IEEE Information Theory Society Newsletter

Vol. 49, No.2, June 1999 Editor: Kimberly Wasserman ISSN 1059-2362

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.

Prof. Tadao Kasami of Hiroshima City University, Japan, 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 Prof. Kasami at the 2000 International Symposium on Information Theory.

Tadao Kasami

Hideki Imai held the following interview with Tadao Kasami in honor of his receipt of the Award.

Interview with Tadao Kasami

Hideki: Congratulations on winning 1999 Claude E.Shannon Award. You certainly deserve this award on the basis of your outstanding contributions in coding theory. I know that you started your career as a researcher at Osaka University. What did you study when you were a graduate student at Osaka University and how did you get involved in coding theory?

Tadao: My supervisor was Prof. Hiroshi Ozaki, an internationally well-known specialist of circuit synthesis theory. Under his guidance, I wrote my master's thesis (1960) on multi-variable positive real function [1], a new concept at that time. Prof. Ozaki advised me to seek a good research field for my Ph. D. thesis other than circuit theory in which there remained only very hard long-standing problems. Almost everyday, I scanned papers in IRE Transactions and so on at the library. For instance, I found a paper [2] by N. Abramson and read it with a strong interest. There continued a rush of epoch-making papers by Bose-Chaudhuri, Peterson and so on. I had to study hard in order to catch up with the progress of coding theory. Finally, I finished my Ph. D. thesis (1963) based on published papers [3-8].

Hideki: How did you meet Prof. W. Wesley Peterson and what did you learn from him?

Tadao: I exchanged letters with Prof. Peterson (Wes) who had been an associate editor of IEEE Trans. on Information Theory. I first had the chance to meet him in 1963 when he visited Japan to attend a URSI meeting in Tokyo. In November 1964, my sincere hope to study under Wes came true by his kind arrangements. I was deeply impressed with his profound knowledge which ran extensively from quantum communication to software engineering. He encouraged me to continue my study [9] on a syntax analysis algorithm for context-free grammar. Wes advised me to select a research subject of main interest in the field. When he suggested weight distribution problems as one of the research subjects, I was afraid that it was too difficult. I still remember his comment to the effect: "You have a permanent position at Osaka Univ. Why don't you try to solve such a problem?"

I am very much happy at the news that Wes has been named as a laureate of the 1999 (15th) Japan Prize for his

Continued on page 29

From the Editor

Kimberly Wasserman

In this issue of the IEEE Information Theory Society Newsletter, I hope you'll enjoy the feature interviews with Tadao Kasami, winner of the 1999 Claude E. Shannon Award, conducted by Hideki Imai, and Kees A. Schouhamer Immink, winner of the 1999 IEEE Edison Medal, conducted by Han Vinck. In the President's Column, Ezio Biglieri discusses the need to develop more efforts to let non-specialists understand the work and activities of information theorists and communications engineers. In the Historian's Column, Anthony Ephremides tells a piscatorial story about the 1986 NATO Advanced Study Institute in Il Cioco. There are also announcements of prestigious awards and medals recently won by members of our Society, and Sol Golomb's puzzle column. Please also note there was an error on page 17 of the last issue (vol. 49, no.1): The names under each of the photographs were inadvertantly switched. The caption for the leftmost photograph should read "Stan Baggen, Martin Bossert, Ludo Tolhuizen, Ulrich Sorger," and the caption under the rightmost photograph should read "Rolf Johannesson, John B. Anderson, and Per Stahl." Please help me to make the Newsletter as interesting and informative as possible by offering suggestions and contributing news. The deadlines for the next few issues are as follows:

Kimberly Wasserman

Issue	Deadline
September 1999	July 15, 1999
December 1999	October 15, 1999
March 2000	January 15, 2000
June 2000	April 15, 2000

Electronic submission, especially in LaTeX format, is encouraged. I may be reached at the following address:

Kimberly Wasserman
Electrical Engineering and Computer Science Department
University of Michigan
Ann Arbor, MI 48109-2122 USA
Tel: +1 (734) 647-3524
Fax: +1 (734) 763-8041
e-mail: wass@eecs.umich.edu

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

Kees A. Schouhamer Immink wins the 1999 Edison Medal

The IEEE Board of Directors has named Kees A. Schouhamer Immink, former research fellow at Philips Research Laboratories, and adjunct professor at the Institute for Experimental Mathematics, Essen University, Germany, the recipient of the 1999 Edison Medal "for a career of creative contributions to the technologies of digital video, audio, and data recording."

Kees A. Schouhamer Immink

Immink's 30-year career with Philips Research Laboratories began in 1968. His work in consumer recording technology started in 1974 when he joined the Philips Optics Research Group. There he and his colleagues conducted pioneering experiments with optical video disc recording. The great success of the Compact Disc Digital Audio System (CD) and other digital recording systems owe much to the work of Kees Immink whose coding methods have had a great impact on data storage. The coding systems he developed are used in essentially all equipment for recording digital video, audio, or data, for example, CD, CD-ROM, CD-I, MiniDisc, CD-Video, DVD, Digital Compact Cassette (DCC), and Digital Video Recorder (DV). Immink has 36 patents, six of which were the basic patents in consumer digital recording products, covering such diverse topics as acoustics, optics, signal processing, servos and coding. He has written numerous articles and co-authored three books.

He is a member of the Royal Netherlands Academy of Arts and Sciences (KNAW) and is a Fellow of the IEEE, Audio Engineering Society (AES), Society of Motion Picture and Television Engineers (SMPTE), and the Institution of Electrical Engineers (IEE) of the U.K. He has been previously honored with the IEEE Masaru Ibuka Consumer Electronic Award, the AES Silver Medal, the IEE Sir J.J. Thompson Medal, and the SMPTE Poniatoff Gold Medal for Technical Excellence.

Immink received a bachelor's degree from Rotterdam Polytechnic and master's and doctoral degrees from the Eindhoven University of Technology, all in electrical engineering.

At the request of the Editor, Professor Han Vinck from the University of Essen held the following interview with Dr. Schouhamer Immink.

Han: First of all, congratulations with this high IEEE award. I hope that you can find a special corner for it in your office at our institute. I hope that this interview gives the IT readers some additional information about your personality and your remarkable career.

Han: For our mostly "academic" type of members it is probably interesting to know why somebody from the industry is a member of the IEEE IT Society?

Kees: I joined the IT Society some 10 years ago after I published my first article (with Gerard Beenker) in the IT Transactions. I have been working with channel codes since 1978 when someone had to be found in the group Optics of Philips Research with some knowledge in that field. I was the only electronics engineer in that group, so the choice was easily made. Besides the compulsory lectures by Piet Schalkwijk at the Eindhoven University, I have no formal training in IT. My first IT conference was Kobe or San Diego, I am not sure which one came first. I have enjoyed the friendly, "family" kind of atmosphere at the ISITs, and I did not find it difficult to make friends as the ISITs are very open to outsiders. The symposia and the Transactions are sources of new ideas for me. To be honest there are also presentations (this is not the monopoly of the ISITs) where I lose track after five seconds. This is not merely lost time, as these presentations give you the opportunity to think instead of work. This is also a source of new ideas.

Han: Today, we have a lot of discussions about the benefit of our society to industry. For which industry is, in your opinion, IT important?

Kees: Shannon worked at Bell Labs, and I think that since 1948 nothing significantly changed as IT still finds its 'home market' in the telecommunications industry. But interesting new markets were added such as for example consumer electronics. Since the digital audio and video revolution started in 1982 with the introduction of the Compact Disc, we see a major impact of IT in our living rooms. A 'simple' digital video recorder as DV has very sophisticated source coding, error correcting systems, and channel coding. Also PCs contain the fruit of 50 years of IT. Who could have imagined some 25 years ago that one could buy a portable CD player (with Reed-Solomon decoders!) for less than $50.

Han: Do you think that more people from industry should join the activities of the IT Society?

Kees: My answer is a very careful yes, because they may find some interesting topics. There are many IEEE conferences every year and the traveling budgets, even in industry, are limited, and thus people have to make a selection. Some people prefer the ICC, Globecom, or related telecom conferences, where they can, for example, see the latest hype of the

Internet or learn the coolest buzzwords. There is a shift in electronics industry in the world from long term research to short term "problem solving", and this is reflected in ISIT participation by industry people. Industrial participation of the ISITs has been very thin during the last 10 years. I did not conduct a formal poll, but I think that during the last 10 years or so participation was less than 15-20 (a few percent) persons. In the upcoming years there will be one less, as I left industry last year to join academia.

Han: To see the impact of Information Theory, I wonder in which of your inventions IT was involved?

Kees: My inventions cover areas such as mechanics, optics, electronics and also coding. In my patents that describe "coding methods and apparatuses" you will find IT as its basis. Most of the ideas described in these patents were published later as Transactions papers.

Han: Many young scientists in Europe have the idea that they can benefit from having a patent on their work. At university level, these ideas also are sometimes in the heads of administrators that want to make money out of science. In this respect your opinion whether researchers at universities should apply for patents instead of trying to publish their results could give some more eye opening information.

Kees: A very careful YES to this question. I do know what this involves: One must invest the time to describe the invention and talk to an attorney, a publication can only be presented after the application (this may result in a significant delay), and there is a price tag to a patent application. The cost might not be that high if the inventor is doing some of the work, like literature search regarding prior art etc. her(him)self. I believe part of the writing of an application can be done without an attorney. Universities in Germany and The Netherlands, and may be many others, provide legal assistance and financial support. The Dutch patent law offers a free-admission procedure if the inventor can show he/she does not have the financial means. But why should you do all this work and take the risk? There are several paths to obtain revenues. Probably, the simplest route is selling the patent (application) outright. It is simple, but selling the invention might mean you lose a great fortune. A second route in the commercialization of your idea is licensing, through which you retain ownership of your patent while allowing another party to make, use or sell the invention. May be the application of a patent is not always a good idea, but it is always worth while, unless of course the study is pure analysis, to use the patent literature as a source of information. Patent literature used to be inaccessible for workers in academia, but that drastically changed a few years ago, when IBM and others started WEB pages that provide access to virtually all patent literature. There are some difficulties that have to be overcome, in particular related to the titles of the inventions as some patent attorneys try to disguise patents by using ambiguous titles. A

whistling kettle is, for example, "A device and/or apparatus for boiling water or other liquids with acoustic signaling". But after a while, you learn to live with that, and the revenue is great as each patent offers by definition a precise description of the new technique.

Han: We just finished a period of 50 years of Information Theory. We all hope that we will have a flourishing new period of 50 years. Do you think that there is a future for IT, and in which areas is there room for new developments? I sometimes have the impression that we are working in the margins.

Kees: I think there will always be research in new coding techniques as channels are changing and competition will be stronger. These new channels and codes require a solid understanding and therefore IT will exist as long as electronics will exist. Margins between proposed codes are indeed becoming smaller and smaller. For example, in 1979, during the Philips/Sony discussions that eventually led to the CD we talked about claimed differences between code performance of 20%. Five years ago, during the DVD standardization, the difference between the two competing code proposals was 6%. The code proposed by Toshiba c.s was a rate 8/15, RLL code while Philips/SONY's code was a rate 8/16, RLL code. The latter, EFMPlus, was adopted. This resulted in a decrease of storage capacity from the proposed 5 to 4.7 GByte. Thus the 6% rate difference resulted in a loss of 300 MByte per disc layer, that is half the storage capacity of the classic CD. As the standard allows up to four layers per disc, the loss in disc capacity is twice the CD capacity. In other words, small 'marginal' differences can make a world of difference. During the last year of my Philips career we discussed codes with SONY engineers for a new product, "to be seen soon", where eventually a code with a 0.2% better rate was adopted. So I agree the differences are getting smaller and smaller, but the impact —royalty income— for industry is still significant.

Han: Continuing the future, the following question could give us some insight about your plans. If you could now choose a new education and a new career, what would you choose?

Kees: I find this question very difficult to answer. The question, I think, means that I am 17 years old again. Statistically speaking I will not choose engineering again as interest for it in the Netherlands, in the whole Western world in fact, is declining. In particular the hard core engineering fields such as mechanics and electrical engineering suffer most. So probably I will choose an education in economics, law, or may be science. I have worked quite intensively with patent attorneys and lawyers during the last six months as I was involved in various litigations. Among others, a litigation in Australia concerning value added tax on Compact Discs. To be honest, law and taxation are not at all as dull or intuitive as I had previously thought.

Han: You received many awards and honors. Which one gave you the most satisfaction and why?

Kees: Yes, I have been spoiled during the last years. I cannot say that award A or B gave me more satisfaction than others. They are all dear to me as they represent tokens of appreciation from my peers in Information Theory, audio and video engineering, and, this year, the Edison Medal by my peers in electrical engineering at large. The Edison Medal, founded in 1906 by the AIEE, was awarded to the pioneers of the electrical arts. The greatest of all, Nicola Tesla, received this award in 1916. It must not have been Tesla's finest hour when he received the medal as the inventors Nicola Tesla and Thomas Edison were not really great 'friends'. According to some sources, Tesla refused to accept the Nobel prize as it would have to be divided with Edison, and it, therefore, remains a great mystery why he decided to accept the medal named after his adversary. The same sources on the Internet report that the only asset Tesla had left in a hotel deposit, when he died in 1942 (his patents on the AC motor and power distribution made him an extremely wealthy man in the late 1900s), was his Edison (gold) Medal. It was, however, not enough to settle his hotel bill. So, I learned from the above story to keep the medal at a safe place, but that I must try to stay away from expensive hotels.

Han: Speaking about electrical art. Your wife, Clazien, is a well-known painter and artist. Did your work influence her?

Kees: I don't know, but I do know that her work has a great influence on me. She makes terrific work, very colorful. I have the possibility to choose work for my office (for a while), and as a result it is always sunny, even when it rains.

Han: Thank you for your time and I hope that you stay in our community for a long time as a scientist, but also as a friend.

Awards

Sergio Benedetto Receives Italgas Prize for Research and Technological Innovation

In October 1998, the Prize Committee of the Italgas Prize for Research and Technological Innovation presented the 1998 Prize to Sergio Benedetto of Politecnico di Torino, Italy. The Italgas Prize is presented every year to two innovative research projects developed by scientists of the European Community in fields of Science and Technology for the Energy, for the Environment, and for Information Systems. It consists of a certificate, a silver plate, and 15 million Italian Lira (about $90,000). The award has been assigned to Sergio Benedetto (and his research partner Pierluigi Poggiolini) for the theoretical and experimental development of "The POLSK Project: Beyond the Limitations of Current Data Transmission Technologies over Optical Fibers," a new modulation technique to transmit information over optical fibers based on the polarization of light.

Robert G. Gallager Wins 1999 Harvey Prize

The American Society for the Technion-Israel Institute of Technology has announced that Robert G. Gallager is the recipient of the 1999 Harvey Prize in the field of Science and Technology. The prize is one of two given annually, and consists of a cash award of 35,000 USD. The Harvey Prize, established in 1972 by the late Leo M. Harvey of Los Angeles, honors major contributions to progress in science, technology, and medicine, as well as contributions to peace in the Middle East. The first winner of this prize was Claude Shannon in 1972. The prize will be presented in Israel on June 16, 1999. Robert G. Gallager is a Professor of Electrical Engineering and Computer Science at the Massachusetts Institute of Technology. An article on Professor Gallager in honor of his receipt of the prize will appear in a future issue of the newsletter.

David A. Huffman wins the 1999 IEEE Richard W. Hamming Medal

The IEEE has announced that David A. Huffman is the recipient of the 1999 IEEE Richard W. Hamming Medal for "for design procedures of minimum redundancy (Huffman) codes and asynchronous sequential circuits, and contributions to analysis of visual imagery." The IEEE Hamming Medal is sponsored by Lucent Technologies and recognizes exceptional contributions to information sciences and systems. It consists of a gold medal, bronze replica, certificate, and cash prize. The medal will be presented at the annual IEEE Honors Ceremony scheduled for June 12th in London. Professor Huffman is a Professor Emeritus of Computer Science at the University of California, Santa Cruz.

James L. Massey Wins 1999 Marconi International Fellowship Award

The Marconi International Foundation has announced that James L. Massey is the recipient of the 1999 Marconi International Fellowship Award. The award honors the name of Guglielmo Marconi, wireless inventor and entrepreneur, and recognizes creative work in communications science or technology and its benefit to humanity. The award consists of 100,000 USD and a work of sculpture. The award will be presented in Marconi's birthplace of Bologna, Italy on April 25th, 1999, the 125th anniversary of his birth. Professor Massey is a Professor Emeritus of Digital Techniques at the Swiss Federal Institue of Technology (ETH) in Zurich, and is an Adjunct Professor at the University of Lund, Sweden. An article on Professor Massey in honor of his receipt of the award will appear in a future issue of the newsletter.

David G. Messerschmitt Receives the 1999 IEEE Alexander Graham Bell Medal

The IEEE has announced that David G. Messerschmitt is the recipient of the 1999 IEEE Alexander Graham Bell Medal "for fundamental contributions to communications theory and practice, including VLSI for signal processing, and simulation and modeling software." The Bell Medal is sponsored by Lucent Technologies and recognizes exceptional contributions to the advancement of communications sciences and engineering. It consists of a gold medal, bronze replica, certificate, and cash prize. The medal will be presented at the annual IEEE Honors Ceremony scheduled for June 12th in London. Professor Messerschmitt is the Roger A. Strauch Professor of Electrical Engineering and Computer Science at the University of California, Berkeley.

The International Technion Communication Day, in honor of Israel Bar-David

The International Technion Communication day took place on Thursday, March 25, 1999 at the new Kogan Auditorium of the Electrical Engineering Department at the Technion-Israel institute of Technology, Haifa, Israel. This forum honored Professor Israel Bar-David, who has recently transferred to emeritus status at the Technion. The event, organized by Professors Gad Eisenstein and Shlomo Shamai, of the EE Dept., Technion, was sponsored by the Electrical Engineering Department of Technion, the Center for Communication and Information Technologies, the Barbara and Norman Seiden Center for Advanced Optoelectronics, the Technion and the Neaman Institute for Advanced Studies. In this meeting, stimulating talks were presented by a gallery of renowned international scientist in the field of communications and information theory, as detailed in the

technical program below. The keynote speaker was the honoree of the meeting, Professor Israel Bar-David, who talked on "Synchronization for the Turbo Age". At the opening, Professor Shlomo Shamai, a member of the IT Society Board of Governors has read the special address of the Society President, Professor Ezio Biglieri. This statement of appreciation, reads: "I am sure to interpret the sentiment of all the members of our society by sending on behalf of the Information Theory Society, this statement of appreciation to one of our most distinguished colleagues. Today, the Technion is celebrating Professor Israel Bar-David who is transferring to emeritus status after a long and distinguished teaching and research career. A proof of the vitality of Information Theory lies in its running the gamut from sublime abstractions to hard-nose concrete. The accomplishments of Professor Bar-David as a scientist witness this in the best of ways. His list of scientific achievements is close to being a syllabus of information theory and it applications: he has made contributions to communication theory, to optical data transmission, to Shannon theory, to coding theory, networks and multiple access, radar and signal processing... Israel bar-David is an inspiration to all of us with his warm humanity and devotion to scholarship. I am proud to be the president of a Society having among its members a man like him."

Program:

(for abstracts see:
http://www-ee.technion.ac.il/comm-day.html)

General Addresses and Greetings:

The Provost: D. Wheis
The Dean: B. Fischer,
and Organizers (G. Eisenstein and S. Shamai).

First Technical Session:

Chair: Moshe Zakai, Technion, Israel.

James Massey, ETH, Switzerland:
"On the Information-Theoretical Wisdom of Israel Bar-David".

Jacob Ziv, Technion, Israel:
"A Universal Prediction Lemma and Applications to Universal Data Compression".

Andrew Viterbi, Qualcomm, USA:
"The End of Coding History or the Start of a New Era? Turbo Decoding and Related Codes".

Second Technical Session:

Chair: Baruch Fischer, Technion, Israel.

Gad Eisenstein, Technion, Israel:
"The 1990's - The Decade of the Optical Amplifier".

Mark Shtaif, AT&T, USA:
"Fiber Optic Communications in the Nonlinear Regime".

Sergio Verdú, Princeton, USA:
"Poisson Communication Theory"

Visit to the Communications Laboratory of the EE Department: General presentation: Israel Bar-David, Technion, Israel. Selected Project Exhibition: organization: Moshe Namer, and Avner Elia, Technion, Israel.

Third Technical Session:

Chair: Jack Salz, Technion, Israel & Lucent, USA.

Amos Lapidoth, MIT, USA:
"Mismatched Decoding Revisited: General Alphabets, Channels with Memory, and the Wide-band Limit". (Joint work with A. Ganti and I. E. Telatar).

Shlomo Shamai, Technion, Israel:
"On Information Theoretic Aspects of Power Control in Multiple-Access Fading Channels".

Joachim Hagenauer, TUM, Germany:
"From Analogue to Digital and Back".

Key-Note speaker: Israel Bar-David, Technion, Israel:
"Synchronization for the Turbo Age".

Conclusion and Short Addresses.

A reception at the EE Department at Technion concluded the meeting.

President's Column

Ezio Biglieri

Ezio Biglieri

In my March column, I briefly commented upon my impression that our work of information theorists or communication engineers is generally not fully appreciated outside of the inner circle of our profession. In part, this is due to the intrinsic difficulty of explaining the fine details of our discipline to nonspecialists (C. P. Snow has commented several years ago on the "two cultures," that make essential to everybody to read Shakespeare, while ignoring the second principle of thermodynamics). However, this difficulty in itself does not forbid many to be informed about such esoteric topics of theoretical physics as the black holes, whose direct relevance to our everyday life is certainly less than that of cellular phones, or of satellite communication systems. Given that the invention of the transistor and the discovery of Information Theory were the two main factors that have shaped our information age as it is now, you will agree with me that the celebrations of their golden jubilees did not receive in the media the coverage they deserve.

I believe that this lack of interest, and hence of appreciation, for our profession is mostly due to the inability, or perhaps better the unwillingness, of engineers to describe to nontechnical people the significance of their work as immediately and forcefully as possible. (Musil's "The man without qualities" has some interesting pages about this.) The research we generate is described in dense, difficult writing replete with jargon intended to be understood only by a few colleagues. In popular perception, engineers (as contrasted with mathematicians and physicians, considered far more interesting people) are hopelessly boring people, who can only talk to other engineers about topics totally deprived of luster. I remember an old Italian cartoon showing a small man, meek and shy, listening with visible embarrassment and boredom to a bigger guy who gestures zealously; a line says, "Two hours ago I confessed to the engineer that I have never quite understood how a radio works." In these days, an engineer who reads literature and goes to the opera twice a year is seen as the modern embodiment of the Renaissance man.

I argue here that we should develop more efforts to let people understand our activity, because the role of the information theorist, and of the communication engineer, is so central in today's society. While some believe that the technological innovations are forced by the intrinsic development of society, others (Marshall McLuhan) believe on the contrary that today's human behavior is mostly determined by the technical tools available (writing, printing, modern communication techniques). The indirect communication has reached such a high degree of development because the modern man has available various and many instruments, like telephone, fax, computer networks, etc. It follows that the history of social changes would reduce to the history of techniques, and hence that the only really decisive maker of change is the communication engineer.

One of the great scientists of our time, Norbert Wiener, addressing the social and cultural implication of the work he was doing, probably better than anybody else viewed the central role that communications can play in our times. Wiener proposes a global worldview in which all disciplines are unified around an axis – communications. In its essence, it translates communications into an activity with considerable social and political value. His main statement can be summarized in this form: *the reality can be entirely interpreted in terms of information and communication*.

In his landmark 1943 article, "Behavior, purpose and teleology," Wiener gives birth to the modern notion of "communications." A few year later, he publishes in Paris, in English, his best-known work, "Cybernetics, or Control and Communication in the Animal and the Machine." Immediately after, he publishes a book whose second edition bears the title "The Human Use of Human Beings: Cybernetics and Society." In this, he describes the results contained in his major scientific publications, and adds a number of reflections on the information society. Wiener's view is centered on the concept of Entropy. The second law of thermodynamics ("the saddest law of nature known," according to Einstein) states that every isolated system tends towards a maximum of homogeneity: its entropy tends to increase, and brings the system towards a state of maximum disorder. On the scale of our universe, this implies what the inventor of thermodynamics, the physicist Ludwig Boltzmann, called the *Warmetod*, the thermal death of the universe. When entropy increases, Wiener says in his "Cybernetics and Society," the universe, and with it all closed systems in the universe, tend naturally to deteriorate and to lose their distinctiveness, to move from the less probable state—– one of organization and differentiation – to the more probable state – a state of chaos and sameness. However, while as a whole the universe tends to run down, there are local enclaves whose direction seems opposite to that of the universe at large, and in which there is a tendency, albeit limited and transient, to an increase of the order. Life finds its home in some of these enclaves.

Wiener then transposes this notion to the field of information exchange. In his book he compares explicitly the

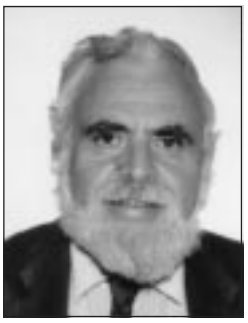
entropy to the action of the devil. There are two kinds of demons, he says: one is that of St. Augustine, called the Imperfection, and the other one is that of the Manichaeans: an obnoxious and malicious devil, one who actively sows disorder and confusion. This distinction is fundamental in Wiener's eyes: for him the "natural" entropy of the universe is original imperfection, rather than willful malice: once the scientist discovers a law of the universe, that does not change (in Albert Eistein's words, Der Herr Gott ist raffiniert, aber boshaft ist Er nicht: God may be subtle indeed, but He is not wicked). Thus, the communication can be confused in two different ways: by nature (the "noise," present in all communication channels) and by those who keep on changing the meaning of messages. Communication can be interpreted as a game played against the forces of confusion, represented by noise and a disturbing agent. Since entropy is the opposite of information, in his strategy of holding back entropy the human being must recognize the decisive importance of the communication tools.

In Wiener's words, "communication is the cement which binds society's fabric together." Those whose work consists of keeping free the communication ways are those on whom depends the perpetuity or the fall of our civilization. Let us read further in Wiener's book: "The process of receiving and using information is the process of our adjusting to the contingencies of the outer environment (...) The needs and the complexity of modern life make greater demands on this process of information than ever before, and our press, our museums, our libraries and textbooks are obliged to meet the needs of this process or fail in their purpose. To live effectively is to live with adequate information."

Since a society is shaped by the messages that circulate in it, Wiener concludes that the society can be understood only through the study of the messages and of the transmission means that belong to it. I cannot think of better words to illustrate the role of the information theorist as a person who is equipped as well as anybody else to understand (and hence to improve) our society.

Golomb's Puzzle Column™ Number 46: Light Switches

Solomon W. Golomb



1. There is an n x n array of light bulbs, with the bulbs located at the lattice points (i, j) in the plane, for $1 \le i \le n$ and $1 \le j \le n$. Next to each bulb is a two-position toggle switch. However, when any switch is flipped, the state of every bulb in the row and column of that location is reversed (from ON to OFF, and from OFF to ON), including, of course, the bulb closest to the switch in question. If the initial condition has all the bulbs in the "OFF" state, show that it is possible, for every n, to find a sequence of switch locations such that, after every switch in the sequence has been flipped, all the bulbs are ON. What sequence of switches with this property is easiest to describe?

2. We repeat the description of the previous problem, but with an additional constraint: It is only permitted to flip a switch that is next to a bulb in the "OFF" condition. Is it still possible to start in the "all bulbs OFF" state and end up in the "all bulbs ON" state? If so, describe a strategy that works for each value of n (not necessarily the same strategy for all n). If not, for which n is there no successful strategy, and why?

Note that in this problem, "all bulbs OFF" is a "Garden of Eden" condition (i.e. it cannot be reached from any other state), and "all bulbs ON" is a "Doomsday" condition (i.e. from that state, no other state can be reached).

Usually, I give you problems of my own invention, or at least ones where I have placed my own spin on an older problem. (For example, Problem 2 is my own variation of the easier Problem 1.) However, the next problem has been around for a long time, and I don't know where it originated; but it fits the theme of this Puzzle Column.

3. You are in Room X, and on the wall are three two-position toggle switches, labelled a, b, c, each with an "ON" and an "OFF" position, and these operate three light bulbs, labelled 1, 2, and 3, in Room Y. From Room X you cannot see or hear or otherwise observe anything in Room Y. Your task is to determine which switch (of a, b, and c) controls which light bulb (1, 2, and 3). All three switches are originally OFF. You can spend as long as you like in Room X, perform any sequence of switch flippings you like, and even make notes on paper, but eventually you must leave Room X and walk down an opaque corridor to the door to Room Y. Once you enter Room Y, there is no turning back, and when you are in Room Y, you must determine the match-up between the three switches that were in Room X and the three light bulbs that you now see in Room Y. Each switch controls one and only one of the three light bulbs. How is it possible to accomplish your task, without violating fundamental principles of Information Theory?

The Historian's Column

A. Ephremides

I have often told stories about the NATO Advanced Study Institutes organized by the late Joseph Skwirzynski, a man of unique personality, peculiar sense of humor, sad, eccentric, and a little mad. The last one in the series took place in 1986 in a quintessential Tuscan locale called "Il Cioco." Nested in verdant hills, it was a lovely location in which to spend two weeks. By that time, many of the participants were "return customers," who knew each other and who had attended at least one of the earlier Institutes in England or in France.

A. Ephremides

Spending two whole weeks penned-up, even in beautiful locations, can be somewhat stressful. Of course, intellectual stimulation abounded in the lecture halls and physical exercise or an occasional escape into the little towns at the foothills provided a dose of diversion. Yet, the confinement and the familiarity (with the environment and with each other) bred the need for additional escapades. One of these, in which I found personal delight, was triggered by a curious suggestion from Jerry Hayes. Jerry lives and works in Canada, has an accent that is unmistakably from the Big Apple, is a man of the world, and hides a lot of mischief under his exuberant demeanor.

So, in the second week of the Institute, overtaken by the culture of the host country and knowing of my keen interest in opera, he came up with the suggestion that there may be a deep relationship between opera and ....fish. His point was that there are many operas whose titles can be minimally altered to convey a name or a notion from the world of undersea life. As evidence he offered some interesting examples. "Madama Butterfly," the popular Puccini classic was awfully close to "Madama Butterfish!" Richard Strauss's "Rosenkavalier" could become "Frozenkavalier" by the mere addition of one letter. Verdi's "Trovatore" sounded like "Pescatore," Wagner's "Tannhauser" could easily sound like "Tannhoyster." And the list went on.

Apart from the utter ridiculousness of these associations, there was an intriguing challenge to test this hypothesis further. So, there we were, two reasonably sane individuals, well-educated, holding responsible places in Society and entrusted by our higher-learning institutions to educate and enlighten the younger generation, engaging in a most foolish, yet highly entertaining, exercise that tried to catalogue additional "opera-fish" associations. In the middle of a lecture, I would look at Jerry at the other end of the hall and see him all of sudden brighten up, break into a huge smile and become red in the face as he was trying to suppress explosive laughter, only to be told at the coffee break that Lehar's "Merry Widow" could be though of as "Herring Widow." And at other times I would find myself jump with delight and anticipation impatiently awaiting the break to tell Jerry that "Porgy and Bess" was a true winner as "Porgy and Bass!" It was out of control. "Siegfried" could be pronounced to rhyme with "fried" as in French Fries! "Nixon in China" could be made into "Nixon in Chinook." We really knew not where to stop. We came up with "Trout and Isolde," "Tuna del Destino," "The Queen of Scales," "Salmon Boccanegra," and on, and on!

Later, and in retrospect, I understood how the minds of prisoners undergo unusual transformations. Touch with reality can be gradually weakened while odd notions can emerge and acquire or perceived significance that seems very natural.

Of course, at the time, we were so enthused with our discovery that we almost became frolicsome. We told others and, to our surprise, they were "hooked" as well. After hearing a talk on Queueing Theory, Jim Massey opined that the profound relationship between opera and fish, that we had empirically discovered, might be attributed to the ...Poisson assumption! And others suggested that the transition from an opera name to a fish name could be prevented by the use of Reed-...Salmon codes! Clearly Pandora's box had been opened; there was no turning back.

I am sure that to many of our readers and especially to those who have seen the Proceedings of the Institute, full of quite serious and insightful presentations, these hilarious happenings must appear as "tales (or is it ... "tails") from the crypt," told by a deranged raconteur. Yet, every word here is true. Up in the mountains of Tuscany, in the middle of a gathering of very bright minds, under the Mediterranean sun, and with the operatic tradition of Italy as a backdrop, some of these minds (not always the brightest) "fished" for diversion in the murky waters of absurdity!

Years later, whenever Jerry and I meet, I can see a twinkle in his eye and, invariably, after reviewing what is new and interesting, we reminisce about fish and opera as both of our minds race secretly and desperately to discover a novel example to add to the list,like "The Magic Fluke", or "Grouperdammerung", or "The Hake's Progress", or.., or..!

Minutes of the IT Society Board of Governors Meeting

Greg Pottie

Cambridge, MA, August 16, 1998

Attendees: Behnaam Aazhang, Julia Abrahams, Vijay Bhargava, Ezio Biglieri, Tom Cover, Michelle Effros, Anthony Ephremides, Thomas Ericson, Hendrik Ferreira, Dave Forney, Tom Fuja, Michael Geselowitz, Jerry Gibson, Joachim Hagenauer, Michael Honig, Hideki Imai, Kees Immink, Bob McEliece, Steve McLaughlin, Urbashi Mitra, David Neuhoff, Vince Poor, Greg Pottie, Ramesh Rao, Shlomo Shamai, Wojtek Szpankowski, Alexander Vardy, Sergio Verdu, Han Vinck, Rick Wesel, Franz Willems, Steve Wicker, Heidi Zazza, Ken Zeger

1. The meeting was called to order at 9:03 AM by Thomas Ericson. Introductions were made.

2. The agenda was approved.

3. The minutes of the previous BoG meeting were approved, after review for follow-up. IEEE press now interested in publishing the special Transactions issue as a book, and it was anticipated that final arrangements would be made shortly.

4. Thomas Ericson made some announcements. He has approved the list of six free memberships to Russian researchers (down from 12, as part of the phasing out process previously approved).

There was some discussion as to whether there should be student members supported, but little enthusiasm for revisiting this decision. The Millenium book project has now been renamed as Engineering Tomorrow. Rob Calderbank has agreed to represent the Information Theory Society in providing prognostications on the future of technology.

5. Ezio Biglieri laid out some options for the BoG meetings for 1999. The first meeting will be held either at the Santa Fe workshop in February or CISS in Baltimore in March; input is solicited. Likewise, there is a choice for the second meeting between South Africa June 20-25 or Metsovo Greece the following week. Discussion on this point suggested that following BoG tradition of holding meetings in countries that hold IT workshops for the first time, South Africa would be favored. The third meeting will be held at the Allerton conference.

6. Heidi Zazza made a presentation on the services IEEE can provide to its Societies. Free assistance can be provided for conferences, conference proceedings, periodicals, financial management, society memberships, TAB support, chapter coordinator support, communications (including posting of material on the web). For a fee, available services include contract review and legal issues, and administrative support.

7. Michael Geselowitz presented material on the IEEE history center. He noted that the late 20th century has been heavily impacted by IEEE related technologies, but the history of these developments have not been widely understood. The history center will undertake oral histories, look at the history of IEEE technologies and societies, perform outreach and education, and conduct scholarly studies and interactions. For books on post-WWII technology, the idea is to produce a series of monographs through each Society to discuss the development of their fields. There will be general volumes for the pre WWI and the inter-war periods. These would be available for sale. The Signal Processing society has already done both technical and Society monographs. A request was made for Societies to provide matching funds to the IEEE Foundation for an endowment to expand the operations. A suggestion was made that each Society should have a designated historian, so that there can be closer coordination. Tony Ephremides was appointed liaison, and will be entrusted with the responsibility of investigating the costs and benefits.

8. Organization improvement. A letter from the evolution task force has been received, inquiring on our opinions on how the IEEE has been reorganized, and what we would like to see in the future. Vijay Bhargava has provided some input.

9. 1998 BoG Elections for terms beginning 1999. Ezio Biglieri was nominated for the office of President. Vijay Bhargava was nominated for first vice-President. Joachim Hagenauer and Victor Wei were nominated for the office of second vice-president. Sergio Verdu then reported on the BoG election committee results, and presented the suggested nominees for BoG membership. The nominees approved by the BoG are Tony Ephremides, Thomas Hoeholdt, Johannes Huber, Kees Immink, John Kieffer, Frank Kschischang, Amos Lapidoth, Upamanyu Madhow, Hiroshi Nagaoka, Prakash Narayan, Alon Orlitsky, Jody O'Sullivan, Vince Poor, Steve Wicker, Raymond Yeung, Bin Yu, and Jacob Ziv.

10. The treasurer's report was made by Benhaam Aazhang. We have recently increased our contributions to long term investments to meet IEEE norms for Societies. Conferences are designed to break even, and have been doing so. This policy will not change. Periodicals have been growing in both income and expenses, with a major contribution to income being institutional sales. There are questions on the impact of electronic publication, and thus options for alternative revenue sources (e.g. exhibitors, tutorial sessions at conferences). A suggestion was made to include a nominal 5% gain from long term investments in the budget.

11. The Information Theory Transactions report was made by Alexander Vardy. There is now no backlog, as the Sep-

tember issue is out. There will have been around 3000 pages by year end, including the special commemorative issue. An announcement on electronic submissions will soon be widely circulated; we are now set up for handling submissions. An electronic database has been set up for the editors to track papers and reviewers. A motion to appoint Ramesh Rao as the new publications editor effective July 1 1999 carried. A new associate editorial position was suggested for papers on sequences, since there are many papers which are now being shared in related areas. The BoG approved the position. We pay roughly $100 for each page published. The reference index takes roughly 150 pages each year; the author and subject indices are only around 10 pages each. Now that we have the digital library and access to Opera, it is proposed that we publish the citation index for the last time in 1998, and thereafter refer members to an electronic site. General agreement was obtained. In a related topic, Ramesh Rao pointed out that the subject index is somewhat out of date with regards to the present areas of specialization, but that reorganizing past listings would be a very large task; we may undertake adjustment of the index with regard to future publications.

Sergio Verdú reported that the special issue is on track for publication in October. Special cover art has been prepared for the approximately 650 page issue. The organizers of the Sante Fe workshop are proposing a special issue along the lines of the workshop theme. There is also the possibility of doing a special issue on codes, systems and graphs, also related to a conference theme in 1999.

12. IT Newsletter. Tony Ephremides reported that the special issue has been produced, and will be made available after the awards banquet at ISIT. The BoG expressed its appreciation to Tony and Jim Massey for their efforts. Michelle Effros reported that IEEE mailed the June Newsletter to the wrong Society; IEEE will pay for remailing it to all our members. The September issue is also ready to go to press. There are continuing complaints on mailing times (even when properly mailed). In particular, overseas expedited mail does not seem to be all that expedited, but no systematic study has been done. It was suggested that time-sensitive overseas material (e.g. conference deadlines) may need to be sent first-class.

13. Claude E Shannon Award. Vijay Bhargava reported that a meeting was held in Ireland to produce a list of nominees; a short list was to be discussed and a decision made before the banquet.

14. Awards Committee. Thomas Ericson reported on the results of the e-mail ballot. The Information Theory Society Paper Award for 1998 was awarded to Ananthram / Verdu for their paper...Congratulations were offered to the authors.

15. Fellows Committee. Vince Poor reported that the Fellows Committee submitted a set of 14 nominations to the IEEE.

16. Digital Library. Steve McLaughlin reported that the CDs are available, and are being handed out to all ISIT registrants, and extra copies will be sold on site. These are a beta version; later versions will have larger search capability. We will need to generate revenue on CDs for continued upkeep of the library. Ramesh Rao reported that an upkeep cost will be roughly $2.50 per page, plus an additional $2000 for formatting. Simple electronic archiving of this will therefore cost roughly $10,000 per year. This does not include cost of distributing additional CDs. The BoG approved performing this task. Ken Zeger proposed continued web access for those who have purchased CDs. However, staffing issues for controlling and ensuring access need to be investigated. There are also costs associated with maintaining one versus multiple sites, and issues regarding draining revenue from the Transactions. A plan will be presented at a subsequent BoG meeting. The BoG expressed its warm appreciation for the work of Ramesh and Steve on this project.

17. Urbashi Mitra reported on membership development. A question that needs to be addressed is what benefits IT membership confers, beyond receiving the Transactions. To raise membership, the matter comes down to how to encourage more people to subscribe, or what other services we could institute to make IT membership more attractive. Mailings to sister Societies are possible, but traditionally have low return on investment. Tom Fuja suggests looking into IEEE interest profiles. Vijay Bhargava has produced a list of chapter chairs, and has produced a list of sections where it would be desirable to institute new ones. Additionally, more use of the distinguished speakers program is encouraged, to build membership at the grassroots level.

18. The symposia and workshops report was made by Tom Fuja.

a. San Diego Workshop. Ken Zeger indicated that the final report not quite ready. There were more than 150 attendees, and a small surplus was generated.

b. Killarney Workshop. Here as well it is expected that the books will be closed soon, with a small surplus expected.

c. Santa Fe Workshop on Detection, Estimation, Classification and Imaging. It was reported to be on track.

d. DIMACS conference on Codes and Trees. Julia Abrahams has produced a handout. There is usually heavy computer science participation, at DIMACS conferences. Information theory involvement at DIMACS has been limited in the past, but there are many resources for encouraging cooperation with its primary areas of sponsorship.

e. ICPWC'99 Feb. 17-19 Jaipur, India. Vijay Bhargava reported that they are expecting an equal mix of overseas, and local attendees.

f. Kruger National Park, June 1999, South Africa. Local arrangements are proceeding well, and they have appointed a travel agent. The technical program is almost finished with about half the speakers identified. An additional loan to help presenters from disadvantaged countries to attend workshop was requested, in amount of $5K, with the conference

organizers undertaking to try to raise funds for this purpose. A motion to approve the additional loan carried.

g. Metsovo, Greece. Wojtek Szpaskowski reported that things are on track. The format is different from most workshops, with shorter talks and more discussion by means of having three panels on the role of IT in multimedia, pricing in networks, and the role of IT in networking. There will be six invited speaker sessions.

h. ISIT 2000, Sorrento, Italy. Ezio Biglieri reported that the anticipated registration fee is $500, which includes lunches. Tutorials on various topics will be offered at cost. A budget was presented which produces a small surplus. A loan in the amount of $40K was requested to get a firm commitment from the conference center and hotel. A motion to approve the loan carried.

i. Proposal for ISIT 2001: Washington DC area. Technical program committee members have been identified, and some sites and times were presented to the BoG. A discussion on timing revealed mid- to-late July to be the most convenient in terms of academic schedules. A motion to approve a proposal for a DC area conference carried. It was further moved and carried that future (annual) ISITs will be held in July.

19. Historical marker in Gaylord, MI. David Neuhoff reported on recent developments. A tentative site has been suggested; it is a new park on Main St. which was the site of Shannon's former residence. It could be made an official state marker; in any case price of around $1K to 2.5K. The park may be named Shannon Park, and a ceremony could be arranged. Some people from the town will be attending the banquet, and interest has been expressed on reporting on ISIT in the town newspaper. A proposal was made to form a small committee and approve $1K now to proceed, and up to $5K in the future. The motion carried.

20. ISIT '98. Dave Forney reported that there were 803 preregistrants, with the expectation of considerable on-site registration. Amos Lapidoth designed the mouse pad and Emre Teletar edited the Shannon paper which were included in each registration package. Digital and analog video cameras, plus still photos will be taken at major events for archival purposes.

21. Awards ceremony. Sergio Verdú will conduct the ceremony to present the Golden jubilee awards, the major IEEE major awards presented by the President of the IEEE, the Information Theory Paper Award, and recognitions for service to the Society.

22. Urbashi Mitra presented the results of the IT logo contest. One logo was the clear choice in member balloting, and the BoG approved the result. A professional will reformat it for use in IT Society publications and correspondence.

23. Additional issues. Fundamentals of Convolutional Codes by Johannesson and Zigangirov is being published by IEEE Press. It was requested that the Information Theory Society sponsor the publication (no financial commitment), so that an announcement can be made in the newsletter. A motion to approve sponsorship carried.

Ezio Biglieri reported on activities related to Vladimir Katelnikov's 90th anniversary. The Communications Society is doing an article for their magazine; this raises the issue of whether we want to do an article on Shannon for the Institute. Thomas Ericson and Ezio Biglieri undertook to find a volunteer. It was suggested that Kitelnikov and his work be the subject of an article in our Newsletter.

Thomas Ericson thanked Jerry Gibson for his long and distinguished service on the BoG. The BoG expressed its appreciation with a round of applause.

Vijay Bhargava suggested that the BoG should similarly honor Thomas Ericson for his work as President of the Society over the past year, and congratulate Sergio Verdú on the occasion of his 40th birthday. This likewise met with enthusiasm.

24. The meeting adjourned at 1:20 PM

Chapters of the Information Theory Society

Vijay Bhargava

Our IEEE represents over 330,000 individuals worldwide. To serve such a large membership, IEEE is organized into ten administrative REGIONS, which likewise, are made up of about 276 local bodies known as SECTIONS. The members of these SECTIONS who have similar technical interest may form CHAPTERS which serve the member interest in many ways. One of the most important is in providing the conduit for technical information to and from members.

At present the Information Theory Society has 24 chapter around the world. A summary with the name of the last known chapter chair follows:

Region 1 (Northeastern USA) Central New England Council (Pankaj Topiwala - pnt@sanders.com); Princeton -Central Jersey (Kenneth J. Kerpez - kerpez@cone.bellcore.com);

Region 2 (Eastern USA) Philadelphia (Moshe M. Kam - kam@lorelei.ece.drexel.edu)

Region 3 (Southeastern USA) Central North Carolina (position vacant); Eastern North Carolina (Thomas W. Powell, Jr. - t.powell@ieee.org)

Region 4 (Central USA) Southwestern Michigan (Delinquent Chapter)

Region 5 (Southwestern USA) Dallas (Delinquent Chapter)

Region 6 (Western USA) San Francisco (Arthur W. Astrin - artastrin@aol.com) Santa Clara Valley (joint with San Francisco)

Region 7 (Canada) Kitchener-Waterloo (David W. Wang - dwang@kingcong.uwaterloo.ca) Montréal (Guy Begin - begin.guy@UQAM.ca)

Region 8 (Europe, Middle East and Africa) Benelux (E. C. Van Der Meulen - ecvdm@gauss.wis.kuleuven.ac.be) France (Gerard D. Cohen - cohen@inf.enst.fr) Germany (Han J. Vinck - vinck@exp-math.uni-essen.de) Israel (Meir Feder - meir@eng.tau.ac.il) Norway (Fritz Bekkadal - f.bekkadal@ieee.org) Romania (Mihai Radu - mradu@main.mta.ro) Russia (Boris S. Tsybakov) Spain (Josep domingo-Ferrer - jdomingo@etse.urv.es) United Kingdom and Repub. of Ireland (Behram Honary -b.honary@lancs.ac.uk)

Region 9 (Latin America) No chapters. However there is a significant concentration of IT Members in Argentina, Brazil and Columbia

Region 10 (Asia and pacific) Beijing (Bao Zong Yuan - bzyuan@center.njtu.edu.cn) Korea Council (Jong-Seon No - jsno@eng.konkuk.ac.kr) (Comprises Changwon, Daejon and Seoul) Taipei (Char-Dir Chung - cdchung@ee.ncu.edu.tw) Tokyo (Kingo Kobayashi -kingo@cs.uec.ac.jp)

There appear to be only 6 or so active chapters. So members may wish to get in touch with their Chapter Chair for possible technical talks and mini workshops. Chapters can take advantage of the IT Society Distinguished Speaker (DS) program. The society will cover upto $500 of DS (defined as a past or present member of the Board of Governors) travel cost when invited by an IT Chapter.

The IT society offers a one time grant of $1000 to a newly established chapter. It is not that difficult to start a chapter. This will be the subject of a future article. In the meantime, please direct your questions to the writer (bhargava@ece.uvic.ca).

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@ece.ucsd.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:

ieee-it.ucsd.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.

CALL FOR NOMINATIONS:

IEEE Medals, Service Awards, and Prize Papers

IEEE has many awards, ranging from prizes for technical achievement to recognition of service to IEEE. The Information Theory Society has many distinguished members, many of whom would be strong candidates for IEEE awards. In the past, when the Society has submitted completed nominations, it has been quite successful. Your help is needed to identify candidates and, equally importantly, help us find people who know the candidates and their work, so that nomination forms can be completed in a substantial way.

Below you will find a list of awards most appropriate to the IT Society. All of the awards listed have a NOMINATION DEADLINE of JULY 1, 1999. We strongly encourage suggestions and or nominations. Suggestions can be directed to Vijay Bharagava at (email: bhargava@ece.uvic.ca. More information on awards and the nomination procedure is also available on the Web at http://www.ieee.org/awards/, or directly from IEEE Awards Department, 445 Hoes Lane, Piscataway, NJ, USA 08855-1331, Tel: (732) 562-3840, Fax: (732) 981-9019, email: awards@ieee.org.

The IEEE Medals: Medal of Honor; Alexander Graham Bell Medal; Richard W. Hamming Medal; Edison Medal; Medal for Engineering Excellence; John Von Neumann Medal; Founders Medal; and James H. Mulligan, Jr. Education Medal.

The IEEE Service Awards: Haraden Pratt Award and Richard M. Emberson Award.

The IEEE Prize Paper Awards: W.R.G. Baker Prize Award, Donald G. Fink Prize Award, and Leon K. Kirchmayer Prize Paper Award (successor to the Browder J. Thompson Memorial Prize Award).

CALL FOR NOMINATIONS

IEEE Information Theory Society Board of Governors

According to its Bylaws the IT-Society should elect each year six new members to the Board of Governors. The election is shall be by mail ballot. The election is prepared by a nomination committee, consisting of the Board President and the two most recent past presidents, with the junior past president as the chairman.

All members are solicited to submit nominations. Any Society member is eligible.

Please send nominations to Thomas Ericson, thomas@isy.liu.se.

WORKSHOP REPORT

Workshop on Coding and Cryptography

Cercle National des Armées
Paris, France
January 11—14, 1999

The first Workshop on Coding and Cryptography was held January 11-14, 1999 at the ''Cercle National des Armées'', Paris, France. It was jointly organized by INRIA (French National Institute for Research in Computer Science and Control) and the research center of the ''Écoles de Coëtquidan". It was sponsored by the DGA (French ministry of defense), the SCSSI and Thomson-CSF.

Our aim was to bring together researchers coming from coding theory and cryptography. More than 120 participants from 21 countries attended the workshop — France (57), United States (18), United Kingdom (6), Russia (5), Germany (4), The Netherlands (4), Sweden (4), Irland (3), South Korea (3), Italy (3), Czech Republic (2), Slovakia (2), Brazil, Bulgaria, Denmark, Israel, Kazakhstan, Mexico, Norway, Spain, Taiwan. A wide range of topics were addressed during the meeting, from the more fundamental, as finite fields theory, lattices and designs to subjects closer to industrial applications as cryptography, convolutional coding or soft decoding of block codes. Algebraic coding theory was treated in all its variety, from the classical problems as code classification or parameter determination to more recent concerns as codes over rings, in particular $\mathbf{Z}_4$. Let us mention also that some of the talks have treated of the interactions between coding and cryptography.

The program committee chaired by Claude Carlet has chosen 48 papers among 76 submissions, all of very good scientific level. In addition we had four outstanding invited talks; Vera Pless presented recent work on the classification of extremal formally self-dual codes (jointly with W.C. Huffman, J. Fields and Ph. Gaborit), Hans Dobbertin exposed a variety of new results in discrete mathematics applied to information protection, Ernst Gabidulin presented a reflection on the design of public-key crypto-systems based on coding theory, in particular by considering non-Hamming metrics, finally Jim Massey exposed an original work on the construction of non-singular matrices providing optimal diffusion in block ciphers.

The participants have enjoyed the nice environment and the high quality of the service offered by the staff of the ''cercle militaire'' as well as the lunches and the banquet.

Organizing committee: C. Carlet (INRIA and Université de Caen, France), G. Cohen (Chairman of the IEEE-IT French Chapter, France), E. Filiol (Centre de Recherche des Écoles de Coëtquidan, France), C. Fontaine (INRIA, France), S. Harari (Université de Toulon, France), N. Sendrier (Chair, INRIA, France),

Local organization: A. Theis-Viemont (INRIA, France), C. Thenault (INRIA, France).

Program committee: D. Augot (INRIA, France), J. Boutros (ENST, France), T. Berger (Université de Limoges, France), A. Burr (University of York, UK), A. Canteaut (INRIA, France), C. Carlet (Chair, INRIA and Université de Caen, France), P. Charpin (INRIA, France), G. Cohen (ENST, France), J.-M. Couveignes (DGA and Université de Bordeaux, France), P. Farrell (University of Manchester, UK), A. Glavieux (ENST-Bretagne, France), M. Girault (CNET Caen, France), S. Harari (Université de Toulon, France), G. Kabatiansky (Russian Academy of Sciences, Russia), D. Lebrigand (Université Paris 6, France), S. Litsyn (University of Tel Aviv, Israel), H. Mattson (University of Syracuse, USA), F. Morain (DGA and École Polytechnique, France), N. Sendrier (INRIA, France), S. Shepherd (University of Bradford, UK), H. van Tilborg (Eindhoven University of Technology, The Netherlands).

Invited talks

On self-dual and formally self-dual codes — *Vera Pless*

New permutation polynomials and applications to codes, sequences and Boolean functions — *Hans Dobbertin*

Metrics generated by linear codes in cryptography — *Ernst Gabidulin*

Optimum transform diffusion — *Jim Massey*

Monday morning — *Code structure*

Construction and classification of quasicyclic codes — *K. Lally, P. Fitzpatrick*

On the complexity of calculating the minimum norm of a binary code — *I. Honkala, A. Lobstein*

Perfect binary codes components — *F.I. Soloveva*

Permutation groups of error-correcting codes — *N. Sendrier, G. Skersys*

Recognition of a binary linear code as a vector-subspace — *A. Valembois*

Monday afternoon I — *Block codes, spherical codes and hash functions*

Bounds on the sizes of ternary weight-constrained codes — *M. Svanstrom*

On the quaternary [18,9,8] code — *J. Olsson*

Spherical codes generated by weighted unions — *T. Ericson, V. Zinoviev*

Monday afternoon II — *Decoding of block codes*

Iterative multistage maximum likelihood decoding of multi-level codes — *D. Stojanovic, M. Fossorier, S. Lin*

Permutation soft decision decoding of some expanded Reed-Solomon codes — *E. Delpeyroux, J. Lacan*

Bit-level soft-decision sequential decoding for Reed Solomon codes — *M. Oh, P. Sweeney*

On bounding the probability of decoding error with the minimum distance — *J.-P. Tillich, G. Zémor*

Tuesday morning — *Cryptography I*

On the relation of error correction and cryptography to an off line biometric based identification scheme — *G.I. Davida, B.J. Matt, R. Peralta, Y. Frankel*

Verifiable self-certified public keys — *S. Kim, S. Oh, S. Park, D. Won*

Authentication frauds from the point of view of rate-distortion theory —- *A. Sgarro*

Cheating in split-knowledge RSA parameter generation — *M. Joye, R. Pinch*

Fair and efficient proof that two secrets are (not) equal — How to solve the socialist millionaires' problem — *F. Boudot, J. Traoré*

Tuesday afternoon I.a (parallel) — *Finite fields*

Finite fields, primitive normal bases with prescribed trace — *D. Hachenberger*

Bounds on the bilinear complexity of multiplication in any extension of $\mathbf{F}_q$ — *S.Ballet*

The a-invariant of some Reed-Muller type codes over the Veronese variety — *C. Renteria, H. Tapia-Recillas*

Multiplicative characters and design of sequences with good autocorrelation — *C. Boursier*

Tuesday afternoon I.b (parallel) — *Channel coding*

On the capacity of distance enhancing constraints for high density magnetic recording channels — *E. Soljanin, A.J. van Wijngaarden*

Algebraic construction of good collision resistant signal sets — *M. Greferath, E. Viterbo*

Code constructions for block coded modulation systems with interblock memory — *C.-N. Peng, H. Chen, J.T. Coffey, R.G.C. Williams*

Tuesday afternoon II — *Coding Theory*

Perfect codes and balanced generalized weighing matrices — *D. Jungnickel, V. Tonchev*

Higher order covering radii — *P. Solé*

Strengthening the Gilbert-Varshamov bound — *A. Barg, S. Guritman, J. Simonis*

Recursive MDS-codes — *E. Couselo, S. Gonzalez, V. Markov, A. Nechaev*

Wednesday morning I — *Cryptography II*

A construction of systematic authentication codes based on error-correcting codes — *S. Xu, H. van Tilborg*

Arithmetic coding and data integrity — *X. Liu, P. G. Farrell, C. Boyd*

Wednesday morning II — *Codes over* $\mathbf{Z}_4$

Negacyclic and cyclic codes over $\mathbf{Z}_4$ — *J. Wolfmann*

Codes of constant Lee or Euclidean weight — *J. A. Wood*

On the covering radius of $\mathbf{Z}_4$-codes and their lattices — *T. Aoki, P. Gaborit, M. Harada, M. Ozeki, P. Solé*

Wednesday afternoon I — *Codes over rings*

Permutation groups of extended cyclic codes over Galois rings — *T. Blackford*

Complete weight enumerators of generalized Kerdock code and linear recursive codes over Galois ring — *A. Kuzmin, A. Nechaev*

On the structure and Hamming distance of linear codes over Galois rings — *G. Norton, A. Salagean-Mandache*

Cyclic and affine invariant codes — *K.S. Abdukhalikov*

Wednesday afternoon II — *Lattices and designs*

Lattices, codes and Radon transforms —- *M. Boguslavsky*

Designs, harmonic functions, and codes — *C. Bachoc*

Extremal polynomials of degree $\tau + 2$ and $\tau + 3$, which improve the Delsarte bound for τ-designs — *S. Nikova, V. Nikov*

On the maximum T-wise independent systems of Boolean functions — *V. Levenshtein*

Thursday morning — *Convolutional codes*

Decoding convolutional codes using a multiprocessor Bidirectional Creeper Algorithm — *V. Imtawil, D.J. Tait*

On low-density parity-check convolutional codes —- *K. Engdahl, K.S. Zigangirov*

A Gallager-Tanner construction based on convolutional codes — *S. Vialle, J. Boutros*

New algorithm to identify rate k / n catastrophic punctured convolutional encoders — *C. O'Donoghue, C. Burkley*

Convolutional-like codes over discrete valuation rings and an application to 2-adic codes — *N. Lagorce*

WORKSHOP REPORT

WIC Midwinter Meeting on Object-oriented Audiovisual Communication

Technical University Eindhoven The Netherlands
January 19, 1999

The Benelux "Werkgemeenschap voor Informatien Communicatietheorie" organised its annual midwintermeeting as usual in middle of January and had also this time an interesting theme: Object-Oriented Audio-Visual Communication. The WIC midwintermeeting attracted around 150 people and was held in the beautiful "Blue Room" of the Auditorium at the Technical University Eindhoven. The meeting was organized by Prof. Jan Biemond (TU Delft), Dr. Andries Hekstra (KPN Research) and Prof. Peter de With (University Mannheim). Local arrangements were made by Dr. Frans Willems (TU Eindhoven). The large attendance was likely due to the rapid and interesting developments in picture coding where for example, the new compression standard MPEG-4 reaches maturity in this time period. This standard is not just based on video compression, but treats images as a set of objects that can be individually generated, processed, coded, and addressed for regeneration at the receiver.

The meeting program was opened and chaired during the morning by Prof. Jan Biemond; he addressed the importance of this emerging technology and explained the meeting program briefly. Furthermore, five keynote speakers presented various aspects of Object-oriented coding. The program is listed below.

Dr.ir. Inald Lagendijk (TU Delft, NL) Introduction to Object-Oriented AV Communication

Ir. Rob Koenen (KPN Research, NL) MPEG-4 overview and operational environments

Ir. Isabelle Corset (Philips Research, France) MPEG-4 video coding overview

Dr.ir. Stef Desmet (KU Leuven, Belgium) Segmentation into video objects

Drs. Paul ten Hage (CWI Amsterdam, NL) Facial coding and animation

Dr. Inald Lagendijk gave a clear explanation of the logical step from existing image coding towards object-oriented video processing. He emphasized the techniques which are required to come to an O-O AV coding system: segmentation of images, advanced and various compression techniques and a layered and flexible system control. Ir. Rob Koenen presented in more detail the flexibility of the MPEG-4 coding standard, in particular the possibility to compose various multimedia objects, with attached descriptions such as sound, graphical features and data. He also showed interesting demonstrations showing some capabilities of the new standard, such as copying and after editing of video persons in a running video sequence and audio with mixed computer-generated audio features on very low bit rates.

The afternoon was chaired by Prof. Peter de With and opened with the presentation of Ir. Isabelle Corset. She presented the differences in coding techniques between the MPEG-2 and MPEG-4 standard. She also gave demonstrations where the picture quality of the standard was shown for various low bit rates. Dr. Stef Desmet explained how images can be segmented into different areas, they are described with features such as texture (details), motion, and shapes. He explained the difficulty of finding objects consistently and he demonstrated with a video tape the results of various experiments. Drs. Paul ten Hage presented a new system with which the faces of human beings can be edited for animations and generating expressions. The system can be used within the MPEG-4 standard for coding computer-generated human beings. The afternoon was closed by Prof. Peter de With, thanking all attendants and speakers and indicating the upcoming WIC symposium in May 1999, at Leuven, Belgium.

Mannheim, Febr. 15, 1999

Peter de With.

CONFERENCE REPORT

1999 IEEE International Conference on Personal Wireless Communications (ICPWC'99)

Jaipur, India
February 17-19, 1999

The fourth ICPWC attracted over 200 delegates from 30 countries. A total of 90 papers were selected for presentation at the conference. These were grouped in sessions entitled: Multicast; IMT-2000 Networks; Ad-Hoc Networks; Detection and Estimation; Random Access; CDMA Systems; Modulation; Equalization; Wireless TCP/IP and 802.11

Networks; Source and channel Coding; Network Architecture and Design; Resource Allocation: Satellite Networks; Wireless Access and Local Loops; Software Radios; Mobility and Handovers and Network Planning and Economics. Tutorials were presented by Vijay Bhargava on "Multimedia Wireless Systems"; by Ramjee Prasad on "GSM Evolution: Toward the Edge"; by Vijay Garg on "Applications of CDMA to Wireless Communications" and by A. Chockalingam on "Internet and Data Services on Wireless Local Loop". A panel discussion on "Advances in Wireless Local Loop Technology" was organized by Eric Barnhart. Participants included Bhasker Ramamurthi and Ashok Seth. Plenary talks were presented by Jorgen Bach Anderson, Anil Kriplani, P. S. Saran, Arvind Krishna, Tero Ojanpera and Anil Sawkar. The conference enjoyed corporate sponsorship from Hughes Software Systems (India), IBM Solutions Research Centre (India), Lucent Technologies (USA), NOKIA (Finland), Qualcomm (USA), Silicon Automation Systems (India) and STZE (France). Copies of the 507 page Conference Proceedings (IEEE Catalog Number 99TH8366; ISBN 0-7803-4912-1) are available from: IEEE Operations Center, P.O. Box 1331, 445 Hoes Lane, Piscataway, NJ, USA 08855-1331; +1-800-678-IEEE (Toll Free in North America); +1-732-981-1393; +1-731-981-9667 (Facsimile); e-mail: customer.service@ieee.org. The fifth IEEE ICPWC is scheduled to be held during the second half of December 2000 in Hyderabad, India. Details may be found on conference web site located at www.citr.ece.uvic.ca/icpwc2000

Vijay Bhargava (extreme left), Tero Ojanpera (extreme right) and several delegates at the ICPWC'99 outdoor conference reception on February 18, 1999.

WORKSHOP REPORT

IEEE 1999 Information Theory Workshop on Detection, Estimation, Classification, and Imaging

February 23-26, 1999
Al Hero, Pierre Moulin, Joseph O'Sullivan, co-chairs

The ITW-DECI was held in Santa Fe, New Mexico at the Hotel Loretto. The workshop started with an opening reception on Tuesday evening, February 23. Three days packed with technical talks and posters followed. The ITW-DECI was a success in every way. Many of the best researchers in the areas covered by the workshop participated. The social events were well received.

The location for the workshop could not have been better. The weather in Santa Fe was perfect. The temperature reached over 70 F during the days and was cool at night. Several participants took advantage of the nearby ski resorts, national parks, and mountains. Most visited one or more of the many wonderful museums in Santa Fe.

Technical Program

Leading off the technical program each day was a plenary speaker. Michael I. Miller from the Johns Hopkins University, Vince Poor from Princeton University, and Andrew Barron from Yale University gave inspirational talks. The complete listing of talks and a Postscript version of the papers is available on the web site for the workshop, http://ifp.uiuc.edu/itw-deci/.

The oral presentation sessions each included invited speakers and were organized by an outstanding technical committee without whom the workshop would not have been such a success. There were eight oral sessions: Regularization (V. Solo), Imaging (D. Snyder), Random Processes (J. Moura), Detection (B. Hughes), Classification (G. Lugosi and A. Nobel), Signal Processing (A. Hero and P. Moulin), Estimation (B. Yu), and Statistical Inference from Compressed Data (A. Hero and P. Moulin). Several of these sessions included contributed papers. Two poster sessions consisting exclusively of contributed papers were organized with the assistance of M. Brandt-Pearce. The poster sessions offered opportunities to interact more closely with the presenters. All of the sessions were lively and well attended.

Social

The workshop brought together researchers from diverse areas. There were 88 registrants, which is close to the ideal

number for this type of focused workshop. In addition to the opening reception, there was a continental breakfast each morning at 8 a.m., a banquet reception, and a banquet on Thursday evening. The banquet dinner had a distinct Southwestern flair.

The staff at Hotel Loretto was very professional, as was the audio-visual company that the hotel uses. The catering was very good overall. The banquet food and presentation in particular were excellent.

The Information Theory Society Board of Governors held a meeting in Santa Fe on Saturday, February 27 at the La Fonda Hotel.

Financial

The financial picture is not complete, however the workshop will return a small surplus.

The workshop was awarded $6000 by the National Science Foundation (through the communications program in CISE), primarily to support the travel of students and junior faculty members. The announcement of these travel grants resulted in more requests than could be awarded; 13 awards were made.

CALL FOR PAPERS

Special issue of the IEEE Transactions on Information Theory: Codes on Graphs and Iterative Algorithms

A special issue of the IEEE Transactions on Information Theory will be devoted to the connections between graphical models, codes and iterative algorithms. Original research papers that make major contributions to research on the application of iterative, graph-based algorithms to decoding and other related detection and estimation problems are sought.

Iterative algorithms, such as belief propagation, turbo-decoding, gradient search and variations of these, have proven to be extremely successful in (approximately) solving various problems in communications.

This has led to a surge of research devoted to understanding and exploiting the connection between codes on graphs and iterative algorithms. One of the main goals of this research is to understand why iterative algorithms work so well empirically on graphs with cycles. Another emerging research direction is the efficient representation of codes on graphs. Much promising research has also been devoted to joint iterative, graph-based treatment of different tasks in a communication system.

Papers for this special issue should relate to the developments described above. Expository papers, survey papers, research papers and correspondence items are welcome. Topics include, but are not limited to, the following:

- Analysis of iterative algorithms in graphical models
- Realization complexity of graphical models for codes
- Graph-based constructions for codes
- Graphical models for sources, channels and signaling systems that are suited for iterative algorithms
- Combined decoding and adaptive filtering / estimation using graphical models

Prospective authors should follow the regular guidelines of these Transactions, except that manuscripts should be submitted directly to phone of the following sites:

Paper	**Electronic (postscript)**
Ralf Koetter Coordinated Science Laboratory University of Illinois at Urbana 1308 W. Main St. Urbana, IL, USA 61801 Tel.: (217) 244 4471	*www.cs.uwaterloo.ca/~frey/cgia.html*

Electronic submission of manuscripts is encouraged.

Guest Editors

G. David Forney, Jr., Motorola, Inc.
Brendan J. Frey, University of Waterloo (co-Editor-in-Chief)

Ralf Koetter, University of Illinois (co-Editor-in-Chief)
Robert J. McEliece, California Institute of Technology
Daniel Spielman, Massachusetts Institute of Technology

Schedule

Submission deadline: Dec. 15, 1999
Selection of papers: Aug. 15, 2000
Publication: Feb., 2001

OPEN CALL

Summer Program: IMA Workshop on "Codes, Systems, and Graphical Models"

August 2-13, 1999
Institute for Mathematics and its Applications
Minneapolis, Minnesota USA

The invention of turbo codes and other capacity-approaching codes has led to an exciting cross-fertilization of ideas betweeen researchers from different backgrounds. The aim of the workshop is to bring together mathematicians, engineers, and computer scientists with diverse specializations, including — but not limited to — coding theory, systems theory, and symbolic dynamics. It is hoped that techniques developed in some of these areas can be applied to problems in other areas within the general theme of the workshop.

The program will consist primarily of invited lectures, with ample time for discussions and interaction. The workshop is open to any researcher in a relevant field who would like to attend and can provide his or her own support. For registration and logistical details, see the workshop Web site at http://www.ima.umn.edu/csg/

The workshop will be subdivided into two main focus areas. The schedule, and the list of speakers follow.

Codes on Graphs and Iterative Decoding
August 2-6, 1999
Dave Forney and Alexander Vardy, co-organizers

Invited speakers:

Michael Tanner
Frank Kschischang
Michael Luby
Ruediger Urbanke
Steve Wicker
David MacKay
Tom Richardson
Robert McEliece
Radford Neal
Brendan Frey
John Lafferty
Dave Forney
Andi Loeliger
Steffen Lauritzen
Randy Bryant
Jim Massey
Ralf Koetter

Connections Among Coding Theory, System Theory and Symbolic Dynamics
August 9-13, 1999
Brian Marcus and Joachim Rosenthal, co-organizers

Invited speakers:

Roger Brockett
Clyde Martin
Jan Willems
Klaus Schmidt
Paul Weiner
Rolf Johannesson
Dominique Perrin
Sandro Zampieri
Brian Allen
Margreet Kuijper
Mike Boyle
Sanjoy Mitter
Paul Siegel
Maria Valcher
Paul Fuhrmann
Roxana Smarandache
Natasha Jonoska
Selim Tuncel
Patrick Fitzpatrick
M. S. Ravi

There will also be room for a small number of contributed papers in the fields covered by the workshop, preferably bridging fields. Authors who would like to present a contributed paper should send a title and abstract to one of the organizers, at least two weeks prior to the workshop.

WORKSHOP ANNOUNCEMENT

DIMACS Center for Discrete Mathematics and Theoretical Computer Science: Workshop on Codes and Association Schemes

November 9 - 12, 1999
DIMACS Center, Rutgers University, Piscataway, NJ

Organizers:

Alexander Barg, Bell Labs, Lucent Technologies, abarg@research.bell-labs.com

Simon Litsyn, Tel Aviv University, litsyn@eng.tau.ac.il

The workshop is of primary interest to mathematicians (coding theorists, combinatorialists) and also to computer scientists and engineers.

Applications of algebraic combinatorics, in particular, theory of association schemes to coding theory account for most important structural results and bounds on the size of codes and designs. This link, understood broadly, will be the main topic of the workshop. Applications to codes include bounds and properties of codes in discrete spaces (Hamming space, Johnson space), packings of lines and other linear spaces in the Euclidean space, quantum codes,

properties of distance enumerators of codes, constructions of codes.

The workshop will include, but is not limited to the following topics:

- applications of the polynomial (linear programming) method;
- properties of codes in discrete metric spaces;
- spherical codes, packings of Grassmanians;
- properties of quantum codes;
- classification and properties of association schemes
- properties of orthogonal polynomials (zeros, asymptotics)
- constructions of codes related to the above methods

Talks will be by invitation. We would like to limit the number of talks in order to leave time for interaction of participants. A list of speakers will be available as the workshop draws nearer.

We intend to put together a volume of proceedings in the AMS-DIMACS series. The volume will include original papers on combinatorial coding theory or surveys written by the participants. A booklet with abstracts of talks will be distributed at the workshop. There is a $35 per day / $5 per day for postdocs and graduate students registration fee for this workshop. For complete information on registration, travel and accommodations please see:

http://dimacs.rutgers.edu/Workshops/AssociationSchemes/

CALL FOR PAPERS

The Third International Conference Distributed Computer Communication NetworkS (DCCN'99) Theory and Applications

November 9 - 13, 1999
Tel-Aviv, Israel

Organizers: Institute for Information Transmission Problems (IPPI) of the Russian Academy of Sciences (Moscow, Russia), Tel-Aviv University (Tel-Aviv, Israel), Center for Technological Education Holon (Holon, Israel), with the cooperation of Information Theory Society of IEEE, the Moscow Chapter of Information Theory Society of IEEE, Russian Ministry of Science and Technology, Russian Scientific and Technical Popov Society for Radio, Electronics and Telecommunications, International Telecommunication Academy (Moscow, Russia) and Israeli Ministry of Science.

The main topics of the Conference include, but are not limited to:

- Performance Evaluation Models for Computer Networks
- Computer Networks Architecture Design
- Queueing Systems: Theory and Applications in Telecommunications
- Computer Network Security
- Protocols, ISDN and Intelligent Networks
- Management and Control of Information Networks
- Measurement and Optimization in Computer Communication Networks
- Dependability of Computer Communication Networks
- Computer Communication Networks in Industry, Business and Finance

Please send your papers (up to 5 pages), or extended abstracts up to three pages in the electronic form in LATEX-files, edited by means of LATEX-2E or LATEX-209, and 2 hard copies format A4 (2000 characters per page). If needed the authors may use also AMSSYMB and LATEXSYM. The authors who don't use LATEX may use also WORD6 or ASCII-codes but this is only in the case if their paper does not contain any formulas. The papers must include the following information: the title of the paper, names of the authors, short information about authors (including organization, postal and e-mail addresses), the abstract (less than 10 lines), the text, the references. All the papers will be refereed, and the accepted papers will be published in the book of Proceedings of DCCN'99. Selected papers will be published in journals "Automation and Remote Control" and "Information Systems and Operations Research".

Please send your papers to:
Prof. V.M. Vishnevsky
DCCN'99-Conference Institute for Information Transmission Problems
Bolshoy Karetny, 19, Moscow 101447, Russia.
E-mail: belozer@iitp.ru
Fax: (7 095) 200 3338

Important dates: Deadline for papers and abstracts in electronic and hard forms: June 5, 1999. Acceptance notification: June 20, 1999. Preregistration at the Conference and Hotel reservation: October 15, 1999.

Registration: The total registration fee is 350 USD for early registration (before September, 15). Late registration (after September, 15) is 400 USD. The fee includes the access to all sessions, Proceedings of the Conference, lunches, coffee breaks, the technical excursions, the cultural program and the gala dinner. Special registration: for students and post-graduate students the special registration fee is 75 USD (without the cultural program), and for accompanying persons the fee is 200 USD. This fee includes the technical excursions, the cultural program and the gala dinner. For participants-new immigrants from Israel the fee is 200 USD. This fee includes access to all sessions, Proceedings of the Conference, lunches, coffee breaks, the technical excursions and the gala dinner.

Hotel Accommodation: The conference will be held in Hotel "Metropolitan",11-15,Trumpeldor St., Tel-Aviv. One night room rate in Hotel "Metropolitan" ****: Per person in double room on B/B basis - 55 USD. Per person in single room on B/B basis - 105 USD. Hotel "Top" ***: Per person in double room on B/B basis - 39 USD. This accommodation prices are valid for early registration.

Payment Method
BANK: LEUMI LISRAEL
BRANCH: 817 HASHMONAIM
91, Hashmonaim str., Tel-Aviv
Account # 110-240700/79
D.N.C. LTD.

Please point out that it is your payment for DCCN'99 and send copy of the payment confirmation to the Fax: (7 095) 299 2904 (7 095) 209 0579

For more detailed information, please contact:

Dr. Nina Bakanova,
E-mail: nina@iitp.ru
Fax: (7 095) 209 0579
http://www.iitp.ru/dccn

SITA'99
1999 Symposium on Information Theory and its Applications

30 November — 3 December 1999
Niigata Japan
Sponsored by the Society of Information theory and Its Application, Japan
Co-sponsored by the IEEE Information Theory Society, Tokyo Chapter and the IEICE Technical Group on Information Society, Japan

CALL FOR PAPERS

The Twenty-second Symposium on Information Theory and Its Applications (SITA'99) will be held on 30 NOVEMBER — 3 DECEMBER, 1999 in Niigata, Japan. General sessions of this symposium solicits paper submission from people who will present new theoretical developments and techniques in information theory and its applications to real world. Topics of interest include, but are not limited to, the following areas:

- Shannon Theory
- Coding Theory
- Source Coding
- Channel Coding
- Data Compression
- Coded Modulation
- Applications of Information Theory
- Cryptology
- Information Security
- Sequence Design and Analysis
- Stochastic Processes
- Image and Speech Processing
- Communication Theory
- Signal Processing
- Computer Network
- Optical Communications
- Spread Spectrum Systems
- Neural Network
- Signal Processing and Coding for Storage
- Others Related

Submission Guidelines

Working Language: Japanese or English

English sessions are provided.

Abstract: 200-word abstract with 5 keywords to be submitted. The title page must include the authors name, affiliation, complete return address, telephone, facsimile, and e-mail address.

Submission Address:
Naohisa Komatsu Professor,
Department of Electronics, Information and

Communication Engineering,
Waseda University
3-4-1 Ohkubo, Shinjuku-ku,
Tokyo 169-8555, Japan
Phone: +81-3-5286-3390,
Fax: +81-3-5273-7367
e-mail: komatsu@kom.comm.waseda.ac.jp

Schedules

Submission of Abstract: 5 September 1999

Notification of Acceptance: 20 September 1999

Submission of Final Manuscript: 20 October 1999

For Further Information Please contact:

SITA '99 Secretariat,
Department Electrical Engineering,
Nagaoka University of Technology,
Nagaoka, Niigata 940-2188, Japan
Phone: +81-258-21-4263,
Fax: +81-258-47-9500
e-mail: sita99@comm.nagaokaut.ac.jp
WWW: http://comm.nagaokaut.ac.jp/SITA99/

CALL FOR PAPERS
INFOCOM 2000

IEEE Infocom 2000

(Israel) http://www.comnet.technion.ac.il/infocom2000
(U.S.A.) http://www.cse.ucsc.edu/~rom/infocom2000
(Japan) http://halo.kuamp.kyoto-u.ac.jp/~infocom
(general) http://www.comsoc.org/confs/infocom

Dan Panorama Hotel, Tel Aviv, Israel
March 26-30, 2000

Sponsored by the IEEE Communications and Computer Societies

Scope

For the last 18 years, Infocom has been the major conference on computer communications and networking, bringing together researchers and implementors of every aspect of data communications and networks presenting the most up-to-date results and achievements in the field.

The 19-th annual conference on Computer Communications, Infocom 2000, will be held at the Dan Panorama Hotel in Tel-Aviv, Israel, during the week of March 26-30, 2000. The conference is sponsored by the technical committees on computer communications of the IEEE Communications and Computers Societies.

The Infocom 2000 organizing committee is soliciting original papers describing state-of-the-art research and development in all areas of computer networking and data communications. Topics of interest include, but are not limited to, the following:

Active Networks
Network Management and Control
BISDN and ATM
Network Reliability
Billing and Pricing
Network Restoration
Congestion and Admission Control
Network Signaling
Distributed Network Algorithms
Network Standards
High-Speed Network Protocols
Network and Protocol Performance
Integrated Control of Networks
Optical Networks
Intelligent Networks
Personal Communications Systems
Internet
Photonic Switching
Internetworking
Protocol Design and Analysis
Lightwave Networks
Quality of Service
Mobility
Routing and Routing Protocols
Multicast/Broadcast Algorithms
Security and Privacy
Multimedia Protocols
Switch Architectures
Multimedia Terminals and Systems
Testbeds and Measurements
Multiple Access
Traffic Management and Control
Network Architectures
Video Networking
Network Design and Planning
Wireless Networks and Protocols

Paper Submission

Papers must be submitted electronically in the manner and format detailed below. Authors for whom this presents a se-

vere problem should contact one of the technical program committee co-chairs to discuss alternatives.

Papers must be formatted according to the IEEE standard format except for the font size, which must be 11pt. To make it easy to adhere to the formatting standard we offer templates and samples for LaTex, MSWord, and FrameMaker (consult at the web pages referenced on top of this message).

Submission must be in PDF. However, the committee will also accept Postscript from Latex, FrameMaker, or MSWord source file. Postscript papers must use only standard PostScript fonts: Times Roman, Courier, Symbol, and Helvetica. (Postscript output from MSWord typically does not work on non-Microsoft platforms. The use of the Apple LaserWriter II printer driver is strongly recommended). The above formatted papers can be submitted in a compressed form (gzip, zip, compress).

Because of the size limitation on the final manuscript, and to ensure that the reviewed paper and the final version have a similar size **papers with more than 11 pages will not be reviewed** (this is roughly equivalent to 20 double-spaced pages).

Papers must be submitted electronically using the Web site at:

<http://www.cs.columbia.edu/~hgs/edas/infocom2000>.

This web page contains exact and detailed instructions. The submission process includes providing detailed contact information. To save space authors can omit this information from the paper itself. Authors will receive an immediate notification of the successful receipt of the file containing their paper. Subsequently, a formal notification will be sent after verifying that the paper can be printed successfully.

Submissions will only be accepted between April 1st and July 1st, 1999

Submission deadlines are strict! Papers that have been improperly submitted or improperly formatted by the submission date will not be considered. To avoid last minute problems, authors are encouraged to submit their papers well in advance of the deadline.

The Review Process

Each paper will typically be reviewed by three independent reviewers, whose reviews will be relayed to the corresponding author. To facilitate the review process authors will be asked to classify the paper according to a list of categories so that the most appropriate reviewers handle the paper. This year a new step will be introduced into the process whereby authors will have a chance to provide a limited rebuttal on the reviews before the program committee makes its final decision.

Travel Grants

Limited travel assistance to students, post-docs and junior faculty for defraying some of the costs of presenting a paper in the conference will be available. Please refer to the conference web sites for further details later this year.

Important Dates

Complete paper due	April 1 - July 1, 1999
Notification of acceptance	October 31, 1999
Final version due	December 3, 1999

Program Committee Co-Chairs
[infocom@comnet.technion.ac.il]

Raphael Rom, Technion, Israel
Henning Schulzrinne, Columbia University, USA

GOLOMB'S PUZZLE COLUMN ™ Number 45:

Solutions to 0-1 Matrices Solutions

Solomon W. Golomb

1. M is an $n \times n$ matrix of 0's and 1's with all rows distinct.

   a. We prove by mathematical induction on n that it is always possible to remove a column from M in such a way that the shortened rows remain distinct.

   The case $n = 1$. If there is only one row, it has no other row to be distinct from, and needs no elements at all. (Since you may find "validity by default" to be suspect, we do the next case individually also.)

   The case $n = 2$. We have a 2×2 matrix of 0's and 1's with distinct rows, so we can find a column in which the two rows differ. Discard the other column.

The general case. Assume that, for all $n \le k$ (where k is at least 2), whenever we have an $n \times n$ matrix of 0's and 1's with all rows distinct, it is possible to remove a column and still have all rows distinct, and consider the case $n = k + 1$. If the left-most column is constant, discard it, and we are done. Otherwise, the left-most column contains **a** 0's and $\mathbf{k+1-a}$ 1's, where $1 \le a \le n$. Consider separately the a $\times$ (k + 1) matrix of the rows beginning with 0 (call it M_0) and the $(k + 1 - a) \times (k + 1)$ matrix of the rows beginning with 1 (call it M_1). In M_0, ignoring the left-most column of "all 0's", we can find $a - 1$ of the remaining columns which make all the rows distinct, by the inductive assumption. In M_1, ignoring the left-most column of "all 1's", we can find $k - a$ of the other columns which make all the rows distinct, by the inductive assumption. In the worst case, if the columns needed to make the rows of M_0 distinct and those needed to make the rows of M_1, distinct are disjoint, we still only need (at most) $1 + (a - 1) + (k - a) = k$ columns to make all $n = k + 1$ rows distinct.

[*Note.* This problem is easily seen to be equivalent to Problem 1E in Van Lint and Wilson's *A Course in Combinatorics*, Cambridge University Press, 1992, for which they suggest a considerably more complicated proof involving graph theory.]

b. The $n \times (n - 1)$ matrix $\begin{bmatrix} 1 & 1 & 1 & \cdots & 1 & 1 & 1 \\ 1 & 1 & 1 & \cdots & 1 & 1 & 0 \\ 1 & 1 & 1 & \cdots & 1 & 0 & 1 \\ 1 & 1 & 1 & \cdots & 0 & 1 & 0 \\ - & - & - & - & - & - & - \\ 1 & 1 & 0 & \cdots & 1 & 1 & 1 \\ 1 & 0 & 1 & \cdots & 1 & 1 & 1 \\ 0 & 1 & 1 & \cdots & 1 & 1 & 1 \end{bmatrix}$ has the property that whichever column is removed, the reduced top row becomes identical to one of the other reduced rows.

2. A typical incidence matrix of a (v, k, λ) design, illustrated for the case $v = 7$, $k = 3$, $\lambda = 1$, is

$$M_7 = \begin{array}{c|ccccccc} & x_1 & x_2 & x_3 & x_4 & x_5 & x_6 & x_7 \\ \hline L_1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ L_2 & 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ L_3 & 0 & 0 & 1 & 1 & 1 & 0 & 0 \\ L_4 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \\ L_5 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ L_6 & 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ L_7 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \end{array}$$

In general, if M is the incidence matrix of a (v, k, λ) design,

$MM^T = \begin{bmatrix} k & \lambda & \lambda & \cdot & \cdot & \cdot & \lambda \\ \lambda & k & \lambda & \cdot & \cdot & \cdot & \lambda \\ \lambda & \lambda & k & \cdot & \cdot & \cdot & \lambda \\ \cdot & \cdot & \cdot & \cdot & & & \cdot \\ \cdot & \cdot & \cdot & & \cdot & & \cdot \\ \cdot & \cdot & \cdot & & & \cdot & \cdot \\ \lambda & \lambda & \lambda & \cdot & \cdot & \cdot & k \end{bmatrix}$ $(k - \lambda)I + \lambda J$, where I is the $v \times v$ identity matrix, and J is the $v \times v$ matrix consisting entirely of 1's.

There are many proofs of the elementary identity $k(k - 1) = \lambda(v - 1)$.

Here is one based on the matrix identity for MM^T.

The sum of all the elements in the product matrix is $v(k+\lambda(v-1))$, because there are v rows, each with one k and $v-1$ λ's. Another way to count this is to observe that there are $v \bullet k$ 1's in the matrix M (v rows each with k 1's), and in the product MM^T, the 1 in position m_{ij} of M multiplies each of the k 1's in the j^{th} row of M^T, so that the sum of all elements in the product MM^T must be $(v \bullet k) \bullet k = vk^2$. Thus $vk^2 = v(k+\lambda(v-1))$, from which $k(k-1) = \lambda(v-1)$.

3. a. The 3×3 matrix $\begin{pmatrix} 0 & 1 & * \\ 1 & * & 0 \\ * & 0 & 1 \end{pmatrix}$ has its three rows $\begin{pmatrix} R_1 \\ R_2 \\ R_3 \end{pmatrix}$ *comparable* (each pair of rows differs in a column where neither has the value "*"), and the rows are also *consistent* (if there is a column where R_i has 0 and R_j has 1, there is no other column where R_i has 1 and R_j has 0). Yet, if we say $R_i < R_j$ if R_i has 0's where R_j has 1's, then we see in our 3×3 example that $R_1 < R_2 < R_3 < R_1$, so that "<" as defined is not transitive.

b. For $n = 3, 7, 13$, and 21, the largest known values of m such that there is an $m \times n$ matrix of comparable and consistent rows are $m = 5, 16, 41$, and 86, respectively. Here are examples:

$$\left[\begin{array}{ccc} 0 & 0 & 0 \\ \hline 1 & * & 0 \\ * & 0 & 1 \\ 0 & 1 & * \\ \hline 1 & 1 & 1 \end{array}\right] \text{ or } \left[\begin{array}{ccc} 0 & 0 & 0 \\ (1 & *| & 0) \\ 1 & 1 & 1 \end{array}\right], \quad n = 7, \left[\begin{array}{ccccccc} 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \hline 1 & 0 & 0 & * & 0 & * & * \\ 0 & 0 & * & 0 & * & * & 1 \\ 0 & * & 0 & * & * & 1 & 0 \\ * & 0 & * & * & 1 & 0 & 0 \\ 0 & * & * & 1 & 0 & 0 & * \\ * & * & 1 & 0 & 0 & * & 0 \\ * & 1 & 0 & 0 & * & 0 & * \\ \hline 1 & * & 1 & 1 & 0 & * & * \\ * & 1 & 1 & 0 & * & * & 1 \\ 1 & 1 & 0 & * & * & 1 & * \\ 1 & 0 & * & * & 1 & * & 1 \\ 0 & * & * & 1 & * & 1 & 1 \\ * & * & 1 & * & 1 & 1 & 0 \\ * & 1 & * & 1 & 1 & 0 & * \\ \hline 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{array}\right] \text{ or } \left[\begin{array}{ccccccc} 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ (1 & 0 & 0 & * & 0 & * & *) \\ (1 & * & 1 & 1 & 0 & * & *) \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{array}\right]$$

[A row in parenthesis means: take all cyclic shifts of that row.]

$$n = 13, \left[\begin{array}{cccccccccccccc} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ (1 & 0 & 0 & 0 & * & 0 & 0 & * & * & 0 & * & * & *) \\ (1 & * & * & 1 & 1 & 0 & 0 & * & * & 0 & * & * & *) \\ (1 & * & * & 1 & 1 & * & 1 & 1 & 1 & 0 & * & * & *) \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{array}\right]$$

$$n = 21, \left[\begin{array}{ccccccccccccccccccccc} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ (1 & 0 & 0 & 0 & 0 & * & 0 & 0 & 0 & * & * & 0 & 0 & * & * & * & 0 & * & * & * & *) \\ (1 & * & * & * & 1 & 1 & 0 & 0 & 0 & * & * & 0 & 0 & * & * & * & 0 & * & * & * & *) \\ (1 & * & * & * & 1 & 1 & * & * & 1 & 1 & 1 & 0 & 0 & * & * & * & 0 & * & * & * & *) \\ (1 & * & * & * & 1 & 1 & * & * & 1 & 1 & 1 & * & 1 & 1 & 1 & 1 & 0 & * & * & * & *) \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{array}\right]$$

When $n = u^2 + u + 1$, we can get $m = u(u^2 + u + 1) + 2$ rows by this construction. It is not known whether any larger m is ever possible. For further details, see "A new result on comma-free codes of even word-length", by B. Tang, S.W. Golomb and R.L. Graham, *Can. J. Math.* vol. 39, no. 3, 1987, pp. 513-526.

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

Tadao Kasami . . .

continued from page 1

contribution to the establishment of coding theory for reliable digital communication, broadcasting and storage (for the details, refer to the Awards columns in IT Newsletter, Vol.49, No.1).

Hideki: Could you tell us a little more about weight distribution problems?

Tadao: First, I thought about what kind of codes were to be considered. A good candidate is a code with a very small weight profile. It is also desirable that a part of the weight profile can be found somehow. The simplest known example is a maximum-length-sequence code. What is the next simplest example, I asked myself? Fortunately, Peterson and Prange [11] showed in 1964 that extended (narrow-sense) BCH codes are invariant under the affine group of permutations. I derived a necessary and sufficient condition on the generator polynomial of a cyclic code whose extended code is invariant under the affine group of permutations [12]. The size of the group is almost the square of the code length. Therefore, if the number of codewords of an invariant code is not larger than the square of code length, then the size of its weight profile must be very small. By using Pless identities [14], I derived weight distribution formulas for such a class of binary codes, e.g., the dual codes of double-error-correcting binary narrow-sense BCH codes. After I wrote a report [15], it occurred to me that the weight profile of the second order Reed-Muller codes could be found [17] and then weight restrictions of subcodes of second order Reed-Muller codes such as the dual codes of extended triple-error-correcting binary narrow-sense BCH codes could be derived. I worked out the details and wrote a report [18] in the summer of 1966.

Hideki: In the area of spread spectrum communication systems, Kasami sequences are very famous and have been put into practical use. How did you invent the sequences?

Tadao: Thank you for your kind question. When I was writing the report [15] in the spring of 1966 (I was staying at the Coordinated Science Lab., Univ. of Illinois-Urbana from February to September in 1966), I referred to tables of experimentally determined crosscorrelations of maximum-length sequences of periods up to 8192 in the reports [19] by Gold and Kopitzke in order to check derived formulas. My interest was mainly in deriving weight distribution formulas. Certainly, a class of weight distribution problems can be translated into crosscorrelation problems among a set of sequences. Kasami sequences are translated versions to terms of crosscorrelations from weight distributions of a class of codes presented in my reports [15,18], and were kindly named by D. V. Sarwate and M. B. Pursley [20]. It is my fortune that the formulas turned out to have such a practical application.

Hideki: You have done much work on Reed-Muller codes. Recently these codes are widely noticed as maximum likelihood decodable codes. Please tell us about your old and new work on Reed-Muller codes.

Tadao: Reed-Muller (RM) codes are my favorite. As you know, they have a very simple mathematical structure. First, the weight structure is simple. In fact, weight distribution formulas for the 2nd order RM codes, weight distribution formulas of weights less than 2.5 times of the minimum weight for the 3rd or higher order RM codes and weight distributions of RM codes of length 512 or less except for the 4-th RM code of length 512 are known [21-24]. Secondly, the trellis structure is simple as is shown by D. Forney [25]. The standard order of components has been shown to be optimal in terms of the state complexities of the trellis diagram [26] by using the generalized Hamming weights [27]. The structure of the subtrellis diagram for low weight codewords has been analyzed by using split weight distributions [28,29].

Last I would like to add an episode on the nesting relation with BCH codes. In the summer of 1965, Dr. Shu Lin (Shu) joined the Univ. of Hawaii to work under Wes and shared an office with me. In September of 1965, Shu noticed that cyclic codes, called punctured RM codes, can be obtained from RM codes by deleting the first component and permuting the remaining components in a certain way. Then Wes showed us a list of exponents of roots of generator polynomials for several punctured RM codes computed by his program. The list was very regular and I proved a theorem [30] to determine generator polynomials. Thus we knew a nesting relation [31] between RM codes and extended BCH codes. The knowledge on the former may be used for the latter. This has been used in determining the minimum weights [32,33] and deriving weight distribution formulas for some classes of BCH codes or related codes as I explained.

I recommend young colleagues to attempt applying a new technique first to RM codes and (if successful), then to extended BCH codes related to RM codes. For example, the recursive maximum likelihood decoding algorithm [34,35] has been applied to RM codes very favorably and then to extended BCH codes related to RM codes favorably. I have enjoyed the work on RM codes.

Hideki: Thank you. It has been a great pleasure to interview you and to provide our readers with a better sense of what you have done in coding theory.

[1] H. Ozaki and T. Kasami, "Positive real functions of several variables and their applications to variable network," IRE Trans., vol. CT-7, 251-260 (1960), also in Multidimensional Systems: Theory & Applications, ed. N.K. Bose, 98-105, the IEEE Press Selected Series (1979).

[2] N. Abramson, "A class of systematic codes for non-independent errors," IRE Trans., vol. IT-5, 150-157 (1959).

[3] T. Kasami, "Systematic codes for non-independent errors," J. Info. Processing Soc. Japan, vol. 1,132-137 (1960).

[4] T. Kasami, “Systematic codes using binary shift register sequences,” J. Info. Processing Soc. Japan, vol. 1, 198-206 (1960).

[5] T. Kasami, “A topological approach to construction of group codes,” J. Inst. Elec. Commun. Engrs. (Japan), vol. 44, 1316-1321 (1961).

[6] T. Kasami, “Optimum linear finite-dimensional estimator of signal waveforms,” IRE Trans., vol. IT-7, 206-215 (1961).

[7] T. Kasami, “Cyclic codes for burst-error-correction,” J. Inst. Elec. Commun. Engrs. (Japan), vol. 45, 9-16 (1962).

[8] T. Kasami, “Optimum shortened cyclic codes for burst-error correction,” IEEE Trans. vol. IT-9, 105-109 (1963).

[9] T. Kasami and K. Torii, “A syntax-analysis procedure for unambiguous context-free grammars,’’ J. ACM, vol. 16, 423-431 (1969).

[10] W. W. Peterson and E. J. Weldon, Jr., Error-Correcting Codes, 2nd ed., MIT Press (1972).

[11] W. W. Peterson and E. Prange, “Symmetry properties of some extended cyclic codes," Summaries of Papers presented at ICMCI, Tokyo, Japan (1964), and W. W. Peterson, “On the weight structure and symmetry of BCH codes,” J. Inst. Elec. Commun. Engrs. (Japan), vol. 50, 1183-1190 (1967) (and also Sec. 8.11 in [10]).

[12] Theorem 8.16 in [10].

[13] F. J. MacWilliams and N. J. A. Sloane, The Theory of Error-Correcting Codes, North-Holland (1977).

[14] Sec. 5.2 in [13].

[15] T. Kasami, “Weight distribution formula for some classes of cyclic codes,” Coordinated Sci. Lab., Univ. Illinois, Urbana, Tech. Rep. R-285, April 1996, and also in T. Kasami, S. Lin, and W. W. Peterson, “Some results on cyclic codes which are invariant under the affine group and their applications,” Info. and Control, vol. 11, 475-496, (1967).

[16] E. R. Berlekamp, Algebraic Coding Theory, McGraw-Hill, 1968.

[17] Theorem 16.34 in [16].

[18] T. Kasami, “Weight distribution of Bose-Chaudhuri-Hocquenghem codes,” Coordinated Sci. Lab., Univ. Illinois, Urbana, Tech. Rep. R-317, Aug. 1966 (also in Combinatorial Mathematics and Its Applications, Univ. of North Carolina Press, 1969). Reprinted in Key Papers in the Development of Coding Theory, ed. E. R. Berlekamp, 268-274, IEEE Press (1974). Also, Sec. 16.4 in [16].

[19] R. Gold and E. Kopitzka, “Study of correlation properties of binary sequences,” Interim Tech. Rep. 1, vols. 1-4, Magnavox Res. Lab., Torrance, CA (1965).

[20] D. V. Sarwate and M. B. Pursley, “Crosscorrelation properties of pseudorandom and related sequences,” Proc. IEEE, vol. 68, 593-619 (1980).

[21] N. J. A. Sloane and E. R. Berlekamp, “Weight enumerator for second-order Reed-Muller codes,” IEEE Trans., vol. IT-16, 745-751 (1970).

[22] T. Kasami and N. Tokura, “On the weight structure of Reed-Muller codes,” IEEE Trans. vol. IT-16, 752-759 (1970). Also, Theorems 10 and 11 in Sec. 15.3 of [13].

[23] T. Kasami, N. Tokura and S. Azumi, “On the weight enumeration of weights less than 2.5d of Reed-Muller codes,’’ Info. and Control, vol. 30, 380-395 (1976).

[24] T. Sugita, T. Kasami and T. Fujiwara, “The weight distribution of the third order Reed-Muller codes of length 512,” IEEE Trans., vol. IT-42, 1622-1625 (1996).

[25] G. D. Forney, Jr., “Coset codes-part II: Binary lattices and related codes,” IEEE Trans., vol. IT-34, 1152-1187 (1988).

[26] T. Kasami, T. Takata, T. Fujiwara and S. Lin, “On the optimum bit orders with respect to the state complexity of trellis diagrams for binary linear block codes,” IEEE Trans., vol. IT-39, 242-245 (1993).

[27] V. K. Wei, “Generalized Hamming weights for linear codes,” IEEE Trans., vol. IT-37, 1412-1418 (1991).

[28] T. Kasami, T. Sugita and T. Fujiwara, “The split weight (w_L, w_R) enumeration of Reed-Muller codes for w_L + w_R 2d_min,’’ Proc. of AAECC, Lecture Notes in Computer Science (Springer), 197-211 (1997).

[29] T. Kasami, T. Koumoto, T. Fujiwara, H. Yamamoto, Y. Desaki and S. Lin, “Low weight subtrellises for binary linear block codes and applications,” IEICE Trans., vol. E80-A, 2095-2103 (1997).

[30] Eq. (7) in Sec. 13.5 of [13].

[31] Sec. 13.5 of [13].

[32] Theorems 9.4 and 9.5 in [10] (also in T. Kasami, S. Lin and W. W. Peterson, “New generalizations of the Reed-Muller codes part I: primitive codes,” IEEE Trans., vol. IT-14, 189-199, 1968. Reprinted in, “Algebraic coding theory: History and Development,’’ ed. I. F. Blake, 323-333, Benchmark Papers in Electrical Eng. and Comput. Sci., Dowden, Huthinson & Ross Inc., 1973.)

[33] T. Kasami and S. Lin, “Some results on the minimum weight of primitive BCH codes,” IEEE Trans., vol. IT-18, 824-825 (1972).

[34] T. Fujiwara, H. Yamamoto, T. Kasami and S. Lin, “A trellis-based recursive maximum likelihood decoding algorithm for binary linear block codes,’’ IEEE Trans. vol. IT-44, 714-729 (1998).

[35] T. Kasami, H. Tokushige, T. Fujiwara, H. Yamamoto and S. Lin, “A recursive maximum likelihood decoding algorithm for some transitive invariant block codes,” IEICE Trans. vol. E81-A, 1916-1924 (1998).

Conference Calendar

DATE	CONFERENCE	LOCATION	CONTACT / INFORMATION	DUE DATE
July 11-16, 1999 :	5-th International Symposium on Communication Theory and Applications (ISCTA'99)	Charlotte Mason College, Ambleside, Lake District, UK	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	
August 2–13, 1999	Workshop on "Codes, Systems and Graphical Models"	Minneapolis, Minnesota, USA	http: / / www.ima.umn.edu / csg	
September 22-24, 1999	37-th Annual Allerton Conference on Communication, Control, and Computing	Monticello, Illinois, USA	37-th Annual Allerton Conference Coordinated Science Laboratory University of Illinois 1308 W. Main Street Urbana, Illinois 61801-2307 USA Email: allerton@csl.uiuc.edu Web: http: / / www.comm.csl.uiuc.edu / allerton /	July 14, 1999
November 9-12, 1999	DIMACS Workshop on Codes and Association Schemes	DIMACS Center, Rutgers University, Piscataway, NJ, USA	Alexander Barg Lucent Technologies Email: abarg@research.bell-labs.com Simon Litsyn Tel Aviv University Email: litsyn@eng.tau.ac.il Web: http: / / dimacs.rutgers.edu / Workshops / AssociationSchemes /	
November 9-13, 1999	The Third International Conference on Distributed Computer Communication Networks (DCCN'99)	Tel Aviv, Israel	Dr. Nina Bakanova Fax: (7 095)-209-0579 Email: nina@iitp.ru Web: http: / / www.iitp.ru / dccn	June 5, 1999
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	
November 30-December 3, 1999	1999 Symposium on Information Theory and Its Applications (SITA'99)	Niigata, Japan	SITA'99 Secretariat Department of Electrical Engineering Nagaoka University of Technology Nagaoka, Niigata 940-2188, Japan Tel: +81-258-21-4263 Fax: +81-258-47-9500 Email: sita99@comm.nagaokaut.ac.jp Web: http: / / comm.nagaokaut.ac.jp / SITA99 /	September 5, 1999

Conference Calendar

DATE	CONFERENCE	LOCATION	CONTACT / INFORMATION	DUE DATE
June 25-30, 2000	I**SIT 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 Tel: +39 011 5644030 Fax: +39 011 5644099 Web: http://www.unisa.it/isit2000	September 15, 1999
March 26-30, 2000	IEEE INFOCOM 2000	Tel Aviv, Israel	Web: http://www.comnet.technion.ac.il/infocom2000 (Israel) http://www.cse.ucsc.edu/~rom/infocom2000 (USA) http://halo.kuamp.kyoto-u.ac.jp/~infocom (Japan)	July 1, 1999

IEEE

Information Theory Society Newsletter

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