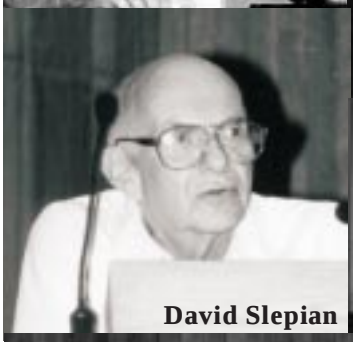

Brockway McMillan

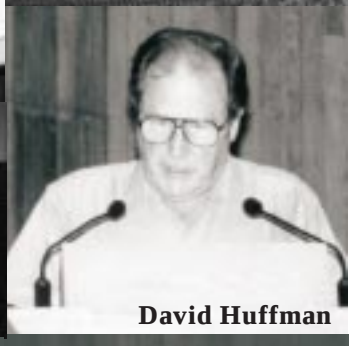

Sol Golomb

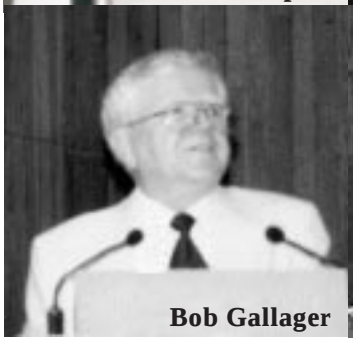

Andy Viterbi

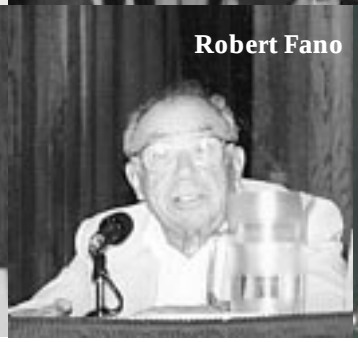

Betty Shannon

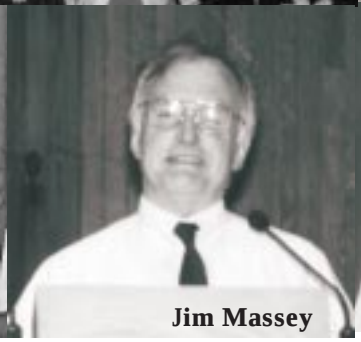

Mark Pinsker


David Slepian


David Huffman


Bob Gallager


Robert Fano


Jim Massey


Peter Elias

Images from ISIT '98

Tadao Kasami Wins the 1999 Claude E. Shannon Award

The Information Theory Society's highest honor, the Claude E. Shannon Award, is awarded annually to an individual who has achieved consistent and profound contributions to the field of information theory. The recipient is chosen by a selection committee consisting of Society officers and two former Shannon Award recipients.

Professor Tadao Kasami of Hiroshima City University has been selected as the 1999 Claude E. Shannon Award recipient. The award was announced at the 1998 International Symposium on Information Theory and will be presented to Professor Kasami at the 2000 International Symposium on Information Theory

An article on Professor Kasami in honor of his receipt of the award will appear in a future issue of the newsletter.

IT Society Paper Award

The 1998 Information Theory Society Paper Award is awarded to Venkat Anantharam and Sergio Verdu for their paper

"Bits through Queues, " *IEEE Transactions on Information Theory*, Vol. 42, No. 1, pp. 4-18, January 1996.

The award was announced at the 1998 International Symposium on Information Theory. More information about the authors and their award-winning paper is scheduled to appear in an upcoming issue of the Newsletter.

Awards

Jacob Ziv Receives the Eduard Rhein Basic Research Award

On April 1, 1998, the Eduard Rhein Foundation announced the 1998 winners of the Eduard Rhein Awards. Professor Jacob Ziv of the Technion, Haifa, Israel, will receive the 1998 Eduard Rhein Prize for his "groundbreaking publications on the theories of information and communication technologies," each of which has "spawned new avenues of research and novel applications" including work in "concatenated channel coding, the Ziv-Zakai bound of estimation theory, and complexity measures for strings of symbols." The Eduard Rhein Prize will be presented on October 10, 1998 in Munich, Germany.

Jacob Ziv

Information Theory Society Logo Contest —

The winner of the Information Theory Society Logo Contest is Dr. Giorgio Taricco.

There were nineteen entries. The winning logo was announced at the banquet of the International Symposium on Information Theory on August 20, 1998 by IT Society President, Thomas Ericson. As the designer of the winning entry, Giorgio will receive $500.

Giorgio studied Electrical Engineering at Politecnico di Torino, Italy, where he received his Dr. Engr. degree (summa cum laude) in 1985. From 1985 to 1987 he was in CSELT, in Torino, where he studied digital transmission systems with channel coding for error control. Since 1991 he has been on the faculty staff at Politecnico di Torino, Dipartimento di Elettronica, where he gives courses in analog and digital communications. His research interests cover the areas of error-control coding, digital communications and information theory with applications to mobile radio systems.

We would like to thank all of the designers who submitted entries to the contest.

1998 Shannon Lecture

The Sphere Packing Problem

N. J. A. Sloane
AT&T Shannon Lab
Florham Park, NJ 07932-0971, USA

Those who heard the talk will surely remember that I played Carl Orff's "Carmina Burana" as the audience was being seated. I felt that drastic measures were needed to wake people up at 08:30.

My original plan was to begin the talk with a second piece of music. I was going to start by digressing to talk about a proposal I made 2 or 3 years ago: the "Eternal Home Page". This is a possible Internet service that some major organization such as the IEEE, Harvard University, AT&T, or even the Vatican, might offer: a home page "in perpetuity';. Such a "perpetual page" or "eternity page" would be a home page that the organization would help the customer set up, with a guarantee that it would last for say 500 years, or until the organization no longer exists. The details are described on my web site[1]*. Almost everyone wants to be remembered by posterity, and I still think this is one of my best ideas, even though I haven't succeeded in getting any organization interested in the proposal. At this point I was planning to play a recording of Jessye Norman singing the moving and unforgettable aria "Remember Me" from Henry Purcell's "Dido and Aeneas". However, in the end I omitted this part of the talk for lack of time.*

What follows is a heavily abridged version of the talk. For much more information (and references) see the Introduction[2] *to the Third Edition of my book with John Conway "Sphere Packings, Lattices and Groups".*

The original title of the talk was "Codes and Lattices", but in the end - keeping in mind my slogan that "codes are to lattices as rock and roll is to classical music" - I decided to talk mostly about sphere packings and lattices.

Although the sphere packing problem has a long history in geometry, the real story begins (of course) with Shannon. The connection is via the sampling theorem. As Shannon observes in his classic 1948 paper, if f is a signal of bandwidth W hertz, with almost all its energy concentrated in an interval of T secs, then f is accurately represented by a vector of $2WT$ samples, which may be regarded as the coordinates of a single point in $\mathbb{R}^n$, $n = 2WT$. Nearly equal signals are represented by neighboring points, so to keep the signals distinct, Shannon represents them by n-dimensional 'billiard balls', and is therefore led to ask: what is the best way to pack 'billiard balls' in n dimensions?

Ambrose Rogers' book on "Packings and Coverings" came out in 1964, and my plan in this talk was to imagine that I was giving a report to Claude Shannon on some of the progress that has been made since 1964. This year is a natural break point in the subject, since John Leech discovered his great 24-dimensional lattice sphere packing around 1965, and this triggered many of the subsequent developments. The report proceeds upwards in dimension, beginning in 2 dimensions.

Dimension 2

The best packing in dimension 2 is the familiar 'hexagonal lattice' packing of circles, each touching six others. The centers are the points of the root lattice A_2. The *density* Δ of this packing is the fraction of the plane occupied by the spheres: $\pi/\sqrt{12} = 0.9069\ldots$.

In general we wish to find Δ_n, the highest possible density of a packing of equal nonoverlapping spheres in $\mathbb{R}^n$, or $\Delta_n^{(L)}$ the highest density of any packing in which the centers form a lattice. It is known (Fejes Tóth, 1940) that $\Delta_2 = \Delta_2^{(L)} = \pi/\sqrt{12}$.

We are also interested in packing points on a sphere, and especially in the 'kissing number problem': find τ_n (resp. $\tau_n^{(L)}$), the maximal number of spheres that can touch an equal sphere in $\mathbb{R}^n$ (resp. in any lattice in $\mathbb{R}^n$). It is trivial that $\tau_2 = \tau_2^{(L)} = 6$

Dimension 3

Just a week before this talk, Thomas Hales at the Univ. of Michigan made a dramatic announcement: he had finally settled the 387-year old Kepler conjecture[3] that no 3-dimensional packing has greater density than the face-centered cubic (or f.c.c) lattice A_3, or in other words $\Delta_3 = \Delta_3^{(L)} = \pi/\sqrt{18}$

In two dimensions the hexagonal lattice is (a) the densest lattice packing, (b) the least dense lattice covering, and (c) is geometrically similar to its dual lattice. There is a little known three-dimensional lattice that is similar to its dual, and, among all lattices with this property, is both the densest

[1] www.research.att.com/~njas/doc/eternal.html
[2] Available from my home page www.research.att.com/-njas/
[3] See N.J.A. Sloane, "Kepler Conjecture Confirmed", Nature, Oct. 1, 1998, p. 435.

packing and the least dense covering. This is the m.c.c. (or *mean-centered cuboidal*) lattice, which is in a sense is the geometric mean of the f.c.c. lattice and its dual the body-centered cubic (b.c.c.) lattice (Conway and the author, 1994).

Dimensions 4-8

Table 1 summarizes what is presently known about the sphere packing and kissing number problems in dimensions ≤ 24. Entries enclosed inside a solid line are known to be optimal, those inside a dashed line optimal among lattices.

The large box in the 'density' column refers to Blichfeldt's 1935 result that the root lattices $\mathbb{Z} \simeq A_1, A_2, A_3 \simeq D_3, D_4, D_5, E_6, E_7, E_8$ achieve $\Delta_n^{(L)}$ for $n \leq 8$. It is remarkable that more than 60 years later $\Delta_9^{(L)}$ is still unknown.

The large box in the right-hand column refers to Watson's 1963 result that the kissing numbers of the above lattices, together with that of the laminated lattice Λ_9, achieve $\tau_n^{(L)}$ for $n \leq 9$. Andrew Odlyzko and I, and independently Vladimir Levenshtein, determined τ_8 and τ_{24}. The packings achieving these two bounds axe unique.

Dimension 9. Laminated lattices

There is a simple construction, the 'laminating' or 'greedy' construction, that produces many of the densest lattices in dimensions up to 26. Let Λ_1 denote the even integers in $\mathbb{R}^1$, and define the n-dimensional laminated lattices Λ_n recursively by: consider all lattices of minimal norm 4 that contain some Λ_{n-1} as a sublattice, and select those of greatest density. It had been known since the 1940's that this produces the densest lattices known for $n \leq 10$. In 1982 Conway and I determined *all* inequivalent laminated lattices for $n \leq 25$, and

Dim.	Densest packing	Highest kissing number	
1	$\mathbb{Z} \simeq \Lambda_1$	2	
2	$A_2 \simeq \Lambda_2$	6	
3	$A_3 \simeq D_3 \simeq \Lambda_3$	12	
4	$D_4 \simeq \Lambda_4$	24	
5	$D_5 \simeq \Lambda_5$	40	
6	$E_6 \simeq \Lambda_6$	72	
7	$E_7 \simeq \Lambda_7$	126	
8	$E_8 \simeq \Lambda_8$	240	
9	Λ_9	272	(306 from P_{9a})
10	Λ_{10} (P_{10c})	336	(500 from P_{10b})
12	K_{12}	756	(840 from P_{12a})
16	$BW_{16} \simeq \Lambda_{16}$	4320	
24	Leech $\simeq \Lambda_{24}$	196560	

Table 1: Densest packings and highest kissing numbers known in low dimensions. (Parenthesized entries are nonlattice arrangements that are better than any known lattice.)

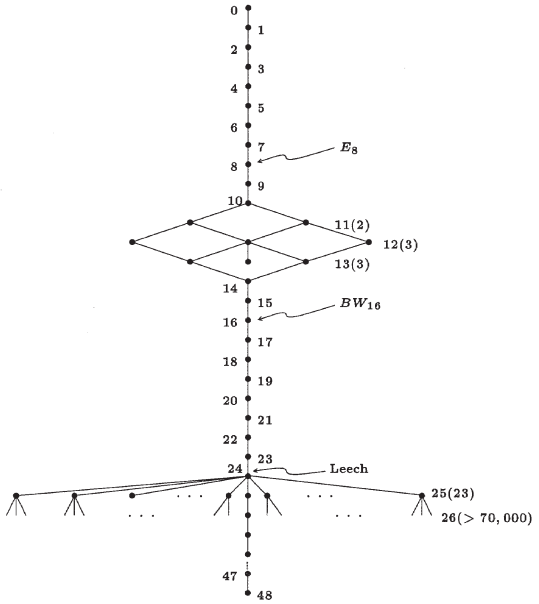


Figure 1: Inclusions among laminated lattices Λn.

found the density of Λ_n for $n \leq 48$ (Fig. 1). A key result needed for this was the determination of the covering radius of the Leech lattice and the enumeration of the deep holes in that lattice.

What are all the best sphere packings in low dimensions? In a 1995 paper Conway and I describe what may be all the best packings in dimensions $n \leq 10$, where 'best' means both having the highest density and not permitting any local improvement. In particular, we conjecture that $\Delta_n^{(L)} = \Delta_n$ for $n \leq 9$. For example, it appears that the best five-dimensional sphere packings are parameterized by the 4-colorings of $\mathbb{Z}$. We also find what we believe to be the exact numbers of 'uniform' packings among these, those in which the automorphism group acts transitively. These assertions depend on certain plausible but as yet unproved postulates.

A remarkable property of 9-dimensional packings. We also showed that the laminated lattice Λ_9 has the following astonishing property. Half the spheres can be moved bodily through arbitrarily large distances without overlapping the other half, only touching them at isolated instants, the density remaining the same at every instant. All these packings have the same density, which we conjecture is the value of $\Delta_9 = \Delta_9^{(L)}$. Another result in the same paper is that there are extraordinarily many 16-dimensional packings that are just as dense as the Barnes-Wall lattice $BW_{16} \simeq \Lambda_{16}$.

Dimension 10. Construction A.

In dimension 10 we encounter for the first time a nonlattice packing that is denser than all known lattices. This packing, and the nonlattice packing with the highest known kissing number in dimension 9, are easily obtained from 'Construc-

Continued on page 35

ISIT '98 Plenary Lecture Report

From Matched Filters to Martingales

Thomas Kailath

1. Introduction

The hopes of the organizers for this special session were that it would cover statistical detection and estimation theory, topics that were major areas of investigation in the first three decades of Information Theory. In recent years, most of the activity in these areas has been reported elsewhere.

The symposium talk covered a number of topics (some old, some new, some borrowed, none blue), going beyond the advertised title. Here we briefly present a few of them. The first is the rapidly growing area of techniques for blind channel equalization using second-order statistics, commonly thought only to apply to minimum phase channels. For potentially non-minimum-phase channels, the only option seemed to be to use higher-order statistics, but these need more data to estimate well and more complicated algorithms, both of which are unreasonable in rapidly changing environments, as encountered, for example, in mobile wireless systems. In Sec. 3, we note the origin of the matched filter and the early (1947) work of Kotel'nikov on optimal signal detection in additive white Gaussian noise. We remark how close, and yet how far, Kotel'nikov was to Shannon's channel capacity concept, even for this special, but important, channel. The final topic is an even briefer review of the search for insight into the structure of likelihood ratios for signal detection. A key concept in uncovering such structure is a generalization, using the modern (post 1967) theory of martingale processes, of the concept of innovations introduced by Bode and Shannon (1950) to provide a more insightful derivation of Wiener's celebrated results on the prediction and filtering of stationary stochastic processes.

2. Blind Channel Equalization

The basic equalization problem is indicated in Fig. 1.

If the channel $H(z)$ is known, or can be identified, we can choose the equalizer (in the absence of noise) as $G(z) = H^{-1}(z)$. Of course $G^{-1}(z)$ will be an IIR (infinite impulse response) filter, even when the channel is (modeled as) an FIR filter. Moreover when $G(z)$ is not minimum-phase, $H(z)$ will be noncausal, but this can be accommodated by introducing a sufficient delay in the equalizer. The problem is to identify $H(z)$. If we make the (common) assumption that the input sequence is an uncorrelated unit variance random process, then the power spectral density of the output of the channel will be $H(z)H^*(z^{-1}) + \sigma^2 I$, if we also have additive white noise of intensity σ^2. While σ^2 can be determined fairly easily, the problem is that we cannot recover $H(z)$ from the product $H(z)H^*(z^{-1})$, unless $H(z)$ is minimum-phase. However, on further reflection, all we have shown is that phase information cannot be recovered from *stationary* second-order statistics, such as the power spectral density function. As mentioned in the introduction, it turns out that phase information can (often) be recovered from *nonstationary* second-order statistics. And in particular from cyclostationary (or periodically correlated) second-order processes.

A New Solution : Use oversampling (when excess BW is available), as is done already for other reasons, e.g., `clock recovery,' leading to what are called fractionally spaced equalizers. We demonstrate now a deeper reason for using such equalizers.

To present the main ideas in the simplest context, consider oversampling the received signal by a factor of two. The transmitted signal is kept at the original rate and to accommodate the oversampling we can repeat the information, so that (see Fig. 2) the oversampled signal can be written as

$$s(z) = (1 + z)S(z^2) = (1 + z)(S_0 + S_2 z^2 + \ldots)$$

We now separate out the even and odd samples of the received signal,

$$y(z) = H(z)(1 + z)S(z^2) \triangleq h(z)S(z^2)$$
$$\triangleq (h_e(z^2) + zh_o(z^2))S(z^2)$$

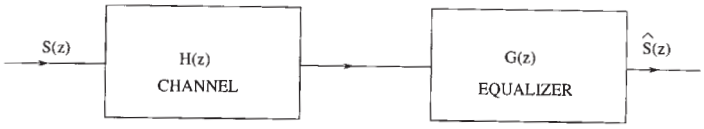


Figure 1

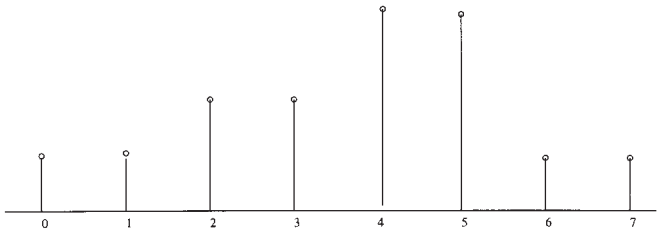


Figure 2

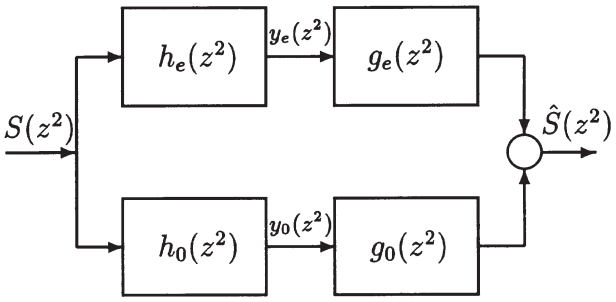


Figure 3

and process them individually before reconstructing the results (see Fig. 3) to obtain

$$\hat{S}(z^2) = \left[g_e(z^2)h_e(z^2) + g_o(z^2)h_o(z^2) \right] S(z^2).$$

But now if $h_e(z^2)$ and $h_o(z^2)$ are coprime polynomials, then we can choose polynomials $\{g_e(z^2), g_o(z^2)\}$ such that (the Bezout identity)

$$g_e(z^2)h_e(z^2) + g_o(z^2)h_o(z^2) = 1 (\text{or } z^d)$$

holds, which means that the signal can be recovered perfectly (or with a delay d). So, in the absence of noise, we shall have perfect equalization, and moreover using FIR filters, provided of course that we can identify $h_e(z^2)$ and $h_o(z^2)$. For this we first form the covariance matrix of the received pair of sequences $\{y_e(k), y_o(k)\}$, and take its z-transform to obtain the power spectral density matrix. Assuming that the input signal sequence can be modeled as uncorrelated equal variance (unity for convenience), this matrix will be as shown below:

$$z\left\{\begin{bmatrix} Ey_e(k)y_e^*(k-i) & Ey_e(k)y_o^*(k-i) \\ Ey_o(k)y_e^*(k-i) & Ey_o(k)y_o^*(k-i) \end{bmatrix}\right\} = \begin{bmatrix} h_e(z^2)h_e^*(z^{-2}) & h_e(z^2)h_o^*(z^{-2}) \\ h_o(z^2)h_e^*(z^{-2}) & h_o(z^2)h_o^*(z^{-2}) \end{bmatrix}$$

Now when $h_e(z^2)$ and $h_o(z^2)$ are coprime, we can find $h_e(z^2)$ as the common factor of the (1,1) and (1,2) entries. Similarly for $h_o(z^2)$! So, in the ideal case, we have shown that we can equalize a nonminimum-phase channel using oversampling FIR filters and second-order statistics.

The basic ideas behind this surprising result were first presented in the paper of Tong, Xu, Kailath (Asilomar Conf. Proceedings, 1991; IT Trans. 94); the presentation given above also uses ideas from further joint work with Hassibi (IT, Jan 95; Asilomar, 93). We should mention that the multiple channels that oversampling allows us to define are directly available when antenna arrays are used; this is explained in the Asilomar 93 paper.

Of course the above procedure is sensitive to the effects of noise and of error in estimating the covariance functions using a finite amount of data. The noise can be accounted for by using least-squares or the more recent H_∞ (minimax) filtering criteria. The development of effective algorithms in the finite data case is currently an area of active research. There are three classes of techniques for approaching this problem: Sylvester Matrix Techniques, Subspace Techniques, and Linear Prediction and Smoothing Techniques.

We refer for details on these results to the now-extensive literature, which appears largely in signal processing journals. Recent survey articles include Liu et al., Signal Processing, 1996, and a follow-up survey by Tong and Perreau, appearing in a special Oct.98 issue of the IEEE Proceedings on Blind System Identification and Estimation.

3. Matched Filters; North, Kotel'nikov and Shannon

The origins of signal detection theory go back to World War II when researchers began to explore the possibilities of replacing human decision makers peering at a radar screen with an automated decision making device. One of the most famous early results here is the matched filter, introduced by the physicist D.O. North in a 1943 RCA Princeton lab report (reprinted in the Proc. IEEE Jul. 1963). The matched filter maximizes the output SNR for a known signal corrupted by additive noise. North makes a remarkably advanced analysis of radar problems, showing great facility with statistical calculations (the Rice distribution appears here) and physical approximations. Unfortunately for us, "at the end of the war, solid-state physics beckoned, and [North] turned to it." [North passed away, in his nineties, a few weeks before the symposium; however, Vince Poor and Sergio Verdú did manage to talk to him by phone a few weeks earlier.] While North computed the probabilities of detection and of false alarm, he was not aware of the Neyman Pearson lemma showing that calculating the likelihood ratio enabled an optimal tradeoff between these two probabilities. The famous mathematician, M. Kac, used to joke that his main contribution to the war effort was providing a reference to the Neyman-Pearson theory to A.J.F. Siegert. In digital communications problems (e.g., FSK, PSK) the criterion is minimiz-

Continued on page 35

Reflections of Some Shannon Lecturers (continued)

The following brief commentaries by four recipients of the Shannon Award provide enlightening personal insight into the minds and attitudes of those who reached the pinnacle of achievement in our field. All but the last of these these reflections were not available in time for their inclusion with those that appeared in the Summer 1998 Special Golden Jubilee Issue of this Newsletter. The final piece, by Jacob Ziv, is reprinted here due to an error in its original printing.

The Eds.

Mark Semenovich Pinsker
(1979 Shannon Award Recipient)

[Editors' Note: Mark S. Pinsker was invited to be the Shannon Lecturer at the 1979 IEEE International Symposium on Information Theory, but could not obtain permission at that time to travel to the symposium. At the 1995 symposium, he was officially recognized by the IEEE Information Theory Society as the 1979 Shannon Award recipient.]

It does not often happen that the name of the founder of a theory and the theory itself are as closely linked as the name of Claude Elwood Shannon and information theory. Many others have contributed to the development of this theory, but Claude Shannon towers over every one of us.

The great Kolmogorov was the first to appreciate the importance of Shannon's ideas for mathematics as a whole. His remarkable words about Shannon made an indelible impression on me. This is what he wrote:

> "In our age, when human knowledge is becoming more and more specialized, Claude Shannon is an exceptional example of a scientist who combines deep abstract mathematical thought with a broad and at the same time very concrete understanding of vital problems of technology. He can be considered equally well as one of the greatest mathematicians and as one of the greatest engineers of the last few decades. ... It is true that Shannon left to his followers the strict mathematical validation of his ideas in cases of real complexity. However, his mathematical intuition is amazingly correct. I know of only one case where his intuition seems to have deceived him: the correctness of the formula for λ at the end of Appendix 7 to his paper 'The mathematical theory of communication' is open to doubt."

The mentioned formula is about "the dimension rate per time unit", based on the calculation of the (ϵ, δ) entropy of a random process per time unit. The most striking thing was that even in this case Shannon's "amazingly accurate" mathematical intuition did not fail him. Years later it was proved that Shannon's formula in Appendix 7 was correct—it was he who was right and not Kolmogorov!

In 1965 Shannon visited Russia at the invitation of the Alexander Popov Scientific and Technical Society of Radio Engineering and Electrical Communications. He met Kolmogorov, Kotelnikov, Siforov and the world chess champion, Mikhail Botvinnik. He even played a game of chess with the latter. He lost, but accepted the defeat with dignity. Boris Tsybakov, who was present at Shannon's meeting with Kolmogorov, told me that Shannon tried to arouse Kolmogorov's interest in a problem of multi-user channels. Many people who chanced to meet Shannon then recall him as a very attractive man with delicate features, a somewhat swarthy complexion, and a graceful stature and style of dress.

In the USSR, information theory, influenced by Kolmogorov, was developing with a visible mathematical "bias", although Kolmogorov himself had a keen interest in the applications of information theory and used to question me closely about various models of communication channels, sources, etc. He admired Shannon's engineering intuition no less than his mathematical insight.

The ideas of Shannon's information theory spread rapidly to a variety of scientific domains and this has been reflected in the activities of our institute in Moscow, the Institute for Information Transmission Problems of the Russian Academy of Sciences. Conceived as a community of engineers and mathematicians, the institute soon incorporated biologists and then linguists. It is now a broad community of scientists whose contributions are known the world over. However, in the beginning was the word of Claude Elwood Shannon.

William L. Root
(1986 Shannon Lecturer)

I was regrettably slow in coming to a real appreciation of Claude Shannon's magnificent theory of information, and unfortunately, was not very much directly motivated and instructed by his work. In 1952 when I joined the staff of the MIT Lincoln Laboratory in Bill Davenport's communication group, I was made aware of Shannon and his 1948 paper. But I was then trying to learn some stochastic process and statistical inference theory and did not pay much attention — not even when a little later Tom Pitcher and I checked through Amiel Feinstein's proof (handwritten by Feinstein on a couple of sheets of paper) of a channel coding theorem.

In 1968 Pravin Varaiya and I published a long paper on the capacity of a continuous-time Gaussian channel for which the signal is transformed by a linear integral operator known only to belong to a certain class of operators. Our treatment was based on a 1959 paper of Blackwell, Breiman and Thomasian "The capacity of a class of channels," with no reference to Shannon. We were certainly motivated and influenced by Shannon's development of information theory, but only through intermediaries. This was my only research

venture into what might be called classical, probabilistic Shannon information theory.

In one instance though I felt Shannon's influence directly in a sort of backhanded way. This was in the late 1970's. I had become interested in coding for channels that are not characterized probabilistically, with the constraint that any admissible code possess a decoding scheme yielding zero error. I was not motivated by any particular thing I had read and was totally unaware of Shannon's classic paper "The zero-error capacity of a noisy channel." In my approach to this problem, I defined a channel as a set of mappings from input (transmitter) to output (receiver), this set to be known to both communicators but the particular mapping in effect over a given time interval unknown to both of them. Included are certain channels with finite, but not necessarily zero, memory. I presented some preliminary results on attainable rates and channel capacity for such channels at a NATO Institute in 1977. At this presentation Jim Massey pointed out that one of my theorems on zero-error capacity was false in the generality stated — a counterexample being provided by a channel whose adjacency graph is a pentagon and discussed in the Shannon paper just mentioned. The zero-error capacity of such a channel had been left as an open problem by Shannon and was not determined until later by L. Lovasz, but Shannon had done enough to give the counterexample. I need hardly add I then read the 1956 Shannon paper. Eventually I accumulated enough special results in this area to warrant a paper in the IT Transactions—at least so I thought, and also, grudgingly, did the editor. The paper appeared in 1982; it incorporates a few of Shannon's results, but I was not able to use his elegant approach to extend what I had done.

David Slepian
(1974 Shannon Lecturer)

Shannon's monumental paper "A Mathematical Theory of Communication" was first published in two parts in the July and October 1948 editions of the Bell System Technical Journal. At that time I was a graduate student in physics at Harvard starting my doctoral thesis. I was granted my degree in the summer of 1949 and in the fall of that year, as a Parker Fellow in physics from Harvard, I went off to Europe to spend my last year as a student.

In September 1950 my real professional career began when I accepted an offer to work in the Mathematics Research Center of Bell Laboratories. I had interviewed at the Laboratories in several departments searching for a physicist and was quite surprised and pleased that the offer came from the Mathematics Research Center, for the truth of the matter was that the part of physics that I enjoyed most was the mathematical one. However, as I had never taken any graduate pure mathematics course, I felt somewhat uncertain that I could handle the job before me. On my first day of the new job, my boss, Brockway McMillan, gave me Shannon's paper to read and study. I had never before heard of Shannon or of Information Theory. Was this paper of importance to me? For the next 32 years, the duration of my entire professional career, at least 3/4 of my waking hours were devoted to pondering this theory and its many consequences. As I worked on and became more familiar with the earlier work on communications, I came to see what a truly remarkable contribution had been made by Shannon. This paper was a gem.

Was this paper of importance to others? At first mainly to the theorists. Many of the remarkable ideas for improving communications that were suggested there were soon seen to be too complicated to be realized practically with the existing technology. But then in the sixties and seventies along came integrated circuits and practical computers and new levels of manipulating signals were attainable. The ideas contained in Shannon's paper could be implemented. The present "explosion of the digital world" is the result. As to the theoretical importance of this paper, as more and more scientists have come to appreciate its generality, its profundity, and its originality, it has come to be regarded by many as the greatest contribution to science and technology by a single scientist in the last half century. I thoroughly agree, as will surely most readers of this *Newsletter*.

The readers of this reminiscence would of course like to hear some words about Shannon himself. My office was two doors down from his for the six years 1951-1956. We were friends who chatted together, sometimes talked shop a bit, but never were co-workers. Claude was way out of my class for me to suggest that, and he by nature was a lone worker, one of the few on the corridor who worked with his door closed. He was much interested in the theory of computers at that time and I believe that the only workers at Bell with whom he collaborated during that period were Edward Moore and David Hagelbarger whose interests were close to his. I consulted with him occasionally on difficulties in my work. He was always ready to hear me out and almost always had an immediate understanding of the problems and useful suggestions to make. But my more usual sources of aid and sympathy were Brock McMillan and Ed Gilbert with whom I consulted much too often, I'm sure.

A good feeling for Shannon's personality can be had from the two interviews with professional reporters that are reproduced in the introduction to *Claude Elwood Shannon, Collected Papers* by Wyner and Sloane, IEEE Press, 1993. I believe two caveats are appropriate with regard to these interviews. They may give the impression that Shannon was shy. I do not think he was; he just did not care to become instant buddies with everyone. They also fail to show how lightly he took life. Many things about our society amused him and he did enjoy to laugh at them privately. In making his many machines I always thought Claude was having great per-

Continued on page 38

President's Column

Thomas Ericson

Thomas Ericson

So the feast is over. ISIT'98 is finished and we are all going back to work. I predicted in my previous column that this symposium should be an exceptional event. Although that was an easy prediction to make I am very pleased to be able to conclude that I was 100 percent right and that the symposium was a complete success. On behalf of the IT-Society I like to express our sincere thanks to all of you who made this success possible. It will not be possible to mention all of you, but a few names deserve to be mentioned explicitly. First of all I like to mention the general co-chairs, Dave Forney and Bob Gallager. I was in a position to closely follow the preparations of the symposium and I can only say that I am deeply impressed by the devotion and skill with which this work was carried through. I also like to mention the two program chairs, Vince Poor and Sergio Verdú. They had to handle a larger number of contributions than ever before in the history of the IT-symposium. I think we all agree that the result was just excellent. It should also be remembered that many of the special events that occurred during this symposium were initiated by Sergio during his term as president of the IT-Society. Those initiatives together with the devoted contributions by all who participated - organizers, authors, invited speakers and others - made this symposium an event that will be long remembered.

What will happen now? We have seen 50 years of marvelous development, what will be the activities carried through during the next 50 years? Information theory is more vital than ever. Exciting work is going on all over the world. However, I don't think anyone is able to even roughly guess what will be the outcome of all these activities in a 50 year perspective. The only prediction I dare to make is that 50 years from now the field will still be active. There will still be exciting problems to attack and there will still be a large number of gifted engineers and mathematicians devoting themselves to those problems. I am pretty convinced that 50 years from now there will again be reasons for an anniversary celebration.

Let us shift perspective. If 50 years from now the IT-Society is still active and if the 100 year anniversary is celebrated, what will the view be that those people taking part in that celebration will have of our present time? What will they regard as the most important of the events taking place right now. Also this, of course, is very difficult to predict. Certainly their view will be very different from ours. One thing that almost certainly will be different at that time is the form of publication. We have already seen the first few steps in the direction towards electronic publication. It is hard to tell exactly how this process will develop, but personally I am fully convinced that electronic publication will fundamentally change the way scientific results are communicated, exchanged and stored. The IT-Society is well ahead in this respect, with the involvement in the OPERA project and with the Digital Library. Clearly, what for us today is advanced high tech will appear very primitive when looked back upon 50 years from now. However, I would not be surprised if - 50 years from now - the production of the Digital Library in connection with ISIT98 will viewed as a turning point within the society and as an important first step in its development towards an entirely new era of scientific documentation. Some of you reading this column might get a chance to be there to see.

The jubilee year is rapidly approaching its end and so is my term as the society president. The present column is the last one I will write in this capacity. It is natural that I conclude with a few personal reflections. It has been a marvelous year with a large number of memorable events. To the BoG, to all officers and to all of you who are involved one way or the other in various tasks within the society, let me say that it has been a great pleasure working with you. I like to thank you all. I knew it before, but now I understand it even better: what makes the IT-Society unique is the quality of the people involved. It is not only the exceptionally high standard of the scientific contributions that makes this society special, but also the very good spirit in which we are interacting. By January 1, 1999 Ezio Biglieri will take over as the next president. Ezio, I wish you a very pleasant term. From time to time it will be hard work, but believe me, it will be exciting all the time. Good luck!

The Historian's Column

A. Ephremides

A. Ephremides

One rarely finds individuals who excel in very diverse fields of endeavor. For example, the well-known (and deceased) Danny Kaye was a superlative actor, an accomplished surgeon, a music conductor of some stature, and a competent aviator, among other things. And, in our field, its very founder was not only a brilliant scientist and engineer but also an inventive hobbyist who built scores of whimsical devices from unicycles to juggling machines. But there is more! If one looks beneath the surface, one finds that many of our colleagues have multiple talents and do excel in areas other than what we best know them for.

These thoughts come to mind when I read some intriguing materials that come my way via (who else?) the Historian "par excellence," Toby Berger, who, in turn, had received them from Don Snyder, to whom they were sent by Bob Price. Through this long chain of communication, there was a danger that, the data processing theorem being always at work, something from the original story might be lost or distorted. So, I will try to tread the ground cautiously.

Many of you are aware of (or perhaps carefully read) the article by Bob Scholtz in the May 1982 issue of the *IEEE Transactions on Communications* about the origins of Spread-Spectrum Communications. That is a fine piece of research that lets unfold some sense out of the murky background (hidden in a veil of secrecy) that preceded the development of spread-spectrum ideas and systems as we know them today. The author gratefully acknowledges in that article the immense help provided by Bob Price who supplied tons of information on the early work of many individuals and groups who contributed to this development.

And, yet, a crucial piece of hidden information eluded even Bob Price's initial search. Thus, the article in the Transactions did not give credit to an unlikely individual who, perhaps more than most, contributed to the development of frequency-hopped spread-spectrum systems. Bob Price discovered this information a little too late for inclusion in the special issue of the Transactions, but gave it full prominence in a subsequent article in the newsletter of the Sperry Research Center in September of 1982. Also, later on, an article in the *IEEE Spectrum* (September 1984) makes reference to this story.

What Bob Price discovered was a fascinating story about a lady who fled Nazi Germany and became a glamorous Hollywood actress and who, during the early phases of World War II, (get ready for this) invented the concept of frequency hopping and obtained a U.S. patent for it! It may be hard to believe, but it is also hard to understand. How could a screen actress have a secret talent for engineering design? And yet, it is all clearly documented.

Hedy Lamarr (the lady's name) was born in Vienna, Austria and, after already becoming famous for a sexy film called "Ecstasy" at the tender age of 19, she married the pro-Nazi armaments manufacturer Fritz Mandl in a marriage arranged by her parents (as one finds in many operas). She became so revolted by her condition and by her husband's dealings that she escaped to the United States where she settled to develop a successful career as an actress.

It gets even more incredible. She met the then avant-garde composer, George Antheil at a Hollywood party. Antheil was known at the time as "the bad boy of music." Lamentably, there are too many such "boys" nowadays! In a coup of explosive motivation and inventiveness, the two of them developed a system that would allow the signal that controlled the trajectory of a torpedo to hop across a wide band of frequencies so as to escape jamming. Apparently motivated by her desire to undercut the armament products of her ex-husband, Ms. Lamarr developed not only the idea but an actual implementation of such a system. A patent for their "Secret Communication System" was granted in 1942. A clipping from the October 1, 1941 edition of the *New York Times* reveals the news that the famous actress had made an invention that was so vital to national defense that, as Colonel L.B. Lent, chief engineering of the National Inventors council, put it, it was classified in the "Red Hot" category. The only information revealed at the time was that the invented device was related to remote control of apparatus employed in warfare.

Bob Price has, since, engaged in many efforts to get Ms. Lamarr the recognition she deserves. He actually interviewed her and tried to persuade IEEE to recognize her with an award (alas, unsuccessfully). Eventually, however, due to the efforts of David Hughes (described in a Naples (Florida) *Daily News* article in March, 1997, as a "researcher at the National Science Foundation") an award in recognition of her and composer Antheil by the Electronic Frontier Foundation was presented at the Computers, Freedom, and Privacy Conference in San Francisco in early 1997. Ms. Lamarr, who from Bob Price's description emerges as an independent and bold spirit, greeted the news about her award with the words: "It's about time!" As of the writing of the materials that came my way, Ms. Lamarr was alive and well in Florida, but shunning the public spotlight.

Photo courtesy of AP Wide World Photos

Photo courtesy of AP Wide World Photos

Now, isn't that a fascinating story? A beautiful, motivated, multi-talented lady whose main activity in which she excelled was acting, touches our field briefly but in a most fundamental way and leaves a memorable imprint of her genius. Buried in U.S. Patent No. 2,292,387, are the details of her invention that anticipated many of the subsequently developed systems such as Sylvania's BLADES and others.

Giving this story the publicity it deserves among our readers has been truly a pleasure. We owe an immense debt of gratitude to the tireless efforts of Bob Price, who unearthed the story and who followed up diligently over the years. Both he and Don Snyder graciously gave permission to use their private communication. In addition, our thanks should go to Toby Berger who truly has an "eye" for items worthy of historical attention.

And this brings me back to my musings about multiple talents that started this column. There must be other examples out there that show that intellectual prowess often manifests itself in diverse ways I am sure that the readers (and I) would love to know about them.

Electronic Submission of Manuscripts to the IEEE Transactions on Information Theory

INFORMATION FOR AUTHORS

Overview:

The *IEEE Transactions on Information Theory* will now be supporting electronic submission of manuscripts. The electronic submission is optional, and is intended to expedite the review process.

Submission Procedure:

The author(s) should submit two e-mails to the Editor-in-Chief, one containing a cover letter and the other containing the postscript file of the paper. Alternatively, postscript files may be submitted via FTP (see below). All e-mails should be addressed to:

submit@it.csl.uiuc.edu

The cover letter must be submitted by e-mail. It should be phrased in the same way as it would be normally phrased for conventional hard copy submission. In addition, this letter must contain the following information items:

- Title and abstract of the paper. The abstract may be appended at the end of the cover letter, as plain text. Do *not* send the abstract as an attachment. In case the abstract contains mathematical expressions, LaTeX notation may be used.
- Information about the postscript file of the paper indicating whether it is submitted by e-mail or via FTP, including the file name (for FTP submission) or the subject line of the corresponding e-mail (for e-mail submission).
- Name, address, phone number, fax number, and e-mail address of all the authors.
- Manuscript type designation (regular paper or correspondence).
- Associate Editorial area suggested by the author(s).

Author submitting e-mail that contains the cover letter will be automatically assigned as the corresponding author for the paper.

The postscript file of the manuscript should be submitted in one of the following two ways. It may be sent by e-mail as plain unencoded ASCII text. The postscript file should be included in the body of the e-mail. Do *not* send it as an "attached" document. The subject line of the e-mail should be composed of the last name of the corresponding author, followed by the "ps" suffix. (For example, a subject line consisting of shannon.ps would be a valid one.) Alternatively, the postscript file may be submitted via FTP (Internet File Transfer Protocol). To do so, authors should access the following FTP site:

ftp.it.csl.uiuc.edu

login as "anonymous" using e-mail address as password, and put the postscript file in the it_submit directory. The file name should be composed of the last name of the corresponding author followed by the "ps" suffix (e.g., shannon.ps). More detailed instructions for the FTP submission procedure may be obtained by sending e-mail to the following address: help@it.csl.uiuc.edu.

Copyright:

Electronic submission implies a transfer of copyright to the IEEE in accordance with IEEE copyright agreement. If a submission is accepted for publication, a written and signed copyright form would have to be provided by the corresponding author.

Review Procedures:

Manuscripts submitted in electronic form will be reviewed according to the usual editorial procedures and standards of the *IEEE Transactions on Information Theory*. However, the intent is to have all communication between authors, editors, and referees by e-mail, thereby expediting the review process.

Hard Copies:

Hard copies of papers submitted in electronic form ordinarily will not be required. However, the authors should be ready to provide such hard copies at all stages of the editorial review process, upon request from the Editor-in-Chief or from the Associate Editor assigned to the paper. In addition, if and when a paper is accepted for publication, two hard copies of the final version of the paper will be requested from the authors.

IEEE Information Theory Society Board of Governor's Meeting, Killarney, June 22, 1998.

Attendees: Venkat Anantharam, Andrew Barron, Vijay Bhargava, Ezio Biglieri, Sean Coffey, Daniel Costello, Anthony Ephremides, Thomas Ericson, Dave Forney, Tom Fuja, Jerry Gibson,Hideki Imai, Kees Immink, Bob McEliece, Steven McLaughlin, David Neuhoff, Greg Pottie, Ramesh Rao, Shlomo Shamai, Alexander Vardy, Han Vinck, Sergio Verdu, Steve Wicker, Jacob Ziv

1.The meeting was called to order at 5:11 PM by Thomas Ericson. Those present introduced themselves.

2. The agenda was approved.

3. Thomas Ericson reviewed decisions of the previous meeting for follow-up actions. The minutes were then approved.

4. Progress on the special newsletter issue was reported by Tony Ephremides. It will include quotes from Shannon award winners and some who know Shannon. It will be mailed as a fifth issue to all IT members and also 1000 copies will be printed for other distribution such as at ISIT. The total cost is expected to be between 15k and 25k. It was suggested it also be posted on the web. Kees Immink moved to authorize spending of up to 25k for the special issue. The motion carried.

Greg Pottie

5. Dan Costello reported on the Golden Jubilee paper awards selections. Fifteen papers were recommended by the committee to receive the award. A suggestion was made to create a set of reprints of the Golden Jubilee and Information Theory Society paper awards, as a book. The book potentially has significant overlap with another IEEE press book. Ramesh Rao suggested that we consider inserting bookmarks in the CD ROM cumulative paper collection, and investigate putting in some classic IRE papers as well. Both matters will be investigated by Steve McLaughlin.

6. Jerry Gibson presented the report of the committee for the Golden Jubilee awards for technological innovations. There are 17 nominees. Thomas Ericson has written letters of congratulations for both the paper and technological awards, extending invitations to the awards ceremony to take place

at ISIT in Cambridge MA. Vijay Bhargava expressed the thanks of the BoG for the work done by the committee chairs.

7. Announcements

i) Andrew Barron reported on Shannon Day at Bell Labs, which also recognized Aaron Wyner's contributions. The activities focused on both the early contributions of Shannon, and later developments. There were roughly 400 attendees; registration had to be stopped a month before because of the large interest.

ii) Sergio Verdú reported on the KNAW Colloquium in Amsterdam. This was a three day colloquium with fifteen speakers and 40 attendees. The small size had the desired effect of generating considerable discussion on the future direction of information theory.

iii) Thomas Ericson reported on the proposed Millenium booklet for the IEEE (intended as a coffee table book). Each Society is supposed to contribute their views on the next millenium; interviews will be done by a professional writer. He is soliciting suggestions on names of Information Theory Society members to be interviewed.

8. The next BoG meeting will be on Sunday Aug. 16 at 9:00 AM in Cambridge MA, at the student center (room to be announced).

9. Thomas Ericson presented the treasurer's report. The Society has a net worth of $1.6M with outstanding loans of $5K to ITW San Diego, Ireland, and South Africa, $25K to ISIT Cambridge, and $10K to ITW Metsovo, Greece. The books have been closed for Haifa and Ulm. It was noted that there is a new grants department in IEEE TAB, to help conference organizers secure outside funding. The contact is Karen Galuchie, k.galuchie@ieee.org.

10. The Information Theory Transactions report was made by Alex Vardy.

i) Increased page budget. The first three issues spanned 1300 pages; the linear projection from this is 3400 pages for the year, which is far above the page budget of 2600. Thus, there is the potential for a backlog given the editorial resources, even though the next two issues appear to be running at a more moderate pace. Given that increased page count is a long term trend, Dave Forney observed that we may need to consider going to 12 issues per year. There was consensus that this is a serious issue requiring some deliberation. The matter will be considered by the editor and associate editors, and will be discussed by the BoG in subsequent meetings.

ii) A report on electronic submission and publication was presented. The new procedure would enable submission by e-mail or ftp, and review would also be done by e-mail insofar as possible. The intention is to speed things up, given the long latency in the mail system (up to three months in a typical review cycle). Also proposed was an extra editorial assistant for the editor in chief, in part to track papers, and in part to deal with new difficulties in format conversion, etc. entailed by electronic submissions. The expected additional cost is 35K per year. Also envisioned is a system for tracking papers on the web, initially internally, possibly later to enable authors some tracking ability. Bob McEliece proposed approval of the report, amended to allow up to 40K per year for additional secretarial support. The motion carried.

iii) The cover text for the Transactions has not changed from 1959, and reads: "A Journal Devoted to the Theoretical and Experimental Aspects of Information Transmission, Processing, and Utilization." A lively discussion was held on whether this text still adequately describes the purposes of the Transactions, and whether new text might be appropriate. There was no consensus on the need for change.

iv) The BoG approved the new associate editors. They are Venkat Anantharam, Phil Chou, Tom Fuja, Sanjeev Kulkarni, Upmanyu Madhow, Jody O'Sullivan, and Ronny Roth. The BoG also expressed its appreciation to Rob Calderbank for his job as the IT editor in chief, and for the retiring associate editors.

v) Sergio Verdú reported on the special anniversary Transactions issue. It will have 25 papers with a total length of approximately 600 pages, and will appear in October. A hard-covered version is being explored with IEEE press, to be structured as a tutorial book. Steve McLaughlin reports that CRC press and Springer-Verlag are both interested, although IEEE Press has not yet committed.

11. Vijay Bhargava reported that the Claude E. Shannon Award committee will be meeting during ITW Ireland, and will come to a decision prior to the banquet at ISIT.

12. Ezio Biglieri gave the report of the awards committee. The committee has nominated an Information Theory Society member for the Japan prize. Additionally, the committee has selected two papers to be nominated for the IT paper award. A mail ballot will be issued to the BoG to decide on the Information Theory Society paper award by August 1.

13. Fellows committee. The nomination process is well under way; the nominations will shortly be forwarded to IEEE.

14. Digital Library Project.

Steve McLaughlin reported on progress in getting the complete IT Transactions on a set of CDs. Testing of the proposed format is being conducted via the web site, and critical comments are being solicited so that the first version of the disks will be as high-quality as possible. A proposed business plan was circulated. The cost of CDs to IT Society members will be $200, and non-IT IEEE members will be $250, which will include IT Society membership for two years, and some web access for updating. For libraries and other institutional buyers, the price will be $1500. The institutions would not be entitled to web access. Sales will hopefully finance an upgrade to a version 2.0, and if sales are strong, updates to a supporting web site. IEEE has been approached for marketing support. A further $60,000 is requested to complete the project, due to increased cost of producing the disk set, and some additional costs in the project, such as new features (searching

abstracts), more pages than additionally estimated, etc. The Signal Processing Society has expressed some interest in undertaking a similar project, and it should be relatively easy to provide cross-links later between the databases of sister Societies. The IT Society will consider some pro bono distribution of disks (e.g., third world countries). The IEEE electronic library project is moving from CDs to the web, and the IT Society's library may be included in this project, with considerable revenue potential. Progress in this area will shape the IT Society's approach to the web, including update mechanisms for the electronic library. The disks have been formatted to have a simple technical path to placing it on the web, but there are numerous issues concerning access costs and operations. A further and related long run item is the issue of electronic publication, and its myriad financial and procedural implications. A motion to approve the additional funds carried.

15. David Neuhoff proposed that there should be a historical marker in Claude Shannon's home town of Gaylord, MI. The town has considerable tourist traffic year round, and would appear to have a suitable site for a marker. The Society would contribute towards its construction. The BoG expressed support for David Neuhoff moving forward with discussions with the city and state governments, and producing a cost estimate by the next BoG meeting. An appropriate member of the town will be invited to attend historical and award ceremonies at ISIT in August.

16. Membership development

Tom Fuja reported that we have 5670 members, down from peak of 7000 members in 1992. A variety of programs were discussed at a membership development retreat in Baltimore on how to improve recruitment, but none seemed to be directly applicable. Vijay Bhargava noted the importance of overseas membership in the IT Society, and the need for region 8 and 10 members on the membership development committee. Hideki Imai and Han Vinck agreed to serve. He stressed the need to arrange local activities, e.g. through the distinguished speakers program, and establishment of local chapters.

17. The symposia and workshops report was presented by Tom Fuja

i) IT Workshop on Detection, Estimation, Classification, and Imaging, Santa Fe, NM, Feb 24-26, 1999. The call for papers is out, and includes details on the conference. The three plenary speakers are Andrew Barron, Vince Poor and Michael Miller. A web site is up.

ii) Julia Abrahams is organizing through DIMACS a conference on Codes and Trees: Algorithmic and Information Theoretic Approaches, Rutgers U., Piscataway, NJ. The focus is on source coding. Technical co-sponsorship was requested, without financial support. A motion to provide this sponsorship carried.

iii) ICPWC'99 Feb 17-19, 1999, Jaipur, India. Vijay Bhargava requested technical cosponsorship and circulated the call for papers. The BoG approved the request.

iv) IMA workshop in Aug 1999 for Codes, Systems, and Graphs. Dave Forney reported that this is a two-week workshop, which is run by the IMA. One week is focussed on systems, the other week on codes and graphs. Co-sponsorship is not requested; a link has been established on the IT website.

v) IT workshop, March, 2000, British Columbia. A proposal is being developed by Steve Wicker and Vijay Bhargava, and will be presented at the next BoG meeting.

vi) Proposal for ISIT 2001, U. Maryland, DC. Prakash Narayan has given a brief summary of what will be proposed at ISIT in August. Other proposals for ISITs in 2001 and 2002 would be welcomed.

vii) Metsovo and South Africa 99. Han Vinck reported that announcements, technical programs and schedules will be coordinated to avoid overlap and ease travel.

18. ISIT 98. Dave Forney reported that the only major change since February was to include a session on Friday afternoon and reduce the number of parallel sessions to six. A party is scheduled for Friday night. The website includes abstracts, which can be downloaded. 82K in support has been raised from government and industry. Consequently, travel support can be supplied to all who applied. The MIT dorms are full, so there is no more budget accommodation. This follows an unexpected change in MIT's story on dorm availability. Other hotel bookings have been somewhat slow, forcing some rooms to be given up.

19. A decision on the logo contest will be made at the next BoG meeting.

20. Joint awards. Ezio Biglieri has contacted the Communications and Signal Processing Societies regarding establishment of joint awards. There has been little real progress thus far.

21. The meeting adjourned at 8:50 PM.

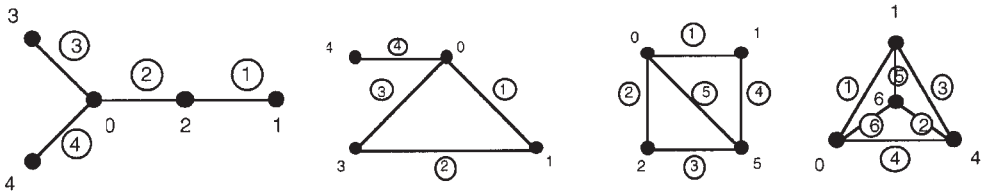
Golomb's Puzzle Column™ Number 44:
Graceful Graphs

Solomon W. Golomb

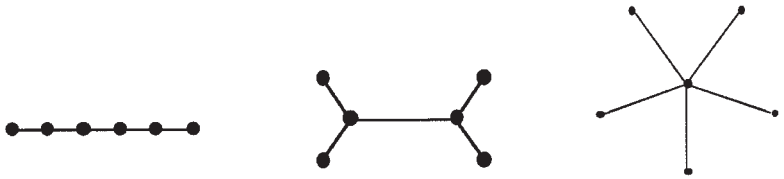
Let *G* be a connected simple graph (no loops, and at most one edge between any two vertices) with *e* edges and *v* vertices. A *graceful numbering* of the vertics of *G* is an assignment of *v* distinct numbers from the set {0, 1, 2, ..., *e*} to the vertices of G such that the edges receive every integer *label* from 1 to *e*, where the *label* on an edge is the absolute value of the difference between the numbers at its two end-points.

If the vertices of G have a graceful numbering, then G is called a *graceful graph.*

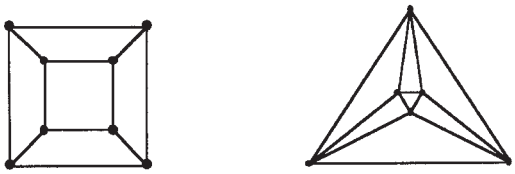
Here are a few examples of graceful graphs.



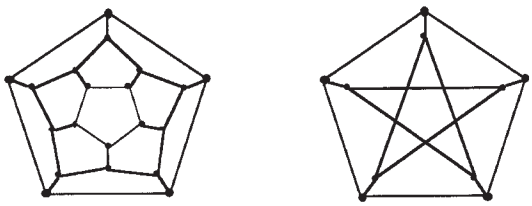
1. Find graceful numberings for the following "trees".



2. Find graceful numberings for the cube and the octahedron.



3. Find graceful numberings for the pentagonal dodecahedron and the "Petersen Graph" if such numberings exist.



The *degree of* a vertex x in a graph G is the number of edges that have x as an endpoint. A *path* on a graph G is a sequence of distinct edges $e_1, e_2, \ldots e_r$ where e_i and e_{i+1} have a vertex in common, for $i = 1,2,\ldots, r-1$. The path is *closed* if e_r and e_1 also have a vertex in common. (A *closed path is* also called a *circuit.)* A circuit consisting of every edge in the graph G is called an *Euler Circuit* of G. Euler proved that a connected simple graph G has an Euler circuit if and only if every vertex in G has even degree.

4. Prove the following theorem: If G is a graph with an Euler circuit, and G has e edges, then G cannot be graceful if either $e \equiv 1 \pmod 4$ or $e \equiv 2 \pmod 4$.

5. Find all connected simple graphs with ≤ 5 vertices which cannot be graceful as a consequence of Problem 4.

6. The "complete graph K_n" has n vertices. Prove that K_n cannot be graceful if $n \geq 5$.

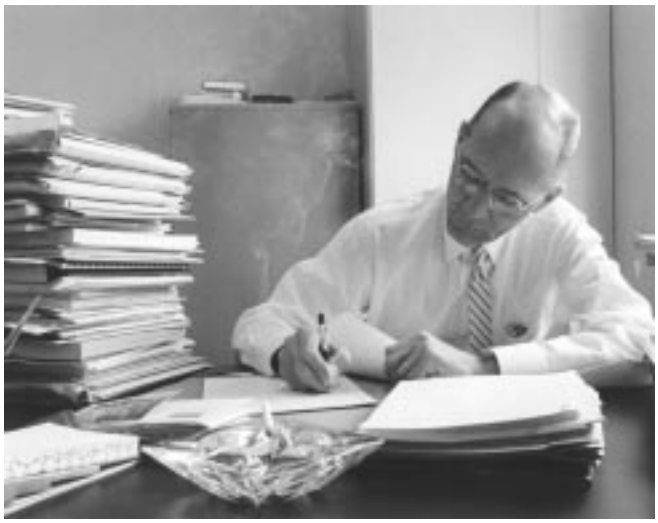
Obituary

Dwight O. North

Among the recipients of the IT Society's Golden Jubilee Awards for Technological Innovation was Dwight O. North, who was cited for his invention of the matched filter. Sadly, Dr. North died on June 26, 1998, just two months before the awards were presented at ISIT'98 at MIT. On September 8, former IT Society Presidents Vince Poor and Sergio Verdú presented the award to Dr. North's wife, Evelyn, at her home in Princeton, New Jersey.

Of course, the importance of the matched filter concept in communications and signal processing hardly needs to be repeated here. Dr. North was the first to formalize this concept, which he published in a 1943 classified report at RCA Labs in Princeton. (North did not use the name "matched filter''. This term was coined by David Middleton and J.H. Van Vleck, who independently published the result a year after North in a classified Harvard Radio Research Lab report.) North's report was later reprinted in the *Proceedings of the IEEE*, in July 1963. This remarkable report introduced not only the matched filter, but also the Rice distribution, the concept of false alarms to set a detection threshold, studies of pre-detection and post-detection integration, among other topics. Its anticipation of so many of the issues that occupied the attention of radar engineers for many years is quite remarkable.

Dwight North, or Don (for his initials - D.O.N.) as he was known to his friends and colleagues, was born in Hartford, Connecticut, and was educated at Wesleyan University and at Caltech, from which he received a Ph.D. in Physics in 1933. From 1934 until his retirement in 1974, he worked for RCA, first in Harrison, New Jersey, and then as an original member of the technical staff at RCA's Princeton labs when they were established in 1942. His interest in noise problems began during the 1930's when he worked on the study of noise in vacuum tubes operating in the 100MHz band, work being conducted at RCA during its development of commercial television. (His interest in noise problems even extended to the naming of the street on which he was a longtime resident in Princeton: Random Road - so named because many of its original residents were RCA "noise" experts, including Dwight North.) During World War II, he worked at the MIT Radiation Lab on the development of radar. After the war, he turned to the study of solid state physics, which occupied most of the remainder of his career at RCA.



According to Evelyn North, Dr. North was typically uninterested in organizational recognitions of his work. However, when he was informed of the Golden Jubilee award in a letter from Society President Thomas Ericsson, he was reportedly very pleased to be recognized in this way. Although Dwight North did not labor long in our field, in inventing the matched filter he left a legacy that will undoubtedly last into the very distant future.

Call For Papers

CISS '99 Conference on Information Sciences and Systems

March 17 - 19, 1999,
Johns Hopkins University,
Baltimore, MD.

Submit a "regular paper" or "short paper" designation, title, summary and a list of 3 - 4 keywords by January 15, 1999 to:

1999 CISS
105 Barton Hall
Dept. of Electrical and Computer Engineering
Johns Hopkins University
Baltimore, MD 21218
Tel: (410)516-7033, Fax: (410)516-5566,
Web: http://www.ece.jhu.edu/ciss99/.

Call For Papers

1999 Information Theory Workshop

Kruger National Park,
South Africa,
June 20 - 25, 1999

Venue: The Berg-en-Dal rest camp in the The Kruger National Park, situated approximately 400km East of Johannesburg, South Africa, provides an ideal wildlife setting for the 1999 IEEE Information Theory Workshop.

This workshop will be the first of two Information Theory workshops to be held during June 1999. The second workshop is taking place in Greece during the week following this workshop (June 27 - July 1, 1999). The organizers of both workshops have co-ordinated their efforts to ensure that the programs of the two workshops will be complementary in nature. This will enable interested parties to attend both workshops. Direct, non-stop service is available between Johannesburg and Athens.

Technical Program: The following sessions are planned with the persons indicated acting as session organizers:

Technical program chairman:	*Han Vinck*
Plenary speakers:	*Jim Massey and Te Sun Han*
Identification:	*Te Sun Han and Rudi Ahlswede*
Cryptology and communication security:	*Henk van Tilborg*
Source coding theory and techniques:	*Frans Willems*
Modeling and performance of high speed networks:	*Tony Ephremides*
Multiuser communication:	*David Tse and Sergio Verdú*
Coding and modulation for fading channels:	*Ezio Biglieri*
Spread-spectrum communication theory and techniques:	*Michael Pursley*
New Results in information theory and coding:	*Mario Blaum*

Sponsorship: The Workshop is sponsored by the IEEE Information Theory Society.

Organizing Committee:
Co-Chairmen

Shu Lin: Dept. of Electrical Engineering, University of Hawaii at Manoa, 2540 Dole Street, Holmes Hall 483, Honolulu, Hawaii 96822, USA. E-mail: slin@spectra.eng.hawaii.edu, Tel: +1-808-956-8403, Fax: +1-808-956-3427.

Hendrik Ferreira: Dept. of Electrical Engineering, Rand Afrikaans University, P.O. Box 524, Auckland Park, 2006, South Africa. E-mail: hcf@ing1.rau.ac.za. Tel: +27 11 489-2463. Fax: +27 11 489-2357.

Local Arrangements

Walter Penzhorn: Dept. of Electrical and Electronic Engineering, University of Pretoria, Pretoria 0002, South Africa. E-mail: Walter.Penzhorn@ee.up.ac.za Tel.: +27 12 420-2164, Fax: +27 12 348-0946.

Francis Swarts: Dept. of Electrical and Electronic Engineering, University of Pretoria, Pretoria, 0002, South Africa. E-mail: fafa@didgeridoo.ee.up.ac.za. Tel: +27 12 420-2872. Fax: +27 12 362-5000.

Recent Results Session: Those interested in a presentation in the new results session are invited to submit a summary, ISIT style, by January 31, 1999, to Dr. Mario Blaum, IBM Research Division, Almaden Research Center K65/C2, 650 Harry Road, San Jose CA 95120, USA, E-mail: blaum@almaden.ibm.com, Tel: +1 408 927-2179, Fax: +1 408 927-4110. Two recent results sessions are planned, one focusing on coding the other on information theory in general.

Social Program: Reception, cocktail, banquet and a day excursion in the Kruger National Park. In addition to this, daily game drives will also be available.

Registration Fee:

On/before April 20, 1999	IEEE Member: US$320	Non-Member: US$370	Students: US $80
After April 20, 1999	IEEE Member: US$395	Non-Member: US$445	Students: US$155

Accommodation: Please contact Annette Raubenheimer at Supersonic Travel (E-mail: sonic@ccnet.up.ac.za, Tel: +27 12 420-4085/6, Fax: +27 12 362-5139, P.O. Box 26032, Arcadia, Pretoria, 0007) for assistance in arranging accommodation for the workshop. **Very Important:** This is the only travel agent through which accommodation for the workshop can be arranged. Please be sure, when contacting Supersonic Travel, that you mention that you are wanting to arrange accommodation specifically for the 1999 Information Theory Workshop.

Further Information: Please contact any of the organizers or visit http://www.wits.ac.za/ITW99.

From the Editor . . .

continued from page 2

process, I will here note a few. Thanks are owed to the regular contributors of columns: Tony Ephremides with his "Historian's Column," Sol Golomb with "Golomb's Puzzles ™", Greg Pottie with the minutes from the Board of Governors Meeting, and Raymond Yeung with his regular column on "New Books" have kept the readers amused, challenged, and informed through all three years of my term as editor. I have also received invaluable support from three Information Theory Society presidents — first Jerry Gibson, then Sergio Verdú, and now Thomas Ericson — to all of whom I owe great thanks both for their regular columns and for their help and encouragement in much of the behind-the-scenes work that goes into the Newsletter's creation. Thanks also go to the incoming Society president, Ezio Biglieri; to the staff at IEEE, in particular Ann Goedkoop, Robin Edwards, Andrea Watson, and Bob Smrek; and to a variety of Society members and officers including Ramesh Rao, Rob Calderbank, Steve McLaughlin, Vijay Bhargava, Ubli Mitra, and Alex Vardy. Finally an enormous number of individuals have willingly contributed their time and talents to writing feature articles, chasing down stories, and keeping me informed of relevant awards and events for the Newsletter; I owe great thanks to all of them and all of the others who have encouraged and challenged me with their feedback.

As usual, your comments and suggestions on the Newsletter — past, present, and future — are welcome. Since the new editor for the Newsletter has not yet been announced, materials for the March 1999 issue of the Newsletter should be sent to my address.

Michelle Effros
Department of Electrical Engineering (MC 136-93)
California Institute of Technology
Pasadena, California 91125

USA

Tel: +1 (626) 395-3729
Fax: +1 (626) 564-9307
e-mail: effros@caltech.edu

Electronic submission, especially in LaTeX format, is encouraged. All submissions will be forward to the new editor. The deadlines for receiving material for the next few issues are as follows.

Issue	Deadline
March 1999	January 15, 1999
June 1999	April 15, 1999
September 1999	July 15, 1999
December 1999	October 15, 1999

CALL FOR PAPERS

3rd International Symposium on Power - Line Communications, PLC'99

Lancaster House Hotel,
Lancaster, UK,
30 March - 1 April 1999
Sponsored by IEEE Communications and Information Theory Chapters (UKRI Sections), H W Communications Limited

General Chairmen

Prof Bahram Honary
Communications Research Centre
Lancaster University
Lancaster
LA1 4YR, UK

Prof A J Han Vinck

University of Essen
Essen, Germany

Secretariat

Dr Nader Zein

Executive Committee Members

Prof M Darnell
University of Leeds, UK

Prof P G Farrell
Lancaster University, UK

Dr P Brown
NOR.WEB DPL Ltd, UK

Dr J Newbury
European Standardisation Committee, UK

Session Organizers

Prof A J Han Vinck
University of Essen, Germany

Dr J Newbury
European Standardisation Committee, UK

Prof B Honary
Lancaster University, UK

Prof Ryuji Kohno
Yokohama National University, Japan

Dr P Brown
NOR.WEB DPL Ltd, UK

1999 International Symposium on Power Line Communications (PLC '99) focuses on the general problem of communications over power lines. The aim is to cover as many topics as possible, from a practical as well as from a theoretical point of view. We intend to stimulate exchange of research results and new problems between scientists and engineers working in this field. Building on the initial success of Essen in 1997 and Japan in 1998, PLC will be held in the UK, from 30 March to 1 April 1999.

You are invited to submit original papers addressing topics in power-line communications for presentation at the conference and for publication in the conference proceedings. Topics may include:

- Channel Characterization
- Modulation, Error-Control Coding and Synchronization
- Experimental Systems
- Simulation
- LSI designs for Power-line Communications
- Spread Spectrum Techniques
- Signal Processing: Algorithms and Devices
- System Architectures
- Power-line Communication Networks
- Power-line Communication Services
- Multiple-Access Techniques
- Developing Standards

Paper Submissions

Authors are invited to submit three (3) copies of abstract (no more than 500 words) in English. Each submission must be accompanied by a letter that includes the following information: full title of paper, author(s), affiliations, postal and email addresses, telephone and fax numbers.

All presenting authors must register as delegates. Submissions should be addressed to the secretariat.

Dr Nader Zein
Communications Research Centre
Lancaster University
Lancaster
LA1 4YR
Fax: 44 1524 594207
E-mail: n.zein@lancaster.ac.uk

Deadlines:

Extended Abstract Nov. 10, 1998
Notification of Acceptance Dec. 10, 1998
Camera Ready Manuscript Due Feb. 20, 1999

1999 Information Theory and Networking Workshop

Metsovo, Greece, June 27–July 1, 1999

An Information Theory Workshop will be held in the beautiful mountain resort village of Metsovo. Off the beaten path and perched at an altitude of 1115 meters (3345 feet) in the magnificent mountain range of Pindos in northwestern Greece, Metsovo will provide a tranquil, and comfortable environment in a friendly setting of traditional Greek hospitality.

The workshop will embrace the main themes of Information Theory, but will also place an emphasis on Communication Networks in an attempt to bring together researchers from both fields.

Technical Program: The technical program will include:

Plenary Talk:	P. Flajolet, J. Kieffer, and P. Varaiya.
Panels:	Role of IT in Multimedia (G. Seroussi, M. Weinberger) Pricing in Networks (C. Courcoubetis, B. Prabhakar) Role of IT in Networking (A. Ephremides, R. Rao)
Invited Sessions:	Network Shannon IT (A. Lapidoth, Z. Zhang) Source Coding (I. Kontoyiannis, N. Merhav) IT and Queueing (V. Anantharam, D. Tse) Fundamentals of Networks (L. Tassiulas) Cryptography and Security (C. Cachin, H. Tilborg) Coding and Communications (D. Forney, A. Vardy)
Recent Results:	There will be a poster session to accommodate recent results.
Program Committee:	Leonidas Georgiadis Philippe Jacquet Wojciech Szpankowski Tony Ephremides (Advisor)
Local Arrangements:	Niovi Pavlidou Apostolos Traganitis
Further Information:	The registration fee is expected to be about $200. For further information please visit the workshop website at http://www.cs.purdue.edu/homes/spa/itw99.html or contact either of the Co-Chairs:

Prof. Leonidas Georgiadis
Aristotle University of Thessaloniki
Dept. of Electrical and Computer Eng.
Thessaloniki, 54006, GREECE
E-mail: leonid@eng.auth.gr
Fax: +(30 31) 996312

Prof. Wojciech Szpankowski
Dept. of Computer Science
Purdue University
W. Lafayette, In 47907, USA
E-mail: spa@cs.purdue.edu
Fax: (765) 494 0739

CALL FOR PAPERS

The 2000 IEEE International Symposium on Information Theory will be held at the Conference Center of the Sorrento Palace Hotel, Sorrento, Italy, from Sunday, June 25, through Friday, June 30, 2000.

Papers presenting contributions to the following areas are solicited:

- Coded modulation
- Coding theory and practice
- Communication complexity
- Communication systems
- Cryptology
- Data compression
- Data networks
- Detection and estimation
- History of information theory
- Multiuser detection
- Multiuser information theory
- Pattern recognition and learning
- Quantum information processing
- Shannon theory
- Signal processing
- Source coding

Papers will be reviewed on the basis of an extended summary of sufficient detail to permit reasonable evaluation. The deadline for submission is September 15, 1999, with notification of decision by February 1, 2000. In view of the large number of submissions expected, multiple submissions by the same author will receive especially stringent scrutiny. Abstracts of the papers presented at the Symposium will appear in the Proceedings. **Four copies** of extended summaries should be mailed to the program co-chair:

Professor Thomas Ericson
Linköpings Universitet
ISY, Datatransmission
SE-581 83 Linköping (Sweden)

It is expected that a small number of grants for the partial reimbursement of travel costs may be available for the authors of accepted papers whose resources would not otherwise enable them to attend the Symposium. Detailed information on the technical program, special events, accommodations, travel arrangements, excursions and applications for travel grants will be posted to the Symposium Web site:

http://www.unisa.it/isit2000

Inquiries on general matters related to the Symposium should be addressed to either of the Co-Chairs:

Professor Ezio Biglieri
Dipartimento di Elettronica
Politecnico di Torino
Corso Duca Degli Abruzzi, 24
I-10129, Torino, Italy
e.mail: biglieri@polito.it
Phone: +39 011 5644030
Fax: +39 011 5644099

Professor Sergio Verdú
Department of Electrical Engineering
Princeton University
Princeton, NJ 08544
USA
e-mail: verdu@princeton.edu
Phone: +1 (609) 258-5315
Fax: +1 (609) 258-3745

CALL FOR PAPERS

5th International Symposium on Communication Theory and Applications, ISCTA '99

Charlotte Mason College,
Ambleside, Lake District, UK,
11-16 July 1999

Organizing Committee

Prof L W Barclay,
Lancaster University, UK

Prof M Darnell,
University of Leeds, UK

Prof P G Farrell,
Lancaster University, UK

Prof B Honary,
Lancaster University, UK

Prof J Lindner,
University of Ulm, Germany

Dr G Markarian,
NDS Ltd, UK

Mr M Maundrell,
DERA Malvern, UK

Prof McEliece,
Caltech, USA

Prof S Wicker,
Cornell University,
New York, USA

Sponsored by IEEE Communications and Information Theory Chapters (UKRI Sections), IEE & H W Communications Limited

The Fifth International Symposium on "Communication Theory & Applications" will be held at the Charlotte Mason College from 11 - 16 July 1999. A major objective of the Symposium will be to pursue the progression from communication and information theory through to the implementation, evaluation and performance of practical communication systems of various types.

Papers are invited in the following areas:

Error Control
Modulation, Demod. and Syncrhoniz.
Data Compression
Cryptography and Security
Communication and Information Theory
Channel Characterization & Modeling
DSP Algorithms & Applications
Communication System Architectures
Networking and Protocols
Multi-Media Techniques
Image and Speech Processing
Simulation and Modeling
Complexity Considerations
Multi-Access Techniques
Spread-Spectrum Techniques
Multi-Functional Coding

Papers will be reviewed on the basis of extended abstracts of about 1000 words with a copy of the full text brought to the Symposium for later publication.The working language for the Symposium will be English.

Three copies of the abstracts together with the attached author information sheet should be sent to the following address:

Prof. P G Farrell
Communications Research Centre
Faculty of Applied Sciences
Lancaster University
LANCASTER LA1 4YR UK
Tel: 44 1524 593427 / 594141
Fax: 44 1524 594207
Email: p.g.farrell@lancaster.ac.uk

Deadlines:

Extended Abstract 8 February 1999
Notification of Acceptance 5 April 1999

Costs

The Symposium will be fully residential with full-board deluxe accommodation being available. Please contact the conference organizers regarding accommodations and expenses.

Workshop Report

1998 IEEE Information Theory Workshop, Ireland

The IEEE Information Theory Workshop was held at the Great Southern Hotel in Killarney, Ireland, from June 22-26, 1998. This coincided with the formation of an Information Theory Chapter of the IT Society in Ireland and the United Kingdom. The workshop co-Chairs were Prof. Seán Coffey and Dr. Pat Fitzpatrick, and the Technical Chair was Dr. Liam Marnane. The workshop was sponsored by the IEEE Information Theory Society, with generous support from the U.S. National Science Foundation, the Irish Industrial Development Authority, the National Microelectronics Centre, and Massana, Inc. The technical program featured the following sessions:

Coded Modulation — Chris Heegard, Cornell

Source Coding — Dave Neuhoff, Univ. of Michigan, and Frans Willems, Eindhoven Univ. of Technology

Algebraic Geometry Codes — Tom Hoholdt, Technical U. of Denmark

Coding Theory — Pascale Charpin, INRIA, Rocquencourt

Shannon Theory — Sergio Verdú, Princeton, and Shlomo Shamai, The Technion

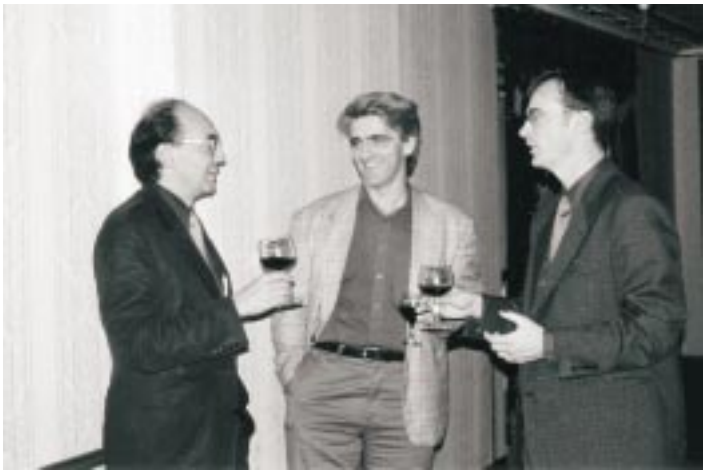
Decoding — Paddy Farrell, Lancaster Univ.

Networks — Tony Ephremides, Univ. of Maryland

Cryptography — Jim Massey, ETH Zurich

Contributed Sessions — Pat Fitzpatrick, Univ. College Cork, and Seán Coffey, Univ. of Michigan

(A full list of the papers and contributors can be found at http://www.eecs.umich.edu/systems/itw98/programme.html.) An IT Society Board of Governors meeting was held on June 22.



Sergio Verdú, Pat Fitzpatrik, and Seán Coffey

The beautiful surroundings of Killarney have long drawn visitors to the area, and the venue hotel was constructed in the 1850's for the aristocratic visitors of the time. This ambiance was enjoyed by 126 participants from 18 countries, as well as 36 participants in the companions program.

The proceedings (ISBN 0-7803-4408-1, 162 pages; IEEE Catalog No. 98-EX131) can be obtained by contacting Prof. Seán Coffey at scoffey@eecs.umich.edu.

Celebration of the 50th Anniversary of Information Theory in Siberia

To commemorate the 50th anniversary of Information Theory a special symposium on the subject was organized within the framework of the Congress on Applied and Industrial Mathematics which was held in Novosibirsk Scientific Center, Russia, in June 22-27, 1998. The congress was sponsored by the Russian Foundation for Basic Research.

The technical program of the symposium included a Congress plenary talk titled "50 years of Information Theory'' by Rudolf Ahlswede, University of Bielefeld , Germany. Other highlights included two symposium plenary talks: "Universal coding via games'' by Flemming Topsoe, University of Copenhagen, Denmark and "Fast and efficient method of constructing an unbiased random sequence'' by Boris Ryabko and Elena Matchikina, Siberian State Univ. of Telecom. and Inform. Sciences (SibSUTIS), Russia. The symposium also included a variety of session talks.

IT Symposium chairman	Boris Ryabko
IT Symposium secretary	Andrei Fionov

Workshop Report

Current Trends in Applications of Information Theory Celebrating the 50th anniversary of Information Theory

Institute of Communication and Computer Systems
National Technical University of Athens, Athens, Greece

On June 30, 1998, the ICCS organized a small celebration for the 50th anniversary of information theory. Invited speakers included: Professor James Massey (ETH), whose presentation was titled "Shannon's Legacy"; Professor Oscar Moreno (UPR), who gave a talk titled "Electronic Signature in the European Union," and Mr. David Herson (director of INFOSEC / DGXIII) who spoke on "Stream Ciphers, Exponential Sums, CDMA Sequences, Expander Graphs." The event also included an introductory technical talk presented by Professor Afrati (NTUA) and Dr. Polemi (ICCS-NTUA) and a variety of contributed talks on applications and implementations of coding theory, cryptology, the interaction between these fields and their impact on security.

Workshop Report

Codes and Trees: Algorithmic and Information Theoretic Approaches

October 5-7, 1998
DIMACS, Rutgers University Piscataway, NJ

Julia Abrahams
Center for Discrete Mathematics and Theoretical Computer Science (DIMACS)
Rutgers University, Piscataway, NJ
abrahams@dimacs.rutgers.edu

The Workshop on Codes and Trees: Algorithmic and Information Theoretic Approaches was held at the Center for Discrete Mathematics and Theoretical Computer Science (DIMACS), sponsored by DIMACS as part of its Special Year on Massive Data Sets, with technical cosponsorship from the IEEE Information Theory Society. It was organized by Julia Abrahams, DIMACS, and Mordecai Golin, Hong Kong University of Science and Technology and currently a DIMACS visitor. The workshop had the aim of making connections between distinct research communities interested in code tree problems of which Huffman coding is the prototype. It was successful in bringing together groups representing the information theory, computer science algorithms, and formal languages communities, thereby promoting research linkages among people and perspectives which are typically disjoint. Approximately 60 participants attended the three day workshop.

Although Huffman coding is a very classical problem, interest in the area continues prompted by its central role in data compression. In recent years, as the need to store and retrieve massive amounts of data increases, compression has become a key technology. In addition, many other problems in diagnostic testing, database search, and circuit design are isomorphic to the Huffman optimization problem and its variants. Furthermore, new developments in optimization theory provide techniques for the resolution of long-standing open questions in the design of optimal coding algorithms.

The program included tutorials by Julia Abrahams, DIMACS, Wolf Bein, University of Nevada, and Veronique Bruyere, University of Mons-Hainaut Le Pentagone, Belgium in addition to a variety of contributed and invited talks. Abstracts are posted at the workshop web site at

http://dimacs.rutgers.edu/Workshops/Codes/index.html.

Ahlswede Fest-Symposium

A symposium on Numbers, Information and Complexity in honor of Rudolph Ahlswede on the occasion of his 60th birthday was held in Bielefeld, October 8-11. The symposium was attended by about 150 participants. More than 80 papers were presented. A "festschrift'' including all contributions is planned to be published during next year.

Among the non-scientific contributions was a retrospective address presented by Gunter Dueck: "One decade next door to R. Ahlswede.'' He gave many interesting views on the background of several of the by now famous joint papers by himself and Ahlswede. Also very much appreciated was a new poem written and recited by Jim Massey in honor of Rudolph Ahlswede. The poem is published in this Newsletter, with the permission of both Jim and Rudi.

Rudi at the Board

It looked extremely gloomy on that Oberwolfach day.
The week had gone by merrily in mathematic' play,
But at the end it had become a serious kind of game
And forty-three participants now wallowed in deep shame.

For on that morn someone did write an Erdös problem down
And challenged the assembled guests, before they left the town,
To give a full solution of the comb'natorial kind
To this problem truly worthy of the keenest human mind.

At first it went quite quickly as those eager brains sped on.
No one could quite believe it—but with just one hour gone
There were just three links missing for the task to be complete,
Two lemmas and one theor'm to prove and they had done the feat.

But there all progress halted and the weak began to fret
That a greater mind was needed now than any they'd seen yet.
With barely thirty minutes left on Oberwolfach's clock,
Two lemmas and that theor'm remain'd and seemed the guests to mock.

A doubting pair got up to go, leaving there the rest
With that hope which springs eternal within the human breast.
For they thought, "If only Rudi would the clock a chance accord,''
They'd put up even money now with Rudi at the board.

But Imre's turn would be the next and after him, Levon
And the former was a slowpoke and the latter, never done.
So on that stricken multitude despair like raindrops poured,
For there seemed but little chance of Rudi's getting to the board.

But Imre proved one lemma in just ten minutes flat
And Levon got the other one in scarcely half of that.
And when the chalk dust settled to reveal what had occurred,
They saw that of those three hard proofs was left now just the third.

Then from that gladdened multitude there rose a joyous cheer.
It rattled all the windows and upset somebody's beer.
It echoed from the cabinet where the Mosel wine is stored,
For Rudi, mighty Rudi, was advancing to the board.

There was ease in Rudi's manner as he stepped up toward his place.
There was pride in Rudi's bearing and a smile on Rudi's face.
And when, distracted by the noise, he tripped upon some cord,
No stranger in the room could doubt 'twas Rudi at the board.

Eighty eyes were on him as he reached down for the chalk.
Forty tongues applauded as he then began to talk.
But when the first five minutes had gone by just like the wind,
Rudi's skilled maneuver reached an irreparable dead end.

ôStop him, stop that faker!" said a kid from Maryland.
And truly they'd have lynched that lad save Rudi raised his hand.
With a smile of Christian charity great Rudi's visage beamed.
He turned back to his daunting task with tricks no one had dreamed.

As on and on he sallied forth at supernatural pace
'Twas clear to all no mortal man could take this Rudi's place.
Up toward a beck'ning heaven, great Rudi's thoughts now soared
And even gods cast envied looks on Rudi at the board.

Once more across that blackboard did his nimble fingers fly.
And soon the wall was full of tau's, some beta's and one pi.
It seemed as if he had it, but just then the hushed crowd knew
That Rudi's new approach had led to dead end number two.

"Fraud!" cried out that same young man and an echo answered
"Fraud!" But one scornful look from Rudi and that nasty boy was awed.
All saw his face grow stern and cold. They felt his neurons strain,
And they knew that Rudi would not make the same mistake again

The smile is gone from Rudi's lips, his teeth are clenched with hate.
He swipes with cruel vengeance his chalk across the slate.
The delta's and the epsilon's now come with dazzling speed,
With here and there a hieroglyph when Rudi feels the need.

"And now it's done," he cries at last, "As you can plainly see.
The theorem's proved, for I have shown that A is less than B."
And as he writes his "Q.E.D." the clock begins to chime
To tell the gasping audience that it's adjournment time.

Oh somewhere in this land of Gauss and Dedekind and Weyl,
Math'matics cheers the hearts of men and makes small children smile.
But joy in Oberwolfach there was none to find that day,
For Rudi's inequality was pointing the wrong way!

James Lee Massey
9 October 1998

Dedicated to an even greater "Rudi" on the occasion of his 60th birthday (and with apologies to Ernest Lawrence Thayer for the plagiarism of his poem, "Casey at the Bat," written some hundred years ago.)

New Books

Raymond Yeung

Basic Methods of Cryptography,
by Jan C. A. van der Lubbe. Cambridge University Press, 1998, 243 pp., £19.95, ISBN 0-521-55559-0 (paperback).
Contents: Introduction to cryptography; Classical cipher systems; The information theoretical approach; The data encryption standard; Shift-registers; Public cipher systems; Authentication and integrity; Key management and network security.

Information Measures for Discrete Random Fields,
by Zhongxing Ye and Toby Berger. Science Press, 1998, 160 pp., ISBN 7-03-006592-1 (Beijing), 1-880132-29-X (New York).

Contents: Information measures of random variables and vectors; Information measures of random processes; Entropic aspects of random fields on trees; Entropy theorem for random fields on trees; Entropic aspects of random fields on $cal Z^d; $epsilon-Entropy and critical distortion of random fields on lattices.

Multiuser Detection,
by Sergio Verdú. Cambridge University Press, 1998, 464 pp., £30, ISBN 0-521-59373-5.
Contents: Multiaccess communications; Code division multiple access channels; Single-user matched filter; Optimum multiuser detection; Decorrelating detector; Non-decorrelating linear multiuser detection; Decision-driven multiuser detectors.

Graphical Models for Machine Learning and Digital Communication,
by Brendan J. Frey. Bradford Book, 1998, 216 pp., $32, ISBN 0-262-06202-X.
Contents: Introduction; Probabilistic inference in graphical models; Pattern classification; Unsupervised learning; Data compression; Channel coding; Future research directions.

Digital Transmission Engineering,
by John B. Anderson. IEEE Press, 1998, 400 pp., $98.95 (List Price), $77 (Member Price), ISBN 0-7803-3457-4.
Contents: Introduction to digital transmission; Baseband pulse transmission; Carrier transmission; Synchronization; Channels; Error correction coding; Receivers for distributed channels; Appendix A — Least square error equalizers.

Fundamentals of Convolutional Codes,
by Rolf Johannesson and Kamil Sh. Zigangirov. IEEE Press, 1998, 600 pp., $89.95 (List Price), $77 (Member Price), ISBN 0-7803-3483-3.
Contents: Introduction; Convolutional encoders — Structural properties; Distance properties of convolutional codes; Viterbi decoding; List decoding; Sequential decoding; Iterative decoding; Convolutional codes with good distance properties; Modulation codes; Appendix A: Minimal encoders; Appendix B: Wald's Identity.

Trellis and Trellis-Based Decoding Algorithms for Linear Block Codes,
by Shu Lin, Tadao Kasami, Toru Fujiwara and Marc Fossorier. Kluwer, 1998, 304 pp., $86.50, ISBN 0-7923-8151-3.
Contents: Introduction; Linear block codes; Trellis representation of linear block codes; state labeling, Trellis construction procedures and trellis symmetry; Trellis complexity; Trellis sectionalization; Parallel decomposition and low-weight subtrellises; Methods for constructing codes and trellises.

Coding for Channels with Feedback,
by James M. Ooi. Kluwer, 1998, 200 pp., £ 66.50, ISBN 0-7923-8207-2.
Contents: Introduction; DMCs: An introduction to the framework; Channels with memory; Unknown channels; Multiple-access channels; Channels with partial and noisy feedback; Conclusions.

Asymptotic Combinatorial Coding Theory,
by Volodia Blinovsky. Kluwer, 1997, 128 pp., $89, ISBN 0-7923-9988-9.
Contents: Coding bounds; List decoding; Covering and packing; Decoding complexity; Channel with defects; Some other problems.

Lectures on the Theory of Stochastic Processes,
by A. V. Skorokhod. VSP, 1996, 184 pp., $59, ISBN 90-6764-206-1.
Contents: Stochastic processes, Definitions, Examples; The Kolmogorov consistency theorem, Classification of processes; Random Walks, Recurrence, Renewal theorem; Martingales, Inequalities for martingales; Theorems on the limit of a martingale; Stationary sequences, Ergodic theorem; Ergodic theorem, Metric transitivity; Regularization of a process, Continuity; Processes without discontinuities of the second kind; Continuity of processes with independent increments, Martingales with continuous time; Measurable processes; Stopping times, Associated s-algebras; Completely measurable processes; L_2-theory; Stochastic integrals; Stationary processes, Spectral representations; Stationary sequences, Regularity and singularity, The prediction of a stationary sequence, Markov processes, Homogeneous Markov processes and associated semigroups; Homogeneous purely discontinuous processes, Conditions for their regularity; Processes with a denumerable set of states; Simple birth and death processes; Branching processes with particles of only one kind; Homogeneous processes and strongly continuous semigroups, Resolvent operator and generator; The Hille-Iosida theorem; Processes with independent increments, Representation of the discontinuous part; General representation of a stochastically continuous process with independent increments; Diffusion processes; Stochastic integrals; Existence, uniqueness, and properties of solutions of stochastic differential equations; Itô's formula with some corollaries.

Digital Signal Processing: A Computer-Based Approach,
by Sanjit K. Mitra. MaGraw-Hill, 1998, 672 pp., ISBN 0-07-042953-7.
Contents: Signals and signal processing; Time-domain representation of signals and systems; Transform-domain representation of discrete-time sequences; Transform-domain representation of LTI systems; Digital processing of continuous-time signals; Digital filter struc-

ture; Digital filter design; DSP algorithm implementation considerations; Analysis of finite word-length effects; Multi-rate digital signal processing; Applications of digital signal processing.

Communication Networks, 2nd Ed.,
by Jean Walrand. MaGraw-Hill, 1998, 512 pp., ISBN 0-256-17404-0.
Contents: Introduction; Operating and design principles; Computers, switches, networks, applications; Physical layer; Data link layer and error control; Local area networks; Network layer; Transport and connections; ATM and SONET; Performance evaluation.

Hands-On Digital Signal Processing,
by Fred Taylor and the Athena Group, Inc. MaGraw-Hill, 1998, 650 pp., ISBN i0-07-912965-X.

Advances in Matrix-Analytic Methods for Stochastic Methods,
Edited by Attahiru S. Alfa and Srinivas R. Chakravarthy. Notable Publications, Inc., 1998, 444 pp., $95, ISBN 0-9665-8470-8.

CDMA Systems Engineering Handbook,
by Jhong Sam Lee and Leonard E. Miller. Artech House, 1998, 1200 pp., $142, ISBN 0-89006-990-5.

Wideband CDMA for Third Generation Mobile Communications,
by Tero Ojanperä and Ramjee Prasad. Artech House, 1998, 452 pp., $102, ISBN 0-89006-735-X.

Personal Wireless Communication with DECT and PWT,
by John A. Phillips and Gerard Mac Namee. Artech House, 1998, 376 pp., $95, ISBN 0-89006-872-0.

Mobile Telecommunications: Standards, Regulations and Applications,
by Rudi Bekkers and Jan Smits. Artech House, 1998, 420 pp., $114, ISBN 0-89006-806-2.

Advances in Mobile Information Systems,
Edited by John Walker. Artech House, 1998, 400 pp., $102, ISBN 0-89006-951-4.

Introduction to Telecommunication Network Engineering,
by Tarmo Anttalainen. Artech House, 1998, 376 pp., $78, ISBN 0-89006-984-0.

Guide to ATM Systems and Technology,
by Mohammad A. Rahman. Artech House, 1998, 404 pp., $76, ISBN 0-89006-306-0.

Understanding Token Ring Protocols and Standards,
by James T. Carlo, Robert D. Love, Michael Siegel and Kenneth T. Wilson. Artech House, 1998, 450 pp., $107, ISBN 0-89006-458-X.

Desktop Encyclopedia of the Internet,
by Nathan J. Muller. Artech House, 1998, 600 pp., $78, ISBN 0-89006-729-5.

Regulation of Telecommunication Carriers,
by Evan T. Leo and Henk J. Brands. Artech House, 1998, 352 pp., $90, ISBN 0-89006-714-7.

Advances in Stochastic Models for Reliability, Quality and Safety,
by W. Kahle, E. V. Collain and J. Franz. Birkh\"auser, 1998, 400 pp., ISBN 3-7643-4049-5.

Broadband Wireless Communications,
by M. Luise and S. Pupolin. Springer-Verlag, 1998, 432 pp., ISBN 3-540-76237-X.

Chaos for Engineers: Theory, Applications, and Control,
by T. Kapitaniak. Springer-Verlag, 1998, 150 pp., ISBN 3-540-63515-7.

The Digital Signal Processing Handbook,
by Vijay K. Madisetti and Douglas B. Williams. CRC Press, 1997, $166, ISBN 0-8493-8572-5.

ATM Technology for Broadband Telecom Networks,
by A. S. Pandya and E. Sen. CRC Press, 1997, 416 pp., $89, ISBN 0-8493-3139-0.

Trellis Decoding of Block Codes,
by Bahram Honary and Garil Markarian. Kluwer, 1997, 288 pp., $88.50, ISBN 0-7923-9860-2.

Wavelet Image and Video Compression,
Edited by Pankaj N. Topiwala. Kluwer, 1998, 452 pp., £ 78.25, ISBN 0-7923-8182-3.

3-D Audio Using Loudspeakers,
by Wiliam G. Gardner. Kluwer, 1998, 168 pp., £ 66.50, ISBN 0-7923-8156-4.

Automated Highway Systems,
Edited by Petros A. Ioannou. Plenum, 1997, 376 pp., $79.95, ISBN 0-306-45469-6.

Multimedia Communications and Video Coding,
Edited by Yao Wang, Shivendra Panwar, Seung-Pil Kim and Henry L. Bertoni. Plenum, 1996, 580 pp., $135, ISBN 0-306-45367-3.

Wireless Applications of Spread Spectrum Systems: Selected Readings,
Edited by Sawasd Tantaratana and Kazi M. Ahmed. IEEE Press, 1998, 500 pp., $69.95 (List Price), $49.95 (Member Price), ISBN 0-7803-2340-8.

Engineering Networks for Synchronization, CCS7, and ISDN: Standards, Protocols, Planning, and Testing,
by P. K. Bhatnagar. IEEE Press, 1998, 528 pp., $89.95 (List Price), $77 (Member Price), ISBN 0-7803-1158-2.

Trellis Coding,
by Christian Schlegel. IEEE Press, 1998, 304 pp., $79.95 (List Price), $68 (Member Price), ISBN 0-7803-1052-7.

ATM Volume II: Signaling in Broadband Networks,
by Uyless Black. IEEE Press / Prentice Hall, 1998, 224 pp., $65 (List Price), $59 (Member Price), ISBN 0-7803-3488-4.

ATM Volume III: Interworking,
by Uyless Black. IEEE Press / Prentice Hall, 1998, 256 pp., $54 (List Price), $49 (Member Price), ISBN 0-7803-3489-2.

Development and Applications of ATM: Selected Readings,
Edited by Mehmet Toy. IEEE Press, 1997, 550 pp., $69.95 (List Price), $49.95 (Member Price), ISBN 0-7803-2310-6.

Direct Digital Frequency Synthesizers,
Edited by Venceslav F. Kroupa. IEEE Press, 1998, 384 pp., $69.95 (List Price), $59.95 (Member Price), ISBN 0-7803-3438-8.

Telecommunications Transmission Handbook, 4th Ed.,
by Roger Freeman. Wiley, 1998, 1204 pp., $175, ISBN 0-471-24018-4.

Radio System Design for Telecommunications,
by Roger L. Freeman. Wiley, 1997, 750 pp., $94.95, ISBN 0-471-16260-4.

CTI in Action,
by Rob Walters. Wiley, 1997, 346 pp., $59.90, ISBN 0-471-96824-2.

ISDN Explained: Worldwide Network and Applications Technology, 3rd Ed.,
by John Griffiths. Wiley, 1998, 528 pp., $74.95, ISBN 0-471-97905-8.

Elements of Network Protocol Design,
by Mohamad Gouda. Wiley, 1998, 424 pp., $74.95, ISBN 0-471-19744-0.

Signaling in Telecommunication Networks,
by John G. Van Boose. Wiley, 1998, 438 pp., $84.95, ISBN 0-471-57377-9.

Switching Theory: Architecture and Performance in Broadband ATM Networks,
by Achille Pattavina. Wiley, 1998, 400 pp., $120, ISBN 0-471-96338-0.

Tracking and Kalman Filtering Made Easy,
by Eli Brookner. Wiley, 1998, 504 pp., $74.95, ISBN 0-471-18407-1.

Introductory Digital Signal Processing with Computer Applications, 2nd Ed.,
by Paul A. Lynn and Wolfgang Fuerst. Wiley, 1998, 416 pp., $54.95, ISBN 0-471-97631-8.

Digital Communication Receivers: Synchronization, Channel Estimation, and Signal Processing, Volume 2,
by Heinrich Meyr, Marc Moeneclaey and Stefan Fechtel. Wiley, 1998, 864 pp., $84.95, ISBN 0-471-50275-8.

Dictionary of Communications Technology: Terms, Definitions and Abbreviations,
3rd Ed., by Gilbert Held. Wiley, 1998, 720 pp., $69.95, ISBN 0-471-97517-6 (paperback).

Solutions to Golomb's Puzzle Column™ Number 43:
Questions About Numbers

Solomon W. Golomb

1. (a) There are six values of n^2 modulo 10, namely 0, 1, 4, 5, 6, 9.

(b) There are 22 values of n^2 modulo 100, namely 00, 25, *E*1, *E*4, ∅6, *E*9, where *E* indicates the five *even* digits 0, 2, 4, 6, 8, and ∅ indicates the five *odd* digits 1, 3, 5, 7, 9.

Everything that occurs as n^2 modulo 100 for all integers n already occurs with $0 \le n \le 25$, because $(25 + a)^2 = (25 - a)^2 + 100a$, *i.e.*, $(25 + a)^2 \equiv (25 - a)^2 \pmod{100}$, limiting the distinct values of n^2 modulo 100 to at most 26 values. However, $5^2 \equiv 15^2 \equiv 25^2 \pmod{100}$ and $0^2 \equiv 10^2 \equiv 20^2 \pmod{100}$, whence there are only 22 distinct values.

For the cases where $n^2 \equiv 1 \pmod{10}$, we have $n \equiv \pm 1 \pmod{10}$, so $n = 10a \pm 1$, $n^2 \equiv 100a^2 \pm 20a + 1 \equiv \pm 20a + 1 \pmod{100}$, so the *tens* digit must be *even*.

For the cases where $n^2 \equiv 4 \pmod{10}$, we have $n \equiv \pm 2 \pmod{10}$, so $n = 10a \pm 2$, $n^2 \equiv 100a^2 \pm 40a + 4 \equiv \pm 40a + 4 \pmod{100}$, so the *tens* digit must be *even*.

For the cases where $n^2 \equiv 9 \pmod{10}$, we have $n \equiv \pm 3 \pmod{10}$, so $n = 10a \pm 3$, $n^2 \equiv 100a^2 \pm 60a + 9 \equiv \pm 60a + 9 \pmod{100}$, so the *tens* digit must be *even*.

For the cases where $n^2 \equiv 6 \pmod{10}$, we have $n \equiv \pm 4 \pmod{10}$, so $n = 10a \pm 4$, $n^2 = 100a^2 \pm 80a + 16 \equiv \pm 80a + 16 \pmod{100}$, so the *tens* digit must be *odd*.

(c) There are 159 values of n^2 modulo 1000. If $n^2 \equiv 0 \pmod{10}$, the six possibilities are $n^2 \equiv 000$, 100, 400, 500, 600, or 900 modulo 1000. If $n^2 \equiv 5 \pmod{10}$, the three possibilities are $n^2 \equiv 025$, 225, or 625 modulo 1000. If $n^2 \equiv 1 \pmod$

10), the 25 possibilities are $n^2 \equiv E01, \emptyset21, E41, \emptyset61$, or $E81$ modulo 1000. If $n^2 \equiv 4 \pmod{10}$, the 50 possibilities are $AE4$ modulo 1000, where A represents all ten possible digits, while as before E represents the five even digits. If $n^2 \equiv 6 \pmod{10}$, the 50 possibilities are $A\emptyset6$ modulo 1000. If $n^2 \equiv 9 \pmod{10}$, the 25 possibilities are $E09, \emptyset29, E49, \emptyset69, E89$ modulo 1000.

Thus, altogether, there are 6 + 3 + 25 + 50 + 50 + 25 = 159 distinct values of n^2 modulo 1000. All of these values will appear with $0 < n < 250$.

2. We are given two sets of index cards, each containing n cards, and each set bearing the numbers from 1 to $2n$, one number on each side of each of the n cards in the set, but in no particular order. It is always possible to place all $2n$ cards on a table in such a way that the visible sides are the numbers from 1 to $2n$, each occurring once. Here is a simple algorithm to achieve this.

   Find the number "1" on a card from the first set, and place this facing upward. Let the flip side of this card contain the number a_1. Find this number on a card from the second set, and place it face up. Let the flip side of this card showing a_1 bear the number a_2. If $a_2 = 1$, we have completed a "cycle" of two cards. Otherwise, find a_2 On a card from the first set, place this card with a_2 facing upward, and let the flip side of this card be a_3. (Note that a_3 cannot be any of 1, a_1, or a_2.) Find a_3 on a card of the second set, place this card with a^3 facing upward, and let the underside of this card show a_4. If $a_4 = 1$, we have completed a "cycle" of four cards. Otherwise proceed as before, and continue until the flip side of a card from the second set bears the number "1", thus completing a cycle of $2k$ cards. If $k = n$, our task is completed. Otherwise, select the card from the first set bearing the lowest remaining number, say b_1, and place this face up. If the flip side shows b_2, find this on a card in the second set and proceed as before, until a second cycle is completed. If any cards remain, start a third cycle using the lowest number still remaining on any card from the first set. Continue until all cards have been used up.

   Note that this procedure always generates a permutation of the numbers from 1 to $2n$ consisting entirely of even-length cycles.

3. The only Pythagorean triple (a, b, c), i.e. positive integers with $a^2 + b^2 = c^2$, such that two of (a, b, c) are prime and the third is twice a prime is (3, 4, 5), or the equivalent (4, 3, 5). To show this, we use Euler's elementary result that every Pythagorean triple (a, b, c) can be written parametrically in terms of two unequal positive integers u and v with $a = 2uv$, $b = u^2 - b^2$, $C = u^2 + v^2$ (or, with the roles of a and b reversed). Note that no member of a Pythagorean triple can equal 2. Hence a = 2uv must be "twice a prime", so one of u, v is a prime and the other equals 1, and since $u > v$, $b = u^2 - 1$ and $u^2 + 1$ must both be prime. But then $b = (u + 1)(u - 1)$ is prime, requiring u – 1 = 1, or u = 2. Then b = (2 + 1) (2 – 1) = 3 and c = u^2+ 1 = 5, while $a = 2u = 4$, as asserted.

4. We want to show that for any positive integer n, with $8n = m$, the sum of all the digits of 8, n, and m, with the digits of the sum re-summed repeatedly until only a single digit remains, is always '8'.

   This is an example of "casting out 9's", or more mathematically, reduction modulo 9. That is, we want to reduce $8 + n + m$, modulo 9. We see that $8 + n + m = 8 + n + 8n = 8 + 9n \equiv 8 \pmod{9}$.

   The proof is trivial, but the result is surprising enough to most people that it makes a nice parlor trick. (You prove your ESP powers by writing the answer, '8', on a piece of paper before knowing which integer n your victim has selected, or even before the number "n" has been selected, depending on whether your want to demonstrate your powers of telepathy or precognition!)

Symposium Report . . .

continued from page 8

tion A' (Leech and Sloane, 1969). If C is a binary code of length n, the corresponding packing is $P(C) = \{x \in \mathbb{Z}^n : x \pmod 2 \in C\}$.

Consider the vectors $abcde \in (\mathbb{Z}/4\mathbb{Z})^5$ where $b, c, d \in \{+1, -1\}$, $a = c - d$, $e = b + c$, together with all their cyclic shifts, and apply the 'Gray map' $0 \to 00$, $1 \to 01$, $2 \to 11$, $3 \to 10$ to obtain a binary code C_{10} containing 40 vectors of length 10 and minimal distance 4. This is our description of a code first discovered by Best. Then $P(C_{10}) = P_{10c}$, is the record 10-dimensional packing.

Higher Dimensions

Figure 2 shows the density of the best packings known up to dimension 48, rescaled to make them easier to read. The vertical axis gives $\log_2 \delta + n(24-n)/96$, where the center density δ is the density Δ divided by the volume of a unit sphere. Lattice packings are indicated by small circles, nonlattices by crosses (however, the locations of the lattices are only approximate). The figure is dominated by the two arcs of the graph of the laminated lattices Λ_n, which touch the zero ordinate at n = 0, 24 (the Leech lattice) and 48. K_{12} is the

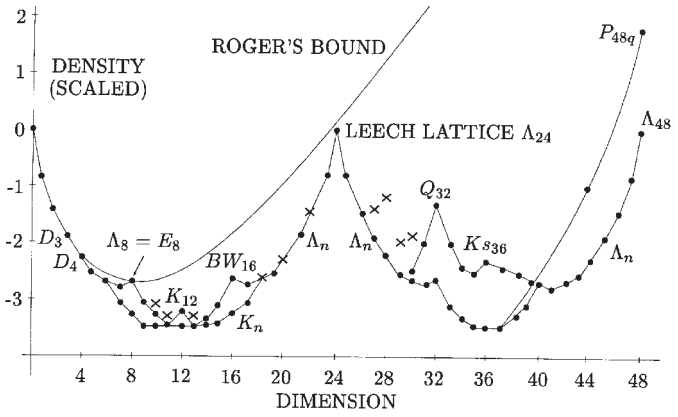


Figure 2: Densest sphere packings known in dimensions n ≤ 48.

Coxeter-Todd lattice, Q_{32} is Quebbemann's lattice, and P_{48q} is an extremal unimodular lattice constructed from a self-dual code of length 48 over $GF(3)$.

That's about the first half of the talk. But I've run out of space. For descriptions of the beautiful packings in Fig. 2, and much more, see the Introduction[4] to the Third Edition of my book with John Conway "Sphere Packings, Lattices and Groups".

[4] Available from my home page www.research.att.com/~njas/

Plenary Lecture . . .

continued from page 10

ing the overall error probability, and here again the likelihood ratio is the key statistic to compute. This was perhaps first recognized by V.A. Kotel'nikov (in the USSR) in a remarkable doctoral dissertation submitted in 1947, The *Theory of Optimum Noise Immunity* (translated into English and published by McGraw-Hill in 1960). [Kotel'nikov's 90th birthday was celebrated in Moscow on Sept. 6 and also acknowledged at the IT Symposium.] The thesis treats binary and multiple signal detection in additive white Gaussian noise, and also parameter estimation problems in digital and analog communication systems; many of the results in it were only rediscovered several years later. In particular, Kotel'nikov used geometrical arguments and interpretations very effectively. Among these one finds the nice geometric interpretation of the threshold effect in bandwidth-expanding modulation schemes such as FM, which was made famous in Shannon's 1949 paper and further elaborated in the classic textbook of Wozencraft and Jacobs. In Kotel'nikov's words: "However, when the length of the curve is increased, the distance between separate "twists" or sections of the curve must decrease, which perforce increases the probability of anomalous errors."

Though Kotel'nikov was very close to the notion of channel capacity for the wideband AWGN channel, he missed it, because (as he mentioned in a conversation on the occasion of the First (and only) Joint IEEE-USSR Academy of Sciences Symposium on Information Theory in Moscow, Dec. 1975), he never even dreamt of the possibility that one could have communication at a nonzero rate with arbitrarily small probability of error. The point is that Kotel'nikov often used the simple "union bound" on the error probability for M equal energy orthogonal signals in white Gaussian noise (in a standard notation, $Pe \le M \exp -(P_{av}/2N_0)T$) and used it to study the advantages of multiple versus binary signaling. It was Shannon's great insight that by allowing M to increase with time, and by using a logarithmic measure of signaling rate,

$$M = e^{RT}, R = (\ln M)/T$$

one could make P_e go to zero as $T \to \infty$, provided that R was not too high:

$$\begin{aligned} P_e &\le M \exp -(P_{av}/2N_0)T \\ &= \exp -[R - (P_{av}/2N_0)]T \\ &\to 0 \text{ for all } R < P_{av}/2N_0 \end{aligned}$$

In fact, of course, the actual capacity of the wideband $AWGN$ channel is higher, $C = P_{av}/N_0$, as was simply demonstrated in the lecture using a result on the asymptotic estimate of the maximum of M i.i.d. normal random variables as $M \to \infty$.

Briefly, the point is that the matched filter output corresponding to the actual transmitted signal is a $N(P_{av}, \sqrt{P_{av} N_o / 2T})$ random variable, while the outputs of the $M-1$ other matched filters are $N(0, \sqrt{P_{av} N_o / 2T})$. It might seem that for large T we will rarely make a mistake, no matter how large M is. However while the "incorrect" matched filter outputs are all very close to zero for large T, their *maximum* value tends, not to zero, but to $\sqrt{P_{av} N_o / 2T} \bullet \sqrt{2 \ln M} = \sqrt{P_{av} N_o R}$. Hence there will certainly be an error unless $\sqrt{P_{av} N_o R} < P_{av}$, i.e., unless $R < P_{av} / N_o = \lim_{W \to \infty} W \log(1 + \frac{P_{av}}{N_o W})$, the capacity of the wideband channel! This pretty argument was shown to me by Jack Stiffler at JPL in 1962. It provides a fine illustration of Shannon's fundamental observation that "Delay has the (additional) function of allowing a large sample of noise to affect the signal before any judgment is made at the receiving point as to the original message. Increasing the sample size always sharpens the possible statistical assertions." (Shannon, 1948, Sec. 19).

The Structure of Likelihood Ratios

Interest in likelihood ratios is again increasing in the information theory community, in part because of the importance of soft decoding in the new turbocodes. A long survey paper in the special Oct. 98 issue of the IT Transactions (with Vince Poor) gives a detailed account of this topic. So, as in the talk, here we even more briefly outline the main message.

Given complete statistical information and adequate computational resources one can always evaluate the L.R. as (in standard notation)

$$L.R. = \lim_{n \to \infty} \frac{w_1(y(t_0^{(n)}), \ldots, y(t_n^{(n)}))}{w_0(y(t_0^{(n)}), \ldots, y(t_n^{(n)}))}$$

However, as with all applications of mathematics to engineering problems, we need to understand enough of the structure of mathematical solution that we can make intelligent approximations when the solution is too complicated to actually evaluate or realistically implement, especially when we only have inaccurate or incomplete knowledge of the parameters in our model. The only recourse we have is to look for structure and insight in the exact (analytic) solutions to as many special cases as possible.

Chief among these is the L.R., first given by Kotel'nikov, for the problem of choosing between the hypotheses

$$H_1 : y(t) = m(t) + v(t) \text{ and } H_0 : y(t) = v(t), \qquad 0 \le t \le T$$

where $m(\cdot)$ is a completely known signal of energy E and $v(\cdot)$ is unit intensity white Gaussian noise (WGN):

$$L(T) = \exp\left[\int_0^T m(t) y(t)\, dt - \frac{1}{2}\int_0^T m^2(t) dt\right] \qquad (1)$$

The basic operation on the data is correlating the possible transmitted signal waveform $m(\cdot)$ against the received waveform $y(\cdot)$. As is well known, this correlation integral can also be computed as the output at time T of a filter *matched* to $m(\cdot)$ (i.e., with impulse response $m(T..)$) and driven by $y(\cdot)$. In other words, North's matched filter derived under a SNR criterion is in fact optimal in the stronger sense (of minimum probability of error).

Exact but more complicated L.R. formulas can be found when the signal is known except say for phase or for phase and amplitude. A very widely studied case is that of Gaussian signals. Here the usual hypotheses are:

$$H_1 : y(t) = z(t) + v(t),\ H_0 : y(t) = v(t)$$

where $v(\cdot)$ is again zero-mean unit-intensity WGN and $z(\cdot)$ is a zero-mean Gaussian random process independent of $v(\cdot)$ and having a continuous covariance function, $K(t,s)$. Then Price (IT, 1956) showed that the L.R. could be calculated as

$$L(T) = (\text{F. Det.}) \cdot \exp \int_0^T \int_0^T y(t) H(t,s) y(s) dt\, ds \qquad (2)$$

where $H(.,.)$ is the solution to the integral equation

$$H(t,s) + \int_0^T H(t,\tau) K(\tau, s) dt = K(t,s), \quad 0 \le t, s \le T \le \infty$$

and F. Det. is the so-called Fredholm determinant, $\Pi_1^\infty (1 + \lambda_i)$, where $\{\lambda_i\}$ are the eigenvalues of $K(.,.)$ over [0,T] $\times$ [0, T].

This is quite an explicit formula, but it illustrates some of the issues we mentioned earlier. First of all, explicit solutions of the integral equation are only available for a very few known functions $K(.,.)$. Are there good approximate solutions for other $K(.,.)$? What can we do if we only have a rough idea of what $K(.,.)$ is? Or when $z(\cdot)$ is a stationary process and we only have a general idea of what its power spectral density function is? How do we compute the Fredholm determinant? And so on.

Being well aware of such issues, Price was very happy to find that under his assumptions, he could show the following: Denote the inner integral in (2) as

$$\int_0^T H(t,s) y(s) ds \stackrel{\triangle}{=} z_e(t).$$

Then for each t, it turns out that $z_e(t)$ is the least-squares estimate of $z(t)$ given *all* (past and future) the observations $y(t) = z(t) + v(t)$, $0 \le t \le T$. The double integral in (2) then becomes $\int y(t) z_e(t)\, dt$, which can be implemented by a filter matched to $z_e(\cdot)$. This is a nice tie-in to the known signal case — when $z(\cdot)$ is random and therefore unknown, we form the mean-square estimate $z_e(\cdot)$ and then proceed (almost) as in the known signal case. An immediate bonus of this interpretation is that it provides a reasonable answer to the previous questions — in the face of limited knowledge, we put in the best estimator we can produce. If for example all we know is that the power spectrum has roughly a certain shape and a certain bandwidth, a first cut at an estimating filter is one with a transfer function roughly the same shape and bandwidth. This may or may not sound reasonable to all readers, but suffice it to say that it was precisely intelligent approximations of this kind that were used in the now-famous

RAKE anti-multipath receiver (Price and Green (Proc. IEEE, 1958)), which is now again gaining attention in the wireless field.

A question is whether such interpretations are available for non-Gaussian signals. In fact they are, and actually in a form much closer to the original L.R. formula (1) for the known signal case. Before presenting this result, however, a further note on the much studied Gaussian case will be useful.

First of all it is important to allow for correlation between the signal and noise processes. For example, in feedback systems the present signal is a function of past observations. It turns out that Price's interpretation breaks down in this case — $z_e(\cdot)$ is no longer an estimate. Secondly, for greatest generality one should allow square-integrable covariance functions. In this case the Fredholm determinant may not exist and the formula (2) breaks down. The appropriate generalization was found by Shepp (Ann. Stat., 1966)

$$L(T) = (\text{F.C. Det.})\, \exp \int_0^T c \int_0^T y(t) H(t,s) y(s) dt\, ds \qquad (3)$$

Here, F.C. Det. = $\Pi_1^\infty (1+\lambda_i) e^{-\lambda_i}$, a so-called Fredholm-Carleman determinant. [The point is that in the general case, $\sum |\lambda_i|$ may diverge, making the usual Fredholm determinant infinite. However the Fredholm-Carleman determinant will exist whenever the L.R. is well defined (see Shepp (1966) or Kailath (IT, May 1970)).] As for the other term, the "c'' between the integrals is used to indicate something that most engineers have never had to face before — the fact that a "new'' kind of integral has to be used, in this case a so-called multiple Wiener stochastic integral. There is really no problem with this — either in theory (we just have to introduce the appropriate definitions) or in practice (the new integral can be (approximately) calculated using available hardware); the same comments apply to the so-called Ito stochastic integral mentioned below. For more on these issues at a tutorial level, see Kailath (IT, 1969, May 1970a).

Here we go on to the promised result for (Gaussian and) non-Gaussian $z(\cdot)$. Following some fundamental work by F.C. Schweppe (IT, 1965), by R.L. Stratonovich and his colleagues (e.g., Stratonovich and Sosulin (1964), and in the Stanford dissertation of T.E. Duncan (1967), the following general result was presented in Kailath (IT, 1969), with a rigorous proof using modern martingale theory in Kailath (IT, July 1970b).

Assume that the signal $z(\cdot)$ has finite energy, but is not necessarily Gaussian, while the noise $v(\cdot)$ is unit intensity white and Gaussian. Also that $z(\cdot)$ and $v(\cdot)$ may be dependent, as long as future $v(\cdot)$ are independent of past signal $z(\cdot)$ (as in feedback communications). Let $\hat{z}_1(t)$ = the causal least-squares estimate of $z(t)$ given past $y(\cdot)$, and assuming H_1 holds (i.e., $y(t) = z(t) + v(t)$). Then the L.R. has exactly the same form as for known signals in *WGN*:

$$L(T) = \exp \int_0^T \hat{z}(t) y(t) dt - \frac{1}{2} \int_0^T \hat{z}^2(t) dt \qquad (4)$$

where $\int(\cdot)$ denotes a so-called Ito stochastic integral. With this definition, (3) can be shown to be equivalent to all earlier explicit L.R. formulas, including (2) and (3). However the real point is that (3) gives a universal structure into which we can insert our best available causal signal estimate to obtain a reasonable approximation to the L.R. Such structural information is the most valuable information mathematical results can give about real world problems! A further indication that this is a basic result is that a similar estimator-correlator structure also holds for the apparently very different non-Gaussian detection problems using jump-process observations. e.g., choosing between Poisson processes with different random rates.

The basic idea underlying the proof is the following result:

Given a process $y(t) = z(t) + v(t)$, introduce the innovations process,

$$\begin{aligned} i(t) &= y(t) - \hat{y}(t|t-) = y(t) - \hat{z}(t) \\ &= \text{the new information in } y(\cdot) \text{ at time t} \end{aligned}$$

Perhaps not surprisingly, this process is white (i.e., its values at different times are *uncorrelated* with each other) but in fact it is also Gaussian, so that they are *independent* of each other.

Moreover $i(\cdot)$ has the same intensity as $v(\cdot)$. Therefore the original hypothesis

$$H_1: y(t) = z(t) + v(t), \qquad H_0: y(t) = v(t),$$

can be replaced by

$$H_1: y(t) = \hat{z}(t) + i(t), \qquad H_0: y(t) = i(t).$$

But $i(\cdot)$ is WGN, and $\hat{z}_1(\cdot)$ is *conditionally known, given past* $y(\cdot)$. Hence it is reasonable that $L(T)$ is the same as in the known signal case, thus leading up to the formula (4).

Of course this heuristic (but rigorizable) argument raises several questions, even before the issue of making it precise. For example (just to begin):

Why *least-squares* signal estimates rather than any others?

Why is $i(\cdot)$ Gaussian, though neither $y(\cdot)$ nor $\hat{z}(\cdot)$ need be?

Moreover, according to the traditional definition, in which a Gaussian process is completely defined by its mean and covariance function, the WGN processes $v(\cdot)$ and $i(\cdot)$ should be indistinguishable. But they are clearly not the same! In fact, $i(t) = y(t) - \hat{z}(t) = (z(t) - \hat{z}(t)) + v(t) = \tilde{z}(t) + v(t) \neq v(t)$. So how can we distinguish them?

To answer these, and several further related questions, we have to bring in some concepts not usually covered in first courses on random processes; in particular, the concepts of sigma fields of events, and of martingales with respect to increasing families of sigma fields. Here we shall assume knowledge of them in order to outline an answer to our last question:

how to distinguish the Gaussian processes $v(\cdot)$ and $\hat{z}(\cdot)$?

Given the processes $\{z(\cdot), v(\cdot)\}$, we introduce the increasing family of sigma fields generated by $y(\cdot) = z(\cdot) + v(\cdot)$, $\mathcal{F}_t = \sigma$

$\{y(\tau), \tau \le t\}$, $0 \le t \le T$, and also the larger family $\mathcal{B}_t = \sigma\{z(\tau), v(\tau), z \le t\}$. [The larger family corresponds to the state of knowledge of an omniscient observer, involved in setting up the original model!] Then we may note that, for s < t,

$$E[v(t) \mid \mathcal{B}_s] = 0 \quad \text{but} \quad E[v(t) \mid \mathcal{F}_s] \neq 0$$

while

$$E[i(t) \mid \mathcal{B}_s] \neq 0, \quad \text{but} \quad E[i(t) \mid \mathcal{F}_s] = 0.$$

So this may be one way in which the processes may be distinguished.

In more traditional language, one would introduce the integrated processes

$$V(t) = \int_0^t v(\tau)d\tau \text{ and } I(t) = \int_0^t i(\tau)d\tau$$

in which case the above statements are equivalent to

$$E[V(t) \mid \mathcal{B}_s] = V(s), E[V(t) \mid \mathcal{F}_s] \neq V(s)]$$

while

$$E[I(t) \mid \mathcal{F}_s] = I(s), E[I(t) \mid \mathcal{B}_s] \neq V(t).$$

In other words, even though $V(\cdot)$ and $I(\cdot)$ are both Gaussian with the same mean and covariance,they are different because $I(\cdot)$ is a *martingale* with respect to the family of sigma fields $\{\mathcal{F}_t\}$ generated by the observations, but is not a martingale with respect to the fields $\{\mathcal{B}_t\}$; the opposite is true for the process $V(\cdot)$. Many other beautiful results arise from martingale theory (as largely developed by French and Japanese probabilists beginning in the late 1960s) in establishing (4) and its generalizations (e.g., Kailath and Duttweiler, IT Nov. 73; Segall and Kailath, Ann. Prob., 1975), discussion of which we must forego here.

However, a final thought, especially appropriate as we celebrate the Golden Jubilee of Information **Theory**, is to recall the words of Ludwig Boltzmann: There is nothing so practical as a good theory.

Reflections . . .

continued from page 12

sonal fun. That he might be demonstrating something of importance seemed quite incidental to him. In fact, in those early days he seemed to take an enormous hidden amusement at all things going on around him in the external world — in his notoriety, in the silly pompous questions his interviewers sometimes asked him, in the fact that he didn't answer his mail, that he made scads of money without really working for it. Everything seemed to secretly amuse him. I can best describe the nature of his cleverness by noting that with a tiny shift in his mores he could have been the world's greatest, most ingenious con-man and its most charming scoundrel. As he was, he was one of its greatest scientist and a remarkable modest original man.

For the last several years, Claude has been a victim of Alzheimer's disease. With Ophelia as she laments in "Hamlet", "O, what a noble mind is here o'erthrown", we all cry out at this most unjust irony of Fate.

Jacob Ziv
(1997 Shannon Lecturer)

I well remember my first visit to Shannon's own study.

I came to MIT to study for my D.Sc. degree in the fall of 1959. Being an R&D engineer, I already knew that it was Information Theory that I would like to learn and investigate. I had first encountered Claude Shannon's monumental contributions after reading and trying to understand Goldman's book on the subject. I was therefore excited when my wife, Shoshana, and I were invited one weekend in the fall of 1959 to an open-house party for all the new foreign students to take place at the Shannon's residence, a beautiful house on top of a hill.

If I remember well, Claude was out-of-town that weekend, but many of the EE faculty were there to host us and warmly greet us. The party took place on the Shannons' huge hillside lawn. We were all impressed by one of the many self-made gadgets: a cable car that took you all the way up to the house. But one could operate it only at dinner time! (A clear message to the Shannon kids to be home for dinner on time!)

After a warm welcome by the faculty, I decided to dare to have a look at Claude's own study. I was impressed by the sight of a huge blackboard behind his desk. The blackboard was covered by a green shade. I was suddenly facing a real dilemma: Should I dare to have a peek at some of Claude's most recent, yet unpublished great results? Finally, after a period of tense hesitation, I moved the shade slightly, only to find out that there was indeed a formula spelled on the blackboard, neatly written in big letters;

$$H = \sum_i p_i \log p_i$$

Claude was apparently ready for us, counting on the fact that at least some of us could not withstand the temptation . . . Since then, I never actually stopped searching for many of the erased results on Shannon's own blackboard.

Conference Calendar

DATE	CONFERENCE	LOCATION	CONTACT/INFORMATION	DUE DATE
February 17–19, 1999	1999 IEEE International Conference on Personal Wireless Communications (ICPWC'99)	Jaipu, India	Dr. Vijay K. Bhargava Dept. of Elec. & Comp. Eng. University of Victoria, P.O. Box 3055 Victoria, BC, Canada V8W 3P6 Tel: +1-250-721-8617, Fax: +1-250-721-6048 e-mail: bhargava@ece.uvic.ca Dr. Ram Gopal Gupta Dept. of Electronics, Govt. of India 6 CGO Complex, Lodhi Road New Delhi 110 003 India Tel: +91-11-436-3095, Fax: +91-11-436-3079 e-mail: guptarg@xm.doe.ernet.in http://www.citr.ece.uvic.ca/icpwc99	September 15, 1998
February 24–26, 1999	IEEE Information Theory Workshop on Detection, Estimation, Classification and Imaging (DECI)	Santa Fe, New Mexico	Prof. Alfred O. Hero III EECS Department U. of Michigan 1301 Beal Avenue Ann Arbor, MI 48109 hero@eecs.umich.edu, http://www.ifp.uiuc.edu/itw-deci	
March 15–19 1999:	IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP)	Phoenix, Arizona	Conference Management Services 3109 Westchester Ave. College Station, Texas 77845-7919 Tel: (409) 693-6000 email: mercer@conf-mgmt.com http://icassp99.asu.edu	September 14, 1998
March 17-19, 1999	CISS '99 Conference on Information Sciences and Systems	Johns Hopkins University, Baltimore, MD	1999 CISS 105 Barton Hall Dept. of Electrical and Computer Engineering Johns Hopkins University Baltimore, MD 21218 Tel: (410)516-7033, Fax: (410)516-5566 Web: http://www.ece.jhu.edu/ciss99/.	January 15, 1999
March 30 - April 1, 1999	PLC'99: 3rd International Symposium on Power-Line Communications	Lancaster House Hotel, Lancaster, UK,	Dr Nader Zein Communications Research Centre Lancaster University Lancaster, LA1 4YR Fax: 44 1524 594207 E-mail: n.zein@lancaster.ac.uk	
June 14-16, 1999	IEEE Signal Processing Workshop on Higher-Order Statistics	Ceasarea, Israel.	Hagit Messer-Yaron Dept. of EE - Systems Tel-Aviv University Tel-Aviv 69978, ISRAEL e-mail: messer@eng.tau.ac.il URL: http://sig.enst.fr/ ~hos99/	
June 15-18, 1999	1999 Canadian Workshop on Information Theory	Kingston, Ontario, Canada	Prof. F. Alajaji Dept. of Mathematics & Statistics Queen's University Kingston, Ontario K7L 3N6, Canada Tel: (613) 545-2423, Fax: (613) 545-2964 Email: fady@polya.mast.queensu.ca Web: http://markov.mast.queensu.ca/~fady/CWIT99/cwit99.html	

Conference Calendar

DATE	CONFERENCE	LOCATION	CONTACT / INFORMATION	DUE DATE
June 20–25, 1999	1999 Information Theory Workshop Kruger National Park, South Africa	Kruger National Park, South Africa	Prof. Hendrik C. Ferreira Dept. of Electrical Engineering Rand Afrikaans University P.O. Box 524 Auckland Park, 2006, South Africa E-mail: hcf@ing1.rau.ac.za Web page: http://www.wits.ac.za/ITW99	January 31, 1999 (recent results)
June 27– July 1, 1999	1999 Information Theory and Networking Workshop	Metsovo, Greece	Prof. Wojciech Szpankowski Department of Computer Science Purdue University W. Lafayette, IN 47907, USA Email: spa@cs.purdue.edu Tel: (765) 494 6703, Fax: (765) 494 0739 Web: http://www.cs.purdue.edu/homes/spa/itw99.html	January 31, 1999 (recent results)
July 11-16, 1999	ISCTA'99 5th International Symposium on Communication Theory and Applications,	Charlotte Mason College, Ambleside, Lake District, UK	Prof. P G Farrell Communications Research Centre Faculty of Applied Sciences Lancaster University Lancaster LA1 4YR UK Tel: 44 1524 593427/594141, Fax: 44 1524 594207 Email: p.g.farrell@lancaster.ac.uk	February 8, 1999
August 2–13, 1999	Workshop on "Codes, Systems and Graphical Models"	Minneapolis, Minnesota, USA	http://www.ima.umn.edu/csg	
November 14-19, 1999.	13th AAECC Symposium on Applied Algebra, Algebraic Algorithms, and Error-Correcting Codes	Honolulu, Hawaii, USA	Prof. Marc Fossorier University of Hawaii Dept. of Electrical Engineering 2540 Dole St., # 483 Honolulu, HI 96822, USA E-mail: marc@spectra.eng.hawaii.edu Web: http://www.irit.fr/ACTIVITES/AAECC/aaecc13.htm	January 15, 1999
June 25-30, 2000	**ISIT 2000**	Sorrento, Italy	Professor Ezio Biglieri Dipartimento di Elettronica Politecnico di Torino Corso Duca Degli Abruzzi, 24 I-10129, Torino, Italy email: biglieri@polito.it Phone: +39 011 5644030 Fax: +39 011 5644099	September 15, 1999

IEEE

Information Theory Society Newsletter

445 Hoes Lane, P.O. Box 1331
Piscataway, NJ 08855-1331 USA