IEEE

IEEE Information Theory Society Newsletter

Vol. 53, No. 3, September 2003 Editor: Lance C. Pérez ISSN 1059-2362

President's Column

Han Vinck

This message is written after returning from an exciting Information Theory Symposium in Yokohama, Japan. Our Japanese colleagues prepared an excellent technical program in the beautiful and modern setting of Yokohama city. The largest number of contributions was in the field of LDPC coding, followed by cryptography. It is interesting to observe that quantum information theory gets more and more attention. The Japanese hospitality contributed to the general success of this year's event. In spite of all the problems with SARS, the Symposium attracted approximately 650 participants. At the symposium we announced Bob McEliece to be the winner of the 2004 Shannon Award. The Claude E. Shannon Award of the IT Society has been instituted to honor consistent and profound contributions to the field of information theory. Bob will deliver his Shannon Lecture at the 2004 Symposium in Chicago. About 20 chairs and the IEEE President Elect Arthur Winston attended the traditional Chapter Chair meeting. It was remarked that the USA chapters are not very active. The German chapter received the 2003 best chapter award for organizing a great number of events in our field. The banquet is the traditional highlight of the social program and, as you can see, I was invited to play the traditional drums.

IT Society President Han Vinck playing traditional Japanese drums.

At the Board of Governors meeting several important decisions were made. I will mention a few to give you an impression of what we are doing during these meetings. First of all, we decided to install the *Distinguished Service Award*. This IT Society Award honors individuals who have shown outstanding leadership in, and provided long-standing exceptional service to, the Information Theory community. Another important topic of discussion was the value of membership. Since the introduction of the electronic library, many universities and companies make this product available to their students and staff members. For these people there is no direct need to be an IEEE member. IEEE membership reduced in general by about 10% and the Society must take actions to make the value of membership visible to you and potential new members. This is an important task for the Board and the Membership Development committee. The Educational Committee, chaired by Ivan Fair, will contribute to the value of membership by introducing new activities. The first action currently being undertaken by this committee is the creation of a web site whose purpose is to make readily accessible educational material related to IT. Future activities of the Education Committee include the possibility of becoming involved in the organization of tutorials and short courses, in conjunction with conferences and/or on-line. Cooperation with the IEEE Educational Activities Board can help to offer high-quality, on-line learning experiences. The utilization of IEEE XPLORE and IEEE Electronic Library will make the material available to a large number of members. I am sure that with your help, we can make this activity to be of great value to our members and students.

Paul Siegel reported as Editor in Chief about our transactions. We now have the largest IEEE journal with about 3500 published pages per year. As reported in my June column, the Board is concerned about the long delay between the submission and publication of a paper. For a full transactions paper the average delay is 2 years. For a correspondence, the delay is 1.5 years. We discussed the possible reasons and the actions that were undertaken by

continued on page 5

From the Editor

Lance C. Pérez

This issue of the IEEE Information Theory Society Newsletter is replete with announcements of awards and honors bestowed upon Society members. We are also fortunate to have an autobiography of Nelson Blachman, who will be celebrating his 80th birthday this October.

Nelson began his career at the same time as David Middleton whose autobiography appeared in the June 2000 Newsletter.

The Information Theory web site has been moved to http://www.ieeeits.org/. The IT web site is full of useful information including pdf versions of the Newsletter. In fact, a pdf version of the most recent Newsletter is posted on the web site soon after it goes to press. For IT members living outside the United States, this may offer more timely access.

Please help make the Newsletter as interesting and informative as possible by offering suggestions and contributing news. The deadlines for upcoming issues of the Newsletter are as follows:

Issue	Deadline
December 2003	October 15, 2003
March 2004	January 15, 2004

Electronic submission, especially in ascii and Word formats, is encouraged.

I may be reached at the following address:

Lance C. Pérez
Department of Electrical Engineering
209N Walter Scott Engineering Center
University of Nebraska-Lincoln
Lincoln, NE 68588-0511
Phone: (402)472-6258
Fax: (402)472-4732
Email: lperez@unl.edu

Lance C. Pérez

Sincerely,
Lance C. Pérez

IEEE

Information Theory Society Newsletter

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

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

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

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

Table of Contents

Honors

G. David Forney and Solomon Golomb Elected to the National Academy of Sciences

Longtime Information Theory Society members G. David Forney, currently Bernard M. Gordon Adjunct Professor in the Department of Electrical Engineering and Computer Science at the Massachusetts Institute of Technology, and Solomon Golomb, currently Andrew and Erna Viterbi Professor of Communications and University Professor at the University of Southern California, were elected to the National Academy of Sciences in the Spring of 2003. The National Academy of Sciences was created in 1863 by a congressional charter approved by U.S. President Abraham Lincoln. Election to the Academy is considered one of the highest honors available to those in science. The NAS is a private, non-profit, self-governing membership body with responsibility for advising the federal government, upon request and without fee, on questions of science and technology.

Jacob Ziv Elected to the American Philosophical Society

Information Theory Society member and Shannon Award winner Jacob Ziv was elected to foreign membership in the American Philosophical Society under Class 1: Mathematical and Physical Sciences. The APS was the United States first learned society and has played an important role in American cultural and intellectual life for over 250 years. Election to the APS honors extraordinary accomplishments in all fields. Presently, there are over 700 members around the world, though 85% of the membership resides in the United States. In the course of the twentieth century, over 200 members of the Society have received the Nobel Prize.

Information Theory Society Members Receive IEEE Awards

Joachim Hagenauer wins the IEEE Alexander Graham Bell Medal

2001 IT Society President Joachim Hagenauer, Professor, Munich University of Technology, Munich, Germany, has been awarded the IEEE Alexander Graham Bell Medal, "for contributions to soft decoding and its application to iterative decoding algorithms".

Claude Berrou and Alain Glavieux win the IEEE Richard W. Hamming Medal

Claude Berrou, Professor, Ecole Nationale Superieure des Telecommunications de Bretagne, Brest, France, and Alain Gavieux, Professor, Ecole Nationale Superieure des Telecommunications de Bretagne, Brest, France, have been awarded the IEEE Richard W. Hamming Medal, "for the invention of turbo codes, which have revolutionized digital communications".

Former Society President Bruce Hajek wins the IEEE Koji Kobayashi Computers and Communications Award

Bruce Hajek, Founders Professor of Engineering, University of Illinois at Urbana-Champaign, Urbana, IL, has been awarded the IEEE Koji Kobayashi Computers and Communications Award, "for the application of stochastic and probabilistic theory to improved understanding of computer-network behavior, particularly, the modeling and performance optimization of multiple-access channels".

Vince Poor Elected Fellow of the ASEE

H. Vincent Poor, Professor in the Department of Electrical Engineering at Princeton University, has been elected a Fellow of the American Society for Engineering Education.

Fellow member status in the ASEE is conferred on members who have made valuable contributions to engineering education. Prof. Poor is one of twelve new fellows recognized at the 2003 ASEE Annual Conference in Nashville, Tennessee.

The Historian's Column

A. Ephremides

When I read the "Three Musketeers" for the first time, I was left with the burning desire to read the sequel, that Alexander Dumas (Père) called "Twenty Years Later". It is exactly twenty years ago (as these lines are being written) that an Information Theory Workshop on Multi-User Information Theory and Systems took place in the resort of Hot Springs, Virginia. Knowing how our field has developed today, I hope that by revisiting that workshop briefly in today's column, our readers may develop a similar desire to review more seriously the record of that workshop. The reversal of time in this twenty-year lapse takes nothing away from Dumas's seminal realization that twenty years is perhaps an optimal time interval for taking snapshots of History.

So, in the lush mountains of southwestern Virginia, an old-world resort hotel, the Homestead, rises from the forest like a mirage. In the middle of June, with some luck, the weather can smile brightly in the Middle Atlantic Region. In 1983, it did. An entire week of perfect long summer days descended on the region with an ideal mix of temperature and humidity. And sixty-nine Information Theorists, along with twelve students who were given gratis admission, and a secretary from the University of Maryland, named Darby Weekly (who has since passed away prematurely) converged to Hot Springs for a special spa treatment that dealt with both mind and body.

First about the body; (please do not take this as any indication of my priorities). The Homestead was, and remains today, a pampering establishment. Its actual hot water springs have been tapped for the creation of a number of massage, skin, rejuvenation, exercise, and other soaking experiences that were all available to the participants. A movie-theater showed first-run flicks every evening. All the meals were included and a "dress-code" required that gentlemen wore tie-and-jacket in the evening. The breakfast cornucopia consisted of unimaginably diverse offerings. The lunch buffet was fabulous and was served outdoors. The dinners were elegant and featured delectable entrees and introduced the participants to Virginia wines, which have grown to become world-class by now. Seeing some of our colleagues, who normally do not don ties and jackets, dressed formally was unforgettable. In short, we felt like royalty. I recall visiting the lunch buffet for the nth time on the last day of the workshop and telling Jack Wolf that this was the last opportunity to — "sin". He answered characteristically, "why the last?".

And now about the mind; this was the first time that the bridging of Information Theory and Networks was formally attempted. The sessions were all focused on "multi-terminal" issues and, although not explicitly addressing networks, revolved around IT concepts as they ought to be reshaped to apply to networks. There were no parallel sessions, no recent result sessions, and all speakers were invited by the session organizers. Each talk was 40 to 60 minutes long. The first session was on Multi-user Information Theory (pretty much as we know it today, except that those were the days of its "dawn") and was organized by Tom Cover. He gave a talk himself that overviewed the area and then Abbas El Gamal (we still miss him), Toby Berger, and L. Ozarow gave talks on Communication Complexity of Computing, Diversity Coding, and Multiple Descriptions respectively.

The second session was on Security, organized by Neil Sloane (then an avid rock climber) and featured C. Pommerance (on Factoring Large Numbers), A. Odlyzko (on Knapsack Public-key Systems), and J. Reeds (on the Breaking of Crypto-Systems previously thought to be secure).

The third session covered Communication Networks directly. It was organized by Bruce Hajek (then an emerging star) and included talks on Flow Control (by Bibb Cain), Routing in Radio Networks (by P. Humblet, where are your Pierre?), Protocol Modes (by Gopinath, where are you Goppi?) and routing in Wireline Networks (by K. Maruyama of IBM).

The fourth session was on Spread-Spectrum for Multi-Access. The stalwart George Turin put it together with Mike Pursley, Chuck Weber, and George himself doing the honors and covering multipath fading effects, coding, and access capacity problems.

The fifth session was on the Theory of VLSI. People with bandwidth-limited minds were asking how did VLSI fit the theme of workshop. Abbas El Gamal organized it in a way that provided the answer. Talks on AT^2 –Lower Bounds for Sorting, Optimization by Simulation Annealing, Complexity for Parallel Computation, Area and Delay Penalties for Restructurable VLSI Arrays, and Distributed Function Computation by C. Thompson, S., Kirkpatrick, T. Leighton, J. Greene, and A. Yao respectively showed both the IT as well as the multi-terminal aspects of VLSI.

Finally, the sixth session on Multi-user Coding was put together by Shu Lin, featuring Victor Wei, himself, and Jack Wolf on Coding for Multi-Access Channels, Coding for Binary Symmetric Broadcast Channel, and Coding for Write-Once Memories, respectively.

All-in-all, this workshop was declared a success and it is fair to say that it caused the "regularization" of the organization of IT workshops every few years (if not more frequently). It is also time to reveal that the organizer of the workshop was myself and that I was assisted by Prakash Narayan who handled the finances. Under his watchful eye a charge for a private massage of one of the invited speakers (who will remain unnamed) was spotted and denied.

In the back country of the Virginia mountains there are still echoes of Information Theory and lore has it that some of us are occasionally still haunting the grounds around the Homestead.

President's Column (continued)

Paul to improve the situation. To support Paul, the Board installed a subcommittee that will investigate how electronics can help to shorten the delays. The communication between editors, reviewers and authors is crucial. Submission of a paper automatically indicates that, in principle, you are prepared to accept a paper to review. New software can help the editorial board to trace the process from submission to publication. Our Transactions and Symposium proceedings also contribute to the revenues of our society. The revenues are generated based on the number of downloads of IT Transactions papers from the electronic library. A new rule for dividing this money among the societies will give an additional $100k in the year 2005. IEEE is also going to refund part of our investment into our own digital library.

During the Symposium I invited the Board of SITA, the Japanese Society for Information Theory and its Applications, to discuss the possibility for further cooperation. SITA is an organization with about 400 members that organizes a yearly symposium and, every two years, the ISITA. In 2004 there will be an ISITA in Parma, Italy. In my view, the Japanese contributions to information theory should be available in English to our members via the digital library. Conference collisions must also be avoided. We also agreed on organizing a joint IT/SITA workshop in the near future. The next president, Hideki Imai, has the right background to implement these ideas. An example of the cooperation with SITA is the organization of the Asia-Europe Workshop on Information Theory together with some European institutions. This year the workshop took place in Kamogawa, just before the 2003 ISIT. Last year's Shannon Award winner contributed to the success of this workshop by playing the harmonica.

In 2003, the society was very successful with the IEEE awards and medals. At the June IEEE meeting in Nashville Joachim Hagenauer, Claude Berrou and Alain Glavieux received the IEEE Alexander Graham Bell Medal and the IEEE Richard W. Hamming Medal, respectively. Bruce Hajek won the IEEE Koji Kobayashi Computers and Communications Award. It is very important that you nominate possible candidates for the IEEE awards. Some of the IEEE awards are not given because there is a lack of candidates. We also need more nominations for the IT Society Best Paper Award and the Joint IT/ComSoc Paper Award. You can find the announcements on our web site or in the March IT Newsletter.

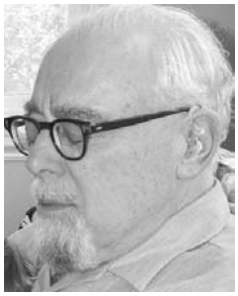
The society needs new activities and initiatives to keep information theory alive and to create new opportunities for our members and students. For this, we need your input and help. Do not hesitate to contact me or one of the other officers or board members. Visit the IT web site at http://www.ieeeits.org/!

Toby Berger playing the harmonica at the AEW banquet.

Han Vinck, Claude Berrou, Joachim Hagenauer and Alain Glavieux after the awards ceremony.

Another Brief Personal History in Science and Information Theory

Editors Note:
This article is, in spirit, a companion piece to the autobiographical sketch by David Middleton that appeared in the June 2000 issue of the Information Theory Newsletter on the occasion of his eightieth birthday. Nelson Blachman is a Fellow of the IEEE, IEE, and the AAAS and resides in Oakland, Calif.



Nelson Blachman 27 October 1923 -

Thanks to a $200 loan from a cousin of my father's, which was later forgiven, I was able to enroll as a freshman in the Case School of Applied Science (now a part of Case Western Reserve University) in the fall of 1940, expecting to study electrical engineering, as I had become an amateur radio operator in 1938. I'd built my own superheterodyne receiver, had designed and built my AM transmitter, and had upgraded my license to Class A in 1939. To earn money for books I got a part-time National Youth Administration job at 25 cents an hour dusting and sweeping the Electrical Engineering Building's classrooms, laboratories, and, best of all, its disused ancient library in the attic. One day while I was sweeping, EE Professor Jack Martin, asked me if I planned to study electrical

engineering. When I said, "Yes," he kindly advised me to plan on going on to law school after Case because the only employment for Jews in that field would be in patent law. Since my father was a lawyer, I was already somewhat acquainted with the field of law. Having lost our home in Cleveland, Ohio, to foreclosure of the mortgage in 1934 with the imposition of a deficiency judgment for the difference between the remaining balance of the mortgage and the amount for which the bank was able to sell the house, my father left his one-man law practice many times to lobby in Columbus in the following two years and succeeded in getting the state legislature to pass Ohio's Deficiency Judgment Relief Act of 1936. He wrote a manual to aid lawyers in using this law for their clients, and in the summer of 1940 I had gone from law office to law office peddling copies of the manual. I thus got to know other lawyers and formed the opinion that this was not the field for me.

Since I didn't want to study law, and the allegation of discrimination against Jews seemed absurd, I rejected the kind advice and might have chosen to specialize in electrical engineering at the end of my freshman year. The school offered the choice among physics and five kinds of engineering, of which only EE appealed to me. In previous years few students had ever chosen physics, but in 1940 physics was included in the freshman curriculum for the first time. It resulted in the quadrupling of the number of sophomores selecting this field.

Some of my brighter classmates persuaded me to join them in choosing physics although I had no idea of how anyone could earn a living in this field outside of teaching, and so I became one of the 16 who selected physics in 1941.

In 1943 on account of the country's involvement in World War II the summer recess was eliminated to accelerate completion of the curriculum. The Physics Department had attained some fame in the field of acoustics because of the work of Dayton C. Miller, who had been its chairman from 1895 to 1931 as well as that of Bob Shankland, its then current chairman. As a result, Ted Hunt, the director of the Underwater Sound Laboratory at Harvard University (HUSL), visited our department that summer and invited four of the remaining 14 of us physics students to join him upon graduation in December.

This was the only job offer that I received, but it was a great opportunity, and the four of us went to Cambridge to help develop sonar for antisubmarine warfare. The Laboratory occupied the Law School's gymnasium despite its lack of a swimming pool, as there were few law students during the war. So there I was, willy nilly going into law. The Laboratory was closed in 1945 at the end of the war, and the building was returned to the law students while I moved to another government-supported research project under Professor E. L. Chaffee in the Physics Department two buildings to the east, where I was able to continue similar work but applying it this time to the effect of noise on AM and FM radio communication. Here I used what I'd learned from Steve Rice's 1944-1945 BSTJ treatise [1] on communication theory, which Malcolm Hebb, who'd headed the Theory Group at HUSL (consisting of him, me, an acoustician, and a mathematician) had recommended that I buy. This was the entry to the field in which I've principally worked all my life.

Taking up part-time postgraduate study in the fall of 1945 when Harvard was glad to accept almost anyone to fill its classrooms, I soon became a full-time student and managed to turn this FM work into a thesis. Students were returning in great numbers from the war in 1947, and my thesis supervisor, J. H. Van Vleck, who in the 1930s had supervised Malcolm Hebb's thesis and who was to receive a Nobel prize in physics in 1977, asked me to finish up and make room for someone else. So I reluctantly complied and left Harvard in June 1947, well launched on my career in physics with applications to electrical engineering but with no training in law.

Professor Van Vleck was also David Middleton's thesis supervisor, Dave having worked with him on radar countermeasures at Harvard's Radio Research Laboratory during the war, and we got our PhD's at the same commencement. Employment in the field of my graduate work prior to starting that study had proved very beneficial to rapid progress in graduate education, and it seems unfortunate that it's relatively rare nowadays.

Being three years older than I, David was able to give me much help subsequently, first in regard to publishing my thesis work and later on, along with Bob Gallager and Bob Price, as a reviewer for McGraw-Hill of my book [2].

While Dave and I had started off somewhat similarly, we went into different work environments after 1947. Although no one is confused about who he is, I've sometimes been flattered to be confused with R. B. Blackman, John Tukey's coauthor in their well known work on the measurement of power spectra [3].

Fortunately the war also stimulated the beginning of an end to discrimination, and I've never encountered difficulties of the sort Jack Martin had described. There was one job offer in 1947 and there was another in 1950 that evaporated when it was discovered that my vision was very poor, but things turned out much better than they might have if I'd gotten either of those positions.

In June 1947 I visited Steve Rice at Bell Laboratories on West Street in New York and got a preprint of his 1948 BSTJ paper [4], which greatly improved my ability to analyze signal-and-noise problems. However, there seemed to be no job opening there at that time. And so I joined the Accelerator Project of the Brookhaven National Laboratory, where I analyzed the noise-like effects of residual gas in the 3-GeVproton synchrotron that was under construction and of the random inhomogeneities in the magnetic field of the machine as well as of noise in the frequency-control system et al., greatly aided by the expertise of my officemate, Ernest Courant, on the diffusion equation in the relativistic regime.

In 1948 I subscribed to the Bell System Technical Journal, and in 1949 I joined the I.R.E., being promptly rewarded by Claude Shannon's papers in the BSTJ [5] and the Proc.I.R.E. [6]. I was ready to appreciate his geometric view of random

Nelson Blachman

signals and noise because, in the summer of 1940, I'd figured out into how many finite and how many infinite regions a set of hyperplanes can divide n-space, thereby developing some feeling for n-dimensional geometry, aided subsequently by Manning's [7], Somerville's [8], and Coxeter's [9] books. But it was probably my hands-on experience building one-tube and then many-tube radios and transmitters that gave me the insight needed for simpler analyses of many problems than could be achieved by more formal methods.

My intuitive feeling for signals and noise came in part from the unpleasant sensations associated with unintentionally coming into contact with high voltages while poking around the bottom sides of tube sockets and among the jumbled resistors and condensers underneath chassis while trying to discover why various devices weren't working properly. The situation has changed radically since the advent of transistors and integrated circuits, the components now being at risk from the high (static) voltages carried by the experimenter rather than vice versa.

The work that has benefited most from the resulting intuition is perhaps the simplified analysis of a signal and noise passing through a memoryless nonlinearity, as represented by four of my papers. The first of these dealt with power-law bandpass nonlinearities [10] (cf. [11]).

Behind [10] lay an intuitive notion of the signal, noise, and signal and noise output of a nonlinearity, which I formalized fifteen years later [12] identifying [13] these uncorrelated time-domain output components with Rice's three infinite double summations of frequency-domain terms [1] for the correlation function of the output of a nonlinearity driven by a signal plus noise.

When the input to the nonlinearity is confined to a narrow band and only the low-frequency or the fundamental-zone or the nth harmonic-zone output is of interest, the analysis of the nonlinearity's performance can be greatly simplified by replacing the nonlinearity by its nth-order Chebyshev transform [14].

In 1968 I updated [10] for the special case of a hard limiter, whose Chebyshev transform for odd n is a hard limiter [15] (cf. [16]), and in the field of FM reception I was able in 1964 to extend Rice's important work [17] to the "click" phenomenon in terms of narrowband signals and noise [18].

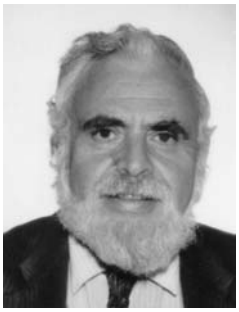
From 1954 to 1997 I served as a consultant on communication theory at the Sylvania Electronic Defense Laboratory, which became a GTE subsidiary and has since become a part of General Dynamics. This job brought a wide variety of communication-theoretic problems to my attention that re-

continued on page 9

GOLOMB 'S PUZZLE COLUMN™

Irreducible Divisors of Trinomials

Solomon W.Golomb



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

If $f(x)$ is an irreducible polynomial of degree n over $GF(2)$, we define the *primitivity* t of $f(x)$ to be the smallest positive integer such that $f(x)$ divides x^t-1, in $GF(2)$ arithmetic. It is well known that t must be a factor of 2^n-1, and if $t=2^n-1$ we say that $f(x)$ is a *primitive* irreducible polynomial over $GF(2)$. Letting $r=(2^n-1)/t$ this can be restated as "$f(x)$ is primitive iff $r=1$ ". It is also well known that the primitivity t of $f(x)$ is the smallest positive integer such that $\alpha^t=1$, where α is any root of $f(x)$.

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

1.If $f(x)$ is primitive, then $f(x)$ divides infinitely many trinomials.

2.If $f(x)$ has primitivity t and $f(x)$ divides no trinomials of degree $<t$, then $f(x)$ divides no trinomials.

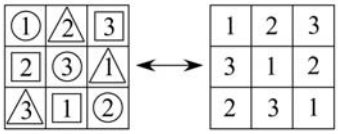
3.If $p\geq 5$ is a prime such that 2 is "primitive" modulo p (i.e. the powers $2^1, 2^2, 2^3, \ldots, 2^{p-1} = 1$ are all distinct modulo p)then the polynomial $f(x)=1+x+x^2+\cdots+x^{p-1} = (x^{p-1})/(x-1)$ is irreducible, and divides no trinomials.

GOLOMB'S PUZZLE COLUMN™

Latin Squares and Transversals Solutions

1. Given a pair of orthogonal Latin Squares, L and L', of order n, each *symbol* in L' occurs in the positions which form a transversal in L. Thus, the n symbols in L' specify n disjoint transversals in L. Conversely, if L has n disjoint transversals, each transversal of L can be used to correspond to a different symbol in L'.

For example:



2. If L is the Cayley table of a group G of order n, and it has a transversal, we can represent this as follows. Let $G = \{ g_1, g_2, \ldots, g_n \}$, and index the rows of L with $g_1, g_2, \ldots, g_n$. For a transversal in L, each row g_i must be paired with a column h_j to get an entry $g_i \times h_j = t_k$, where "×" is the group operation, and all three of $\{g_1, g_2, \ldots, g_n\}$, $\{h_1, h_2, \ldots, h_n\}$, and $\{t_1, t_2, \ldots, t_n\}$ are permutations of the n elements of G. If now we right-multiply each equation $g_i \times h_j = t_k$ by a fixed element $p \in G$, we get a "new" transversal (truly new if p is not the identity element in G), because

$$\begin{array}{l|l} g_1 \times (h_1 \times p) = (t_1 \times p) & g_1 \times h'_1 = t'_1 \\ g_2 \times (h_2 \times p) = (t_2 \times p) & g_2 \times h'_2 = t'_2 \\ \vdots & \\ g_n \times (h_n \times p) = (t_n \times p) & g_n \times h'_n = t'_n \end{array}$$

where $\{ h'_1, h'_2, \ldots, h'_n \}$ is a new permutation of the elements of G, and $\{ t'_1, t'_2, \ldots, t'_n \}$ is a new permutation of the elements of G, disjoint respectively from $\{ h_1, h_2, \ldots, h_n \}$ and $\{ t_1, t_2, \ldots, t_n \}$. Thus, each group element $p \in G$ generates a new transversal, disjoint from the others. (We used the associative law for groups when we took $(g_i \times h_j) \times p = g_i \times (h_j \times p)$.) Thus, if L is a Cayley table, one transversal gives a "complete set" of n disjoint transversals, and hence an "orthogonal mate" L'.

The converse is trivial. If L has an "orthogonal mate" L', it has n disjoint transversals, so surely at least one transversal.

3. If $p = n+1$ is prime, $n > 1$, and L is the Cayley table of Z_p^x, the multiplicative group modulo p (which has order n), we will assume that L has a transversal, and obtain a contradiction. As in the previous problem, a transversal of L looks like:

$$(*) \qquad \begin{array}{l} g_1 \times h_1 = t_1 \\ g_2 \times h_2 = t_2 \\ \vdots \\ g_n \times h_n = t_n \end{array}$$

where $\{ g_1, g_2, \ldots g_n \}$, $\{ h_1, h_2, \ldots, h_n \}$, and $\{ t_1, t_2, \ldots, t_n \}$ are each permutations of $\{ 1, 2, \ldots, n \}$. By Wilson's Theorem of elementary number theory, $n! = (p-1)! \equiv -1 \pmod{p}$. Multiplying all n equations (*) together modulo p, we get

$$\begin{aligned} (g_1 \times h_1)(g_2 \times h_2) \cdots (g_n \times h_n) &\equiv t_1 \times t_2 \times \cdots \times t_n \pmod{p} \\ (p-1)! \cdot (p-1)! &\equiv (p-1)! \pmod{p} \\ (-1) \cdot (-1) &\equiv -1 \pmod{p} \\ +1 &\equiv -1 \pmod{p} \end{aligned}$$

a contradiction.

4. "The number of mutually (pair-wise) orthogonal Latin Squares (MOLS) of order n cannot exceed $n-1$".

Proof. It is no loss of generality to rename the elements in each of the Latin Squares so that each top row consists of 1, 2, 3, $\cdots$, n. Next, we simultaneously permute the remaining rows (which disturbs neither Latin-ness nor orthogonality) so that the second row of the first Latin Square begins with "2". We now ask what the possibilities are for the left-most elements of the second rows of the remaining, mutually orthogonal Latin Squares. From the corresponding elements in the top rows, all the ordered pairs 11, 22, 33, $\ldots$, nn have already occurred, so these left-most positions in the second rows must all be distinct from each other, and from the "2" in the first Latin Square. Moreover, since each sits below a "1" in the top row of its Latin Square, no entry in row 2, column 1, can be "1". This leaves the $n-2$ values 3, 4, $\ldots$, n, and limits the number of mutually orthogonal Latin Squares of order n to at most $1+(n-2) = n-1$.

Note: A construction for $n-1$ MOLS of order n is known whenever there is a field of n elements (thus, $n = p^k$, p prime and $k \geq 1$). Whether this can happen for any other values of n is unknown in general, has been shown to be impossible for infinitely many $n \neq p^k$, and has never been successfully constructed for any $n \neq p^k$.

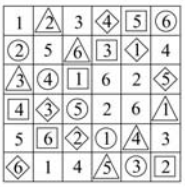
5. "If a Latin Square L of order n has $n-1$ disjoint transversals, then it has n disjoint transversals."

Proof. Each transversal of L consumes one cell in each row, one cell in each column, and one of each of the n symbols. Hence, $n-1$ disjoint transversals consume $n-1$ cells in each row, $n-1$ cells in each column, and $n-1$ of each of the n symbols. Thus, what remains in L is one cell in each row, one cell in each column, and one each of the n symbols, i.e. an n^{th} disjoint transversal.

6. Here is a Latin Square of order 6 with four disjoint transversals, whose elements are enclosed in the figures,circle, triangle, square, and diamond, respectively.

Note: Euler further conjectured that no pair of orthogonal Latin Squares of order n exists when $n = 2m$, where m

is odd. This was shown to be false, in 1959, for all $n > 6$, by R.C. Bose, S.S. Shrikhande, and E.T. Parker. In fact, it has been shown that if $M(n)$ is the maximum number of MOLS of order n which actually occur, then $\liminf_{n\to\infty} M(n) = \infty$.



Nelson Blachman - continued

sulted in many of the foregoing papers and others applying these ideas as well as some on random processes, information theory, et al. For a complete list of my publications, see http://home1.GTE.net/blachman/ .

From 1951 to 1954 I'd worked at the Office of Naval Research (ONR) in Washington, and for occasional relaxation from my forty years at GTE I took leaves of absence to do scientific liaison at ONR's London Branch and to work at the Naval Research Laboratory as well as to teach in Madrid under the Fulbright program. I feel that I've been the beneficiary of much good luck during the course of my career, including my poor vision's not utterly failing until 2000. Fortunately I was able to acquire software by then that speaks aloud my keystrokes and whatever's on my computer screen. So I've not been stopped in my research work although it's slowed down somewhat while Internet communication continues unabated. At GTE in Mountain View there were few other communication theorists with whom to interact, but I'm grateful to the many friends in many places, such as Lorne Campbell, with whom I corresponded in the good old days via snailmail and during the past fifteen years via e-mail.

References

[1] S. O. Rice, "Mathematical analysis of random noise," Bell Sys. Tech. J., vol. 23, no. 3, pp. 282-332, 1944, and vol. 24, no. 1, pp. 46-157, 1945.

[2] N. M. Blachman, Noise and Its Effect on Communication. New York: McGraw-Hill, 1966; 2nd ed., Malabar, Fla.: Krieger, 1982.

[3] R. B. Blackman and J. W. Tukey. "The measurement of power spectra from the point of view of communications engineering," Bell Sys. Tech. J., vol. 37,pp. 185-282 and 485-569, 1958; reprinted by Dover, New York, 1958.

[4] S. O. Rice, "Statistical properties of a sine wave plus random noise," Bell Sys. Tech. J., vol. 27, no. 1, pp. 109-157, Jan. 1948.

[5] C. E. Shannon, "A mathematical theory of communication," Bell Sys. Tech. J., vol. 27, pp. 379-423 and 623-656, 1948.

[6] C. E. Shannon, "Communication in the presence of noise," Proc. Inst. Radio Engrs., vol. 37, no. 1, pp. 10-21, Jan. 1949.

[7] H. P. Manning, Geometry of Four Dimensions. New York: Dover, 1956 (reprint of Macmillan, 1914).

[8] D. M. Y. Somerville, An Introduction to the Geometry of N Dimensions. New York: Dover, 1958 (reprinted from Methuen, 1929).

[9] H. S. M. Coxeter, Regular Polytopes, 3rd ed. New York: Dover, 1973.

[10] N. M. Blachman, "The output signal-to-noise ratio of a power-law device," J. Appl. Phys., vol. 24, no. 6, pp. 783-785, June 1953.

[11] W. B. Davenport, Jr., "Signal-to-noise ratios in bandpass limiters," J. Appl. Phys., vol. 24, no. 6, pp. 720-727, June 1953.

[12] N. M. Blachman, "The signal times signal, noise times noise, and signal times noise output of a nonlinearity," IEEE Trans. Inform. Theory, vol. IT-14, no. 1, pp. 21-27, Jan. 1968.

[13] N. M. Blachman, "The uncorrelated output components of a nonlinearity," IEEE Trans. Inform. Theory, vol. IT-14, no. 2, pp. 250-255, Mar. 1968.

[14] N. M. Blachman, "Detectors, bandpass nonlinearities, and their optimization: inversion of the Chebyshev transform," IEEE Trans. Inform. Theory, vol. IT-17, no. 4, pp. 398-404, July 1971.

[15] N. M. Blachman, "The output signal-to-noise ratio of a bandpass limiter," IEEE Trans. Aerosp. Electron. Systems, vol. AES-4, no. 4, p. 635, July 1968.

[16] J. Kuhar, Jr., and D. L. Schilling, "Signal-to-noise ratios for bandpass limiters," IEEE Trans. Aerosp. Electron. Systems, vol. AES-4, no. 1, pp. 125-128, Jan. 1968.

[17] S. O. Rice, ``Noise in FM receivers,'' ch. 25, pp. 395-422 in M. Rosenblatt, ed., Time-Series Analysis. New York, Wiley, 1963.

[18] N. M. Blachman, ``FM reception and the zeros of narrow-band Gaussian noise,'' IEEE Trans. Inform. Theory, vol. IT-10, no. 3, pp. 235-241, July 1964.

IEEE

ISIT 2004 Chicago

IEEE INFORMATION THEORY SOCIETY it

CALL FOR PAPERS

The 2004 IEEE International Symposium on Information Theory will be held in Chicago, Illinois, from Sunday, June 27, through Friday, July 2, 2004. The theme of ISIT 2004, "Exploring New Connections," represents a focus on fostering new connections among people, technical areas and ideas, both within the traditional boundaries of Information Theory, and beyond in related fields. Keynote speakers for ISIT 2004 will be Persi Diaconis, Ueli Maurer, Thomas J. Richardson and Martin Vetterli.

Previously unpublished contributions to the following areas will be solicited:

Coded modulation	Coding theory and practice
Communication complexity	Communication systems
Cryptology and data security	Data compression
Data networks	Detection and estimation
Information theory and statistics	Multiuser detection
Multiuser information theory	Pattern recognition and learning
Quantum information processing	Shannon theory
Signal processing	Source coding

The following tutorials will be offered on Sunday, June 27:

Gilles Brassard: Quantum Information Processing
Michael Fitz, Giuseppe Caire, Hesham El-Gamal: Space-Time Coding
Brendan Frey: Probabilistic Inference Algorithms and Applications
Ueli Maurer: Cryptography

The conference site is the Chicago Downtown Marriott Hotel, located on the "Magnificent Mile" of Michigan Avenue, near the Chicago river and lake front.

Papers will be reviewed on the basis of an extended abstract (not exceeding six pages) of sufficient detail to permit reasonable evaluation. The deadline for submission is **December 1, 2003**, with notification of decisions by March 15, 2004. The deadline will be strictly enforced. In view of the large number of submissions expected, multiple submissions by the same author will receive especially stringent scrutiny. All accepted papers will be allowed twenty minutes for presentation, and one-page abstracts will be printed in the conference proceedings. Authors are strongly encouraged to submit electronic versions of their summaries in the form of Portable Document Format (PDF) files. Detailed information on paper submission, the technical program, special events, tutorial sessions, accommodations, travel arrangements, excursions and applications for travel grants will be posted on the Symposium web site:

`http://www.isit2004.org`

Inquiries on general matters related to the Symposium should be addressed to `chair@isit2004.org`.

ISITA 2004

Parma, Italy, October 10-13, 2004

FIRST CALL FOR PAPERS

The 2004 International Symposium on Information Theory and its Applications, sponsored by the Society of Information Theory and its Applications (SITA) with the technical co-sponsorship of the IEEE Information Theory Society, will be held in Parma, Italy, from Sunday, October 10, through Wednesday, October 13, 2004.

Topics of interest include, but are not limited to, the following:

- Error Control Coding
- Coded Modulation
- Communication Systems
- Detection and Estimation
- Spread Spectrum Systems
- Signal Processing
- Rate-distortion Theory
- Stochastic Processes
- Data Networks
- Multiuser Information Theory
- Coding Theory and Practice
- Data Compression and Source Coding
- Optical Communications
- Mobile Communications
- Pattern Recognition and Learning
- Speech/Image Coding
- Shannon Theory
- Cryptology and Data Security
- Applications of Information Theory
- Quantum Information Processing

Papers will be selected on the basis of an extended summary (not exceeding 3 pages). The deadline for submission is March 26, 2004. Notification of decisions will be made by June 14, 2004.

The papers accepted will appear in the Proceedings. Detailed information on the technical program, special events, accommodations, and registration will be posted to the Symposium web site

www.sita.gr.jp/ISITA2004

Inquiries on matters related to the Symposium should be addressed as follows:

General matters:
isita2004@sita.gr.jp

Technical program matters:
isita2004tpc@sita.gr.jp

Deadline for the submission of extended summary	**March 26, 2004**
Notification of paper acceptance	**June 14, 2004**
Deadline for final paper submission	**July 16, 2004**
Deadline for author registration	**July 16, 2004**

Symposium Committees

General Chairs
Ezio Biglieri (Politecnico di Torino)
Katsuhiro Nakamura (Chiba Univ.)

General Secretaries
Alessandro Nordio (Politecnico di Torino)
Kouichi Yamazaki (Tamagawa Univ.)

Finance Chairs
Kenji Nakagawa (Nagaoka Univ. Techn.)
Giorgio Taricco (Politecnico di Torino)

Finance Secretary
Jun Muramatsu (NTT)

Publications
Tomoharu Shibuya (Nat. Inst. Multimedia Edu.)
Emanuele Viterbo (Politecnico di Torino)

Organizing Secretariat
STILEMA (Italy)

Registration
Hiroki Koga (University of Tsukuba)

Local Arrangements
Tadashi Fujino (Univ. Electro-Commun.)

Publicity
João Barros (Munich Univ. of Technology)
Ikuo Oka (Osaka City University)
Manabu Kobayashi [web] (Shonan Inst. Tech.)

Technical Program Committee

Chairs
Umberto Mengali (Università di Pisa)
Hirosuke Yamamoto (University of Tokyo)

Vice Chair
Hiroshi Kamabe (Gifu University)

Secretary
Mitsuharu Arimura (Univ. Electro-Commun.)

International Advisory Committee

Chair
Hideki Imai (Univ. of Tokyo)

Conference Calendar

DATE	CONFERENCE	LOCATION	CONTACT/INFORMATION	DUE DATE
September 1-5, 2003	**3rd International Symposium on Turbo Codes and Related Topics**	Brest, France	http://www-turbo.enst-bretagne.fr/	March 31, 2003
September 24-25, 2003	**InOWo'03 - 8th International OFDM Workshop**	Hamburg, Germany	Prof. Hermann Rohling Department of Telecommunications TU Hamburg-Harburg, Ei§endorfer Str. 40 D-21073 Hamburg, Germany Tel: +49 (0)40 42878 3228 Fax: +49 (0)40 42878 2881 email:rohling@tu-harburg.de http://ofdm.tu-harburg.de	TBA
October 1-3 2003	**41st Annual Allerton Conference on Communication, Control and Computing**	Allerton House Monticello, Illinois, USA	R. Srikant and V. Veeravalli allerton@csl.uiuc.edu http://www.comm.csl.uiuc.edu/allerton	July 3, 2003
December 1-5, 2003	**GLOBECOM 2003**	San Francisco Marriott San Francisco, CA	Ms. Patricia Dyett IEEE Communications Society 305 E. 47th St., 9th Floor New York, NY 10017 +1 212 705 8999 (Fax) +1 212 705 8943 GLO2003C@comsoc.org	February 15, 2003
January 14-16, 2004	**5th International ITG Conference on Source and Channel Coding**	Fraunhofer Institute for Integrated Circuits, Erlangen, Germany	Prof. Dr.-Ing. J. Huber (Email: scc04@LNT.de) http://www.LNT.de.itg/	July 21, 2003
June 27 - July 2, 2004	**2004 IEEE International Symposium on Information Theory (ISIT)**	Chicago, Illinois, USA	See CFP in this issue http://www.isit2004.org	Dec. 1, 2003
July 19-24, 2004	**2004 Stochastic Networks Conference**	Centre de Recherches Mathematiques Universite de Montreal Montreal, Canada	http://www.stanford.edu/group/stochnetconf/	
September 1, 2004	**2004 ICC**	Paris, France	http://www.icc2004.org	TBA
November 29-December 3	**GLOBECOM 2004**	Dallas, Texas, USA	http://globecom2004.org	July 21, 2003
September 4-9 2005	**2005 IEEE International Symposium on Information Theory (ISIT)**	Adelaide, AUSTRALIA	TBA	

IEEE Information Theory Society Newsletter

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