IEEE Information Theory Society Newsletter

Vol. 49, No. 4, December 1999 Editor: Kimberly Wasserman ISSN 1059-2362

Reflections on the 1998 Information Theory Society Paper Award: Bits through Queues

Venkat Anantharam (Berkeley) and Sergio Verdú (Princeton)

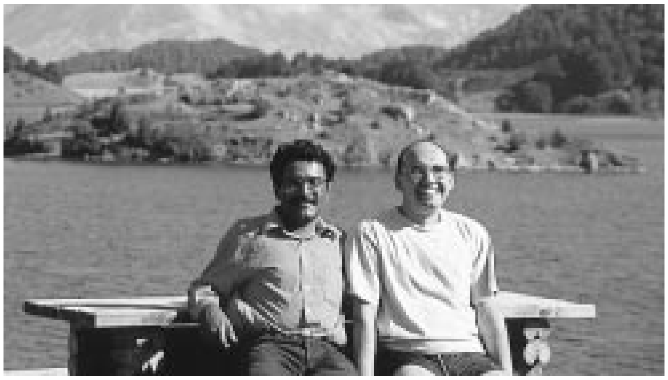


Photo Credit: David Tse

Venkat Anatharam and Sergio Verdú.

I. Love Letters In Empty Envelopes

Information can be sent in the timing of messages, in addition to, or in lieu of, their contents. Granted that the timing of messages may suffer the random whimsies of the postal service, the Internet, or the florist delivery. But if the secret lovers are information theorists, reliable communication in the presence of uncertainty should be more than just a dream.

And while we are at the subject, how about cheating the long distance telephone company: free calls by encoding information in the number of rings and the times between calls.

Timing can indeed be used to subvert security boundaries in a communication network by leaking information through the timing of packets while ostensibly sending only innocuous information. It can also be used to provide hidden channels for collusion among agents involved in a negotiation over a network.

Timing information can also be "piggybacked" on existing communication systems, especially in data networks, acting as a bandwidth-booster.

II. You Gotta Have Nerves

We perceive the world through timing channels. This was established in experiments on the electrical activity of nerve fibers as early as the beginning of the 20th century. Neurons produce spikes and information is communicated through the *timing* of the spikes [2]. For instance when a muscle is stretched with different forces, the firing rate of the neurons in the muscle fiber increases in relation to the applied force. The question of how neurons code complex stimuli into the timing patterns of spike trains is one of the central question of bioinformatics.

A fascinating recent book about the bioinformatic motivation for the study of timing channels is [3]. This book contains a wealth of information about the results of investigations of neural pathways in various animal species. The importance of timing of neural spikes in conveying information is suggested by a number of the experiments described in this book. For instance, many biologically significant sounds have time scales of the order of 5-20 ms during which time at most 1-2 spikes can be produced by a cell firing at 100 spike / sec. Experiments with echo locating bats have shown that they can respond to a single neural spike that appears to occur at a precise time relative to the arrival of the echo. Moths have been shown to exhibit bat-evading behavior on the basis of cries that are only loud enough to produce one or two spikes. There is evidence that only about five spikes suffice for a human being to recognize a face.

Continued on page 21

From the Editor

Kimberly Wasserman

In this issue of the *IEEE Information Theory Society Newsletter*, I hope you'll enjoy the article by Venkat Anantharam and Sergio Verdú on their paper "Bits through Queues," which received the 1998 IT Society Pize Paper Award. There is also an interview with W. Wesley Peterson, winner of the 1999 Japan Prize, conducted by Hideki Imai. I also hope you'll enjoy the columns by IT Society President Ezio Biglieri and Historian Anthony Ephremides, as well as Sol Golomb's puzzle column. In addition, there are announcements of prestigious awards recently won by members of our Society.

We note in sadness the passing of David A. Huffman and Josef Raviv; obituaries can be found on page 6 - 7.

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:

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

Electronic submission, especially, in LaTex, PDF, Postscript, ascii, or Word formats, is encouraged. I may be reached at the following address:

Kimberly Wasserman
Electrical Engineering and
Computer Science Department
1301 Beal Ave.
University of Michigan
Ann Arbor, MI 48109-2122 USA
Tel: +1 (734) 647-3524
Fax: +1 (734) 763-8041
Email: wass@eecs.umich.edu

Kimberly Wasserman

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

W. Wesley Peterson Wins the 1999 Japan Prize

The Science and Technology Foundation of Japan has selected Dr. W. Wesley Peterson as a recipient of the 1999 Japan Prize for his establishment of algebraic coding theory for reliable digital communication, broadcasting, and storage (for more details, refer to the Awards column in *IEEE Information Theory Society Newsletter*, vol. 49, no. 1, March 1999). The Japan Prize, established in 1985, is awarded to people from all parts of the world whose original and outstanding achievements in science and technology are recognized as having advanced frontiers of knowledge and served the cause of peace and prosperity for mankind. Each year, the Science and Technology Foundation of Japan chooses two prize categories, which are information technology and life sciences for 1999. Peterson is the laureate for information technology, and will receive Y 50 million (about US $450,000). The prize was presented in Tokyo on April 28, 1999.

Prof. W. Wesley Peterson. (Photograph presented by courtesy of the Science and Technology Foundation of Japan.)

At the request of the editor, Hideki Imai held the following interview with Wes Peterson in honor of his receipt of the prize.

Hideki: First of all, congratulations with this one of the biggest prizes in science in the world. I hope that this interview gives the IT readers better sense of your personality as well as what you have done in coding theory. You are particularly well known for your book "Error-Correcting Codes," the "bible" for algebraic coding theory, which had a profound effect on the evolution of the fields of digital communication and storage. I myself started my career as a coding theorist by reading this bible. I was deeply impressed by beautiful applications of modern algebra to the very practical development of error-correcting codes. First I would like to ask you, Wes, how did you introduce modern algebra into coding theory and start algebraic coding theory?

Wes: There was algebra-related work on coding in the early 1950's. Golay discovered the code that bears his name in 1949. Hamming's original paper came in in 1950, and later by Reed in 1954 and by Miller in 1954. Slepian's 1956 paper on "Binary Signaling Alphabets" was algebraic. However, the discovery of cyclic codes, to the best of my knowledge by Eugene Prange in 1957, represented a very significant step forward, and with that work in the area increased greatly. Prange knew that Hamming codes and the Golay code could be arranged so that they are cyclic. I would say that Prange's work marked the beginning of what we think of now as algebraic coding theory. I was doing some work with Gene Prange and the Air Force Cambridge Research Laboratories at about that time and when I went to Boston, I often stayed at Gene's apartment. When he showed me cyclic codes, I was very impressed. I was convinced that this was a really important concept. I studied cyclic codes very hard starting probably in 1957, and I understood them really well. However, I found that research very frustrating, because I could prove all the known results in several ways, but I could not find any new results. Many times I gave up, only to start again soon, because I always felt that this was a really important concept. Then in the summer of 1959 I was working at the IBM research laboratories. Professor R.C.Bose came to the labs and gave a lecture about a new class of codes discovered by him and D.K. Ray-Chaudhuri. He could construct t-error-correcting codes for any t, but he couldn't predict exactly how many independent check symbols there were, nor did he know an effective method for error correction. I was prepared — all of my study of cyclic codes finally had some value. I recognized quickly that these were cyclic codes, and as a result I knew immediately how to encode and calculate the parity checks and I know how many independent parity check symbols there were in each code. Quite quickly, I could also find an effective method of decoding. It was a very exciting time for me. After that Professor Bose and I felt quite close. His work and his seminar were very important to me, and my work made his codes important, also.

Hideki: You have also done fundamental work on hardware detection of errors in arithmetic and in logical operations. Wes, please tell us about error-detection and correction for arithmetic and logical operations.

Wes: I was working at IBM in the summer of 1957. It was known that one could check arithmetic operations using *n mod m* as the check symbol for *n*. For example, a check mod 3 will detect any single error in any digit or carry of an addition. I asked myself, is there any other way to check addition in which the hardware for checking is completely independent of the hardware for adding? It is important that the hardware be independent, so that you know that an error in the hardware cannot affect both the result of the addition and the check symbols in such a way that the error is hidden. I formulated the problem as follows: for each number n, you have a check symbol $c(n)$. Then what is required is that for any two numbers n_1 and $n_{2,}$ the adder calculates n_1+n_2 and the checker calculates

$c(n_1+n_2)$ from $c(n_1)$ and $c(n_2)$. If we name the operation that the checker does \$, then $c(n_1+n_2)$ must equal $c(n_1)\$c(n_2)$. Now we can see that the function *c* is what mathematicians call a homomorphism. Now this is reduced to a problem in mathematics, and it is well known that the homomorphic image of the integers is isomorphic to either the integers or the integers modulo some integer *m*. So the answer is that if you have an adder and a separate checker, the only possible checker is, except for the coding, a *mod m* checker for some choice of *m*, or a duplicate of the adder.

One well-known computer scientist said that this is a very profound and important result. On the other hand, I have been told by several mathematicians that it is completely trivial. I guess the truth of the matter is somewhere in between. After it is formulated as a mathematical problem, it is a trivial mathematical problem, but stating the problem as a mathematical problem is an important step. And the result tells computer engineers something that they did not know.

Now we know about adding. What about other processing that the computer does? Bit-by-bit exclusive-or can be checked using error-correcting codes. Since the exclusive-or of two code words in a group code is also a code word, the parity checks for the exclusive-or sum of the information bits in two code words can be calculated completely independently of the information bits by simply exclusive-or adding the check bits, so this operation can be checked with an independent checker. It is possible to prove that since this is also a homomorphism, the check symbols must be essentially parity checks on the information. I don't believe these results have ever been published.

Next we should consider the computer bit-by-bit or and and instructions. I thought about this some and could find no way to check either or or and simpler than to duplicate the hardware for processing a full word. One day I described what I knew about checking an adder and my lack of progress in finding analogous results for and and or to Michael Rabin. He said, it must be possible to check and and or— they have good algebraic properties. However, the next day he came in with a proof that you could not check and or or more simply than by duplicating the hardware for processing a full word.

Hideki: Although it is not widely known in the coding theory community, you made a great contribution to psychology. This is an unexpected application of a theory to a totally different area. Could you talk about the application of signal detection theory to psychology?

Wes: When I was a graduate student, my dissertation research concerned vacuum tubes, but in addition I worked on another project sponsored by the U.S. Army Signal Corps. On this project, I worked with Ted Birdsall and Bill Fox on the problem of optimum signal detection in radar. We wrote a paper entitled "The Theory of Signal Detectability." The paper was quite badly written — obviously the work of some graduate students — but the content was OK. That may be the first place where the parameter E / N_0 (ratio of signal energy to noise power per unit bandwidth) appeared. For some reason that I could never fully understand, the project director hired a psychology graduate student, Wilson P. Tanner. We called him Spike. He was interested in detection of weak stimuli by humans. He had heard about Shannon's work — this was soon after Shannon's book was published. He came to me and to Ted many times and said "I want to apply Shannon's theory to detection of stimuli by humans." and we would say, "Shannon's theory doesn't fit. It doesn't address that problem." Finally one of us (I don't remember which) said to Spike, "Why don't you try using the theory we have developed for radar?" He agreed, so we helped Spike design some experiments.

Traditionally, there were two kinds of experiments in the field. There were yes-no experiments, where the subject sometimes was presented with a stimulus, and sometimes not, and the subject had to tell whether the stimulus was present or not. The other common format was to present the subject with a stimulus in one of several places, and the subject was to determine which place. There was debate about which method was valid.

We designed experiments of both kinds. Spike chose hearing a weak signal in a background of white noise. In the multiple-choice experiment, the signal was presented at one of four times. In the yes-no experiments, the time when the signal might appear was known to the subject. Of course, the ability to detect depended on the signal-to-noise ratio, or more precisely, E / N_0. If we assume a value for E / N_0, then we could predict the error probability for an optimum detector for either kind of experiment. For most of Spike's experiments, he would do a yes-no experiment and use the results to estimate E / N_0, assuming the human did optimum detection. Then he would predict the error probability for the multiple-choice experiment and compare that with the actual measured results. The results were remarkable, more consistent than any other existing psychological data. Spike submitted a paper to *Psychological Reviews*. It was recognized as a very important piece of work and published immediately. Now this is considered to be a seminal piece of work in Cognitive Psychology, one of the reasons that Cognitive Psychology exists today. At this point in time, graduate students in cognitive psychology are required to read our paper on signal detectability because it is considered fundamental in their field. I feel sorry for them.

Spike's dissertation advisor had just completed a treatise on threshold detection and Spike's work made this obsolete. The advisor couldn't accept that and refused to accept Spike's work. To make a long story short, it was about ten years before Spike was awarded a Ph.D. degree, in spite of the importance of his work. Several students working under him, notably John Swets and Dave Green, received Ph.D.'s before he did.

Hideki: On April 29 I organized an academic discussion meeting entitled "Theory of Error-Correcting Codes: Its Past and Future" as an important event of the Japan Prize week.

At that meeting you met more than twenty representative coding theorists in Japan. Please give me some comments on coding theory in Japan.

Wes: There have been important contributions to coding theory by Japanese from the beginning, and interest in the subject seems to be increasing. There was an impressive collection of research presented at our technical discussion, and certainly some of that work is of very high quality. There have been several times in the past when the general feeling among information theorists that coding theory was dead — all of the solvable problems has been solved and the problems that remain unsolved were too hard to be solved. Each time this proved to be not true. Someone solved a new, important problem, and this resulted in new life for coding theory. It is clear that coding theory is not dead now, and in particular, not dead in Japan now.

Hideki: You have lived in Hawaii for a long time. What bought you to Hawaii and how are you enjoying Hawaiian life?

Wes: I came to Hawaii because I felt that I could continue to teach and do research here, and I could enjoy outdoors and the ocean all year long. I have been able to do research here. There have been some very good opportunities. However, what has become most important to me is the mixture of eastern and western culture. My students are a very diverse group. There are more oriental students than Caucasian students, and there are many foreign students as well as local students. I enjoy working with all of them. And of course, my wife is Japanese and she has contributed a great deal to my wonderful life.

Hideki: You are a very fluent speaker of Japanese. You gave your speech at the Japan Prize award ceremony partly in Japanese and it was really impressive and moving. How did you learn Japanese?

Wes: In 1962 when I was at the University of Florida, I applied for a Fulbright grant to go to Japan and then I found several Japanese people there in Gainsville who were willing to help me start learning Japanese. There were Tokuji Suzuki, who recently retired from Chiba University, his wife Ayako, and Norihito Tambo, who is now president of Hokkaido University. I actually worked in Taiwan in 1963-64, but I visited Japan three times that year and met Tadao Kasami at that time. I continued to study Japanese a little, and then I decided to take a sabbatical in 1971 and go to Japan to work with Dr. Kasami. When I was studying Japanese in preparation for that, I met my wife Hiromi. I think the question is, with all those opportunities, why don't I know Japanese much better than I do? I wish I had studied Japanese more, but of course my research and teaching have had a higher priority than learning Japanese.

Hideki: Finally, I would like you to give some advice to young scientists in the information technology area.

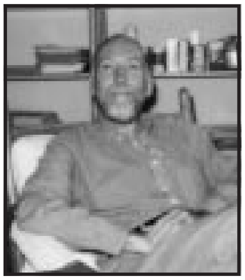
Wes: I have no profound ideas. I would say to them simply to always learn more and more, and always look for good problems to try to solve. My experience is that you have to be well prepared for your research, and a little lucky, to find a good problem and a solution to it. If you are well prepared and always studying and looking for good opportunities, eventually you will be lucky.

Hideki: Thank you very much for your time. I hope that you will enjoy good health for many years to come and participate in the Honolulu Marathon Race every year. I also hope that you will visit Japan again and again.

Wes: Thank you. I most certainly will visit Japan often and I will look forward to seeing you again.

Awards

Kees A. Schouhamer Immink Wins the AES Gold Medal



The Board of Governors of the Audio Engineering Society (AES) has named Kees A. Schouhamer Immink, the recipient of the AES Gold Medal with the following citation: "For a career of major contributions to consumer-electronics digital audio equipment." The AES Gold Medal is AES's highest medal presented for a career of meritorious achievement in audio engineering. Kees Immink was born in Rotterdam, the Netherlands, on December 18, 1946. He obtained M.S. and Ph.D degrees at the Eindhoven University of Technology. He is, since 1995, an adjunct professor at the Institute for Experimental Mathematics, Essen University, Germany.

Bin Yu elected Fellow of the Institute of Mathematical Statistics

Bin Yu, member of the Board of Governors of the IT Society, has been elected Fellow of the Institute of Mathematical Statistics, ‘’in recognition of contributions to the development, dissemination and application of mathematical statistics;" in particular, for her “important wide-ranging research contributions in empirical processes, information theory, genetics, Markov chain Monte Carlo, data compression, and density estimation.”

She joins several distinguished contributors to Information Theory who have achieved this distinction in the past, e.g. David Blackwell, Leo Breiman, Thomas Cover, Robert Gray, Thomas Kailath, David Slepian and Moshe Zakai. Bin Yu is affiliated with the Mathematical Sciences Center of Bell Laboratories-Lucent Technologies, on leave from the University of California, Berkeley.

Hideki Imai Receives Honorary Ph.D.

Prof. Hideki Imai of the University of Tokyo, Japan, received the honorary degree of Ph.D from Soonchunhyang University, Korea, for his significant contributions to promoting research in communications and information security both in Japan and Korea. The award ceremony was held in Soonchunhyang University on August 9th, 1999, with the attendance of Dr. Chun Soo Lee, the President of Soonchunhyang University, Prof. Man Young Rhee, the Ex-President of Korea Institute of Information Security and Cryptology, the Deans, and the Secretary-General. This is the twelfth honorary Ph.D degree of Soonchunghyang University.

David A. Huffman, Computer Expert, Dies at 74

David A. Huffman, who developed a fundamental mathematical technique in the early years of computer science that remains vital to data storage and transmission, died this past October in a hospital in Santa Cruz, Calif. He was 74 and lived in Santa Cruz. He died after a ten-month battle with cancer, his family said.

Huffman developed the Huffman Coding Procedure, the result of a term paper he wrote while a graduate student at the Massachusetts Institute of Technology in the 1950’s. The procedure assigns strings of 0’s and 1’s to each character in a file so that the length of the string depends on the frequency with which the character appears in the file. It provides a way to compress data files so they occupy a smaller amount of electronic memory. Referred to by computer scientists as Huffman Codes, the method is a fundamental component of an undergraduate computer science curriculum and is widely used, not only for the compression of text, image and audio files, but also for the management of files in large computer systems and for the compression of data for transmission by fax machines, modems and high-definition television broadcast.

A native of Ohio, Huffman earned a B.S. in electrical engineering from Ohio State University at the age of 18. After serving in the Navy, he earned his master’s degree from Ohio State and his Ph.D. from M.I.T. In 1967, after 14 years on the M.I.T. faculty, he moved to the University of California at Santa Cruz as the founding faculty member of the computer science department. He played a pivotal role in the development of the department’s academic programs and the hiring of its faculty, and served as chairman from 1970 to 1973.

“David Huffman alone gave the place credibility,” said Patrick Mantey, dean of engineering at the Santa Cruz campus. He retired in 1994, but as a professor emeritus continued to teach and meet with students until recently.

This year, Huffman received the Richard W. Hamming Medal from the Institute of Electrical and Electronics Engineers in recognition of his exceptional contributions to information sciences, but he was too ill to accept the award in person.

Over his career, Huffman did seminal work in many areas of computer science. After studying the properties of certain mathematical surfaces, he began a longtime hobby of bending paper and vinyl into convoluted forms considered by many to be works of art. His work was exhibited several times, most recently at the Xerox Palo Alto Research Center in October 1998.

“The essence of Huffman was to take the complex and make it gorgeous,” said Peter Neumann, a computer scientist at SRI International in Menlo Park, Calif.

Huffman was also an outdoor enthusiast who enjoyed hiking and traveling and kept poisonous snakes as pets. He qualified as a scuba diver when he was close to 70 years old.

Huffman is survived by his wife, Marilyn, of Santa Cruz; his brother, Donald Huffman of Westerville, Ohio; two daughters, Elise and Linda Huffman, both of Santa Cruz; a son, Stephen, of Santa Cruz; a stepdaughter, Marti Homer Kehlet of Sacramento, Calif.; a stepson, Darin Homer of Prunedale, Calif., and two stepgrandchildren.

Obituary Josef Raviv, 1934 - 1999

Dr. Josef Raviv, the IBM scientist, IEEE Fellow, and member of the IEEE Information Theory Society, who founded and led the company's research activities in Israel for more than 25 years, died in an auto accident this past October while vacationing on the South Island of New Zealand.

Raviv, 65, his wife Joanna, and a longtime friend, Prof. Kurt Weiser, a microelectronics materials expert at the Technion's Microelectronics Research Center in Haifa, Israel, were killed after their car hit a bridge and fell into Jacob's River, south of the Fox Glacier near the island's west coast.

Dr. Raviv is widely regarded as a pioneer of the Israeli hi-tech industry. He helped establish the concept of linking industrial research to the marketplace more than 25 years ago, when he led IBM's research activities as head of the IBM Israel Scientific Center, which was established in Haifa in 1972. When the Scientific Center became the Haifa Research Laboratory in 1982, Raviv served as its first director. While the scientific center began with just three researchers, IBM's Haifa Research Lab today employees 300 employees and 100 students and is its largest research lab outside the U.S. Earlier this year, Raviv was name Director of the newly formed Haifa Development Center within IBM's Technology Group.

Born in Poland in 1934, Raviv moved to Israel when he was four years old. After finishing gymnasium (high school) in Tel Aviv, he studied at Stanford University in California (B.S. 1955; M.S. 1960, both in electrical engineering), and at the University of California-Berkeley (M.A. 1963 in mathematician sciences; Ph.D. 1964 in electrical engineering and computer sciences). He then joined IBM's T.J. Watson Research Laboratory in Yorktown Heights, New York.

A 1974 technical paper ("Optimal Decoding of Linear Codes for Minimizing Symbol Error Rate") he co-authored provided the basis for a key algorithm (known as the "backward / forward" algorithm) that helped enable computers to understand a human's natural language, translate between languages and synthesize speech. Last year in honor of the 50th anniversary of the formulation of Information Theory, the IEEE Information Theory Society selected Raviv's paper to receive one of 15 Golden Jubilee Paper Awards to honor "outstanding papers...whose impact...is now widely recognized."

Raviv was president of the Israel Association for Information Processing (1986-90) and received its Lifetime Achievement Award in 1995. He was elected Fellow of the IEEE in 1990 and was Governor of the International Council for Computer Communications (1985-96). He published numerous paper and received eight patents.

Raviv was a member of the board of directors of two companies, Elbit Medical Imaging and Softel, and served on the board of the University of Haifa. He was also the founding Professor and one of the heads of the Hebrew University Engineering School and was serving as the chairman of its international and national advisory board.

The Ravivs are survived by three children and six grandchildren.

President's Column

Ezio Biglieri

In his September column our historian Anthony Ephremides argued, in his usual ornate tones and with more than a whiff of irony, that the invention of telecommunications should be ascribed to the ancient Greeks. Leaving irony aside, one could say even more: that the Greeks invented science altogether. This, at least, is what Alan Cromer, a scientist and an educator, claims in his book "Uncommon Sense: The Heretical Nature of Science" (1993). Science, he argues, did not arise as a natural and inevitable end-product of our innate intelligence and curiosity, but rather as a historical accident, the invention of a particular culture in a unique historical and political period. We may take democracy for granted in our time, but it is in fact a rare event in human history: it existed for less than two centuries in Athens and in a small number of Greek states, to resurface in the Western world more than two millennia later. In the political meetings of democratic Athens men learned for the first time to persuade each other by rational arguments: hence, scientific thinking, which is analytic and objective, owes to the Greek democratic penchant for dialogue and debate (and the brilliance of Euclid, Archimedes, *et al.*). Contrasting the Greek practice of debate to other cultures' reliance on prophets for acquiring knowledge, Cromer contends that, had it not been for the Greeks, we might still be animists or dependent on religious prophets for our cosmology and cosmogony. It was the rebirth of Greek science in the Renaissance, combined with the age of exploration and Gutenberg's invention of movable type, that generated Copernicus, Galileo, and Newton, and created today's world dominated by science and technology.

The idea that direct democracy generated science is indeed an intriguing one: but the point I would like to stress in this column is that the opposite is also true. That is, the understanding of science is a powerful tool to foster democracy by shaping people's ability to participate actively to public decisions. This is true not only when it comes to, say, shutting down a nuclear reactor for safety reasons or choosing whether or not to import genetically engineered steaks, but also, in a less direct way, in order to promote rational skepticism against public gullibility. People who believe weird things — mind reading, abduction by extraterrestrials, and the like — are more likely to be attracted by phony leaders and phony ideologies. Now, almost every modern irrationalism can be defeated by elementary scientific tools, when well applied.

A subtler reason for promoting understanding of science is that its status as a repository of "objective truth" may transform the scientist in the modern equivalent of a prophet. A person not versed in science is likely to rely uncritically on the opinion of self-proclaimed "scientists" to delegate decisions that have a bearing on everybody, and to believe in ideas that woo our trust by donning scientific garb. Moreover, "if one is accustomed to not understanding everything oneself but knowing that others do understand — for how else could they have produced these technological miracles? — then one will demand certainty and guarantees also where one cannot properly expect them — in the sphere of decisions of meaning and values." (see Ruediger Safranski, "Martin Heidegger," 1998, p. 91).

Postscript: This is my last column for this Newsletter. By January 1, 2000 Vijay Bhargava, a scholar and a bon vivant, will take over as the next President of the Society. The other newly elected BOG officers, Joachim Hagenauer (First Vice-President) and Tom Fuja (Second Vice-President) will collaborate with Vijay to provide competent leadership next year. You can see them in action at the Board of Governors meetings scheduled for year 2000, the first at the Princeton Conference this March, then at the annual Information Theory Symposium in Sorrento, Italy, and then in Honolulu, at ISITA2000. I wish you all Happy Holidays and a Happy New Year!

The Historian’s Column

A. Ephremides

In the early days of its development, Information Theory carried a much broader perceived content than it does today. In fact, it was Claude Shannon himself who admonished the community to “take it easy”, so-to-speak, and to scale back its imagination concerning the bold interpretations that were being offered for the “meaning” of Information Theory in diverse fields like biology, cybernetics, physics, and the like. Today, we may be experiencing a “rebirth” of the tendency to expand the principles of Information Theory beyond the narrow confines of Communication. As part of the gold jubilee celebrations in 1998, seven experts reviewed and documented the impact of Information Theory on such fields as Economics, Complexity, Signal Processing, Physics, etc. It may be argued that this “rebirth” is more sound, cautious and secure, than the euphoric and expansive boldness of the early years.

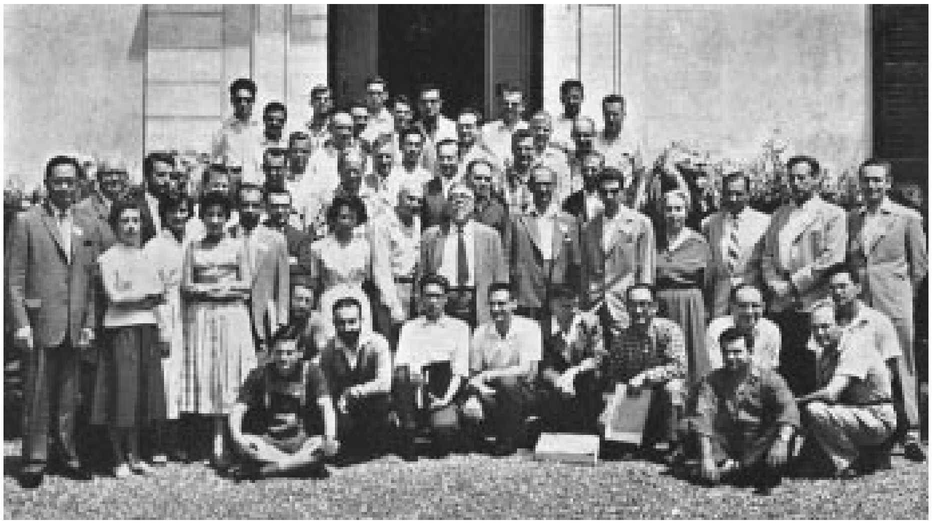
These thoughts came to my mind as I was perusing a splendid document from that early period. It is the “Supplemento” of the publication “Nuovo Cimento” of the Italian Society of Physics (No. 2, third trimester of 1959, Vol. XIII, Series X). It contains the proceedings of a very unusual meeting, called a “course”, that took place in the Villa Monastero of Varenna in Northern Italy in 1958 from July 7 to July 19. This was the seventh such “course” of the International Summer School of Physics at Varenna, and the first ever on Information Theory. It consisted of a series of lectures and seminars delivered by a distinguished group of twenty-eight (28) “docents” to a group of only thirty one (31!) students. These must have been very privileged students indeed. They were mostly Italian and amongst their names I was not able to recognize any who made a subsequent career in Information Theory.

The list of “docents”, or lecturers, was an impressive “who’s who” at the time. It was headed by Norbert Wiener (who, as the “course” Director Eduardo Caianiello stated in his opening remarks, was elected by acclamation Permanent Chairman of the meetings at Varenna) and it included W. Davenport, R. Fano, D. Huffman, B. McMillan, D. Slepian, P. Green, F. Stumpers, as well as renowned people from other fields like linguists M. Halle and B. Mandelbrot, psychologists E. Newman and G. Moruzzi, biologists W. Reichardt, B. Hassenstein, V. Baitenberg, Computer Scientist L. Lofgren and others.

Director Caianiello referred to the field of Information Theory as the mathematical foundation of Cybernetics. And the contents of the lectures ranged from what is now understood as “mainstream” Information Theory to truly adventuresome topics (from an Information Theoretic viewpoint) such as “Men and Information,” “Morphology of Nerve-nets”, “Non-biological Filters,” “Nervous Center of Insect Eyes,” “Statistical Macro-linguistics,” etc., etc.

To give you a flavor of the level of development of the field at that time let me quote from D. Slepian’s lecture on Coding Theory (you can spot David at the extreme right of the second row from the top in the photo, due northeast from Norbert Wiener in the epicenter). After thanking McMillan and Fano who gave lectures based on Shannon’s 1948 paper, he observed that the portion of the theory they discussed was by then rather fully developed. And he said, in vintage Information-theoretic style, that “Drs. McMillan and Fano have been kind enough to leave for me to discuss that part of the theory about which no one knows anything. I can, therefore, safely feel well qualified to speak”! That was Coding Theory at the time; haven’t we gone a long way since then?

There is so much to report from that meeting that I will have to resort to future columns to do justice to it. Unlike other events, however, which I have had the fortune to attend (and, hence, be able to offer a more personal view of them), this “course” was before my time (in this sense, it is “pre-history”) and I will have to rely on the information in the Nuovo Cimento proceedings. Thus, there will be no anecdotes from the human interactions side of the event. The recorded material itself, however, is a goldmine. And we will sample its nuggets in due time.



Attendees of 7th Course of International Summer School of Physics at Varenna. (From “Supplemento”, Volume 13, Series X, “Nuovo Cimento”, No. 2, 1959.

Minutes of the June 20, 1999 Meeting of the Board of Governors of the IEEE Information Theory Society

by Greg Pottie

Board Members Present: E. Biglieri, A. Ephremides, T. Ericson, M. Fossorier, T. Fuja, J. Hagenauer, J. Huber, S. Verdú, A. J. H. Vinck, F. Willems, R. Yeung

Others Present: H. Ferreira, D. Neuhoff, B. Rimoldi, M. Varanasi, A. Vardy

1. The meeting was called to order at 9:20 AM and introductions were made.

2. The agenda was approved.

3. The minutes of the 2/27/99 BoG meeting were approved.

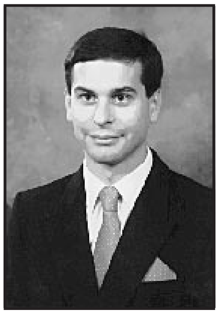
4. Dave Neuhoff announced that an ad hoc committee chaired by Neuhoff has been investigating the possibility of erecting a statue or plaque in honor of Claude Shannon in Gaylord, Michigan. Artist Eugene Daub has been contacted and has provided some samples of his work as well as some preliminary sketches. Following the committee's recommendation, the BoG set a provisional limit of $35,000 (including the cost of the base and transportation). The committee (Neuhoff, Costello, Fuja, and McLaughlin) will remain intact and will present one or more alternative designs before the BoG meeting in Fall 1999. The committee was also encouraged to contact other parties who may be potentially interested in a Shannon plaque/statue - e.g., AT&T, Lucent, the University of Michigan, MIT, etc.

Ezio Biglieri made the following announcements:

- James Massey recently received the 1999 Marconi International Fellowship Award.
- Robert Gallager recently received the 1999 Harvey Prize.
- Encyclopaedia Britannica is currently revising its entries related to electronics and electro-technology. IEEE has been asked to identify members who may be well-suited to participating in this revision, and IEEE has passed the request along to the societies.
- The book version of the 50th-anniversary Transactions will be in production in July.

5. Reports were heard regarding IT awards.

- J. Hagenauer presented the recommendation of the Award Committee regarding the 1999 IT Prize Paper Award; only one paper was forwarded by the Awards Committee for the BoG's consideration. The BoG accepted the Committee's recommendation; a ballot will be mailed out to the BoG members, who will vote on the nominee, There was some discussion of the number of people on the committee and the timing of the nominations. It was recommended that the article of the Society bylaws dealing with the IT Prize Paper Award be revised in the sense of allowing a wider range of competence in the selection committee.



- IEEE is giving each Society the opportunity to nominate a fixed number of people for a "Third Millenium Award" - to be given "For outstanding contributions to the Society or its area of technology." An IT Society nomination committee will be established and the following three criteria (equally weighted) will be used in making nominations: 1. Quality and quantity of research publications in our field. 2. Editorial service to the Society as Editor-in-chief of the Transactions and/or as associate editor. 3. Service to the IT Society as exemplified by service as a Society officer, as a member of the Board of Governors, and/or as an organizer of an ISIT and/or IT Workshop. The nomination committee will consist of the current president (chair), the two most recent past presidents, the two vice presidents, and the Editor-in-Chief of the IT Transactions.
- The 2000 Claude E. Shannon Award Committee consists of Joachim Hagenauer (chairman), Vijay Bhargava, Ezio Biglieri, Jim Massey, and David Forney.
- The IEEE Communications Society has agreed to establish a new Joint Paper Award with the IT Society to promote and recognize work done in the areas of intersection between the two societies. The BoG agrees in principle with the draft proposal prepared jointly by Ezio Biglieri on behalf of the IT Society and Lin-shan Lee on behalf of the ComSoc. The Awards Committee will formulate a set of rules to be approved at the September BoG meeting. The bylaws of the IT Society will also be suitably modified.

6. The following people were nominated to stand for election to the BoG for a three-year term starting in 2000: Tom Hoholdt, Michael Honig, Torleiv Klove, Ryuji Kohno, Amos Lapidoth, Prakash Narayan, Joseph O'Sullivan, Robert McEliece, Ramesh Rao, Han Vinck, Victor Wei, and Steve McLaughlin.

7. Han Vinck made a report on behalf of the Ad Hoc Committee on IT Book Translations; some publishers have been contacted and have expressed interest in publishing Society-subsidized English translations of important information theory books not currently available in English. Han was encouraged to select one book as a "test case" and see what kind of deal can be worked out with a publisher.

8. Marc Fossorier presented the treasurer's report. Among the items in the report:

- The Society had a net worth of $1,555,520 as of 30 April 1999. This included $1,148,370 in long-term investments and $305,780 in cash equivalents.

- On November 30, 1998 the cash equivalents held by the Society was only $42,630. (This was before the '99 dues and subscriptions began to come in.)
- Regarding the financial records of Society-sponsored meetings:
  - The financial records of the 1998 Information Theory Workshop held in San Diego are closed. There was a surplus of $3,469.
  - The financial records of the 1998 Information Theory Workshop held in Killarney are being prepared. There will be a deficit of $1,252 due to currency fluctuations.
  - The financial books of the 1998 ISIT in Boston have been submitted and are under review.
- The BoG voted to keep the non-member subscription price at $445, declining to increase it to $550 as suggested by IEEE. The BoG asked Fossorier to prepare detailed recommendations regarding the Society budget for 2001 and regarding the balance of long-term funds versus cash-equivalents - taking into account the low level of cash available at the end of 1998 and the potential need to increase subscription prices.

9. Alex Vardy presented the Editor's Report for the Transactions. Among the items in the report were these:

- The two special issues are going forward - one on "Information Theoretic Imaging" and another on "Codes on Graphs and Iterative Algorithms".
- Over the last three months, 40% of the papers submitted to the Transactions on Information Theory were submitted electronically,
- A second Publications Editor was approved - Erik Agrell of Chalmers University; a budget of $10,000 to support Agrell was also approved. This position is in addition to the Publications Editor position held by Ramesh Rao of UCSD.

10. A report from Web Editor Ramesh Rao was distributed.

- A request for $2000 per year to maintain web access to the IT Digital Library was approved, as was an additional $3000 to be held in reserve for hardware repairs / replacement.
- A request for $2000 per year to obtain .pdf copies of the IT Newsletter for display on the web page was approved.

11. Thomas Ericson delivered a report from the ad hoc committee on electronic publishing and asked that BoG members provide input to the committee on this rapidly-changing and very important subject.

12. Tom Fuja introduced a succession of reports on Society-sponsored meetings.

- Hendrik Ferreira reported on the South African workshop. There were (approximately) 115 registrants and financially the workshop appears to be on-track to breaking even. The BoG thanked the organizers of the workshop for their excellent job.
- Tony Ephremides indicated that the Metsovo workshop is on track.
- Prakash Narayan delivered a status report on the planning of the 2001 ISIT to be held in Washington DC. The ISIT will be held June 24-29. The organizers have decided to use IEEE Travel and Conference Management Services for a number of functions (e.g., registration, budgeting, facility management, etc.) at a cost of $9,500. Hotel negotiations with the Omni Shorehamn are currently under way. There was some discussion of the use of a large Technical Program Committee - i.e., approximately 70 members; it was agreed that this was an experiment with a new approach and the results will be assessed.
- Bixio Rimoldi made a presentation proposing the 2002 ISIT be held in Lausanne, Switzerland; the co-chairmen would be Rimoldi and Jim Massey and the technical co-chairs would be Amos Lapidoth and Emre Telatar. The BoG voted to approve Lausanne as the 2002 site. This was done with the understanding that the proposal to hold ISIT 2002 in Japan - which was discussed at the February 27, 1999 BoG meeting - had been withdrawn due to potential conflicts with the 2002 World Cup, also to be held in Japan. The BoG asked that the Japan organizers be encouraged to submit a proposal for 2003 or 2004.

13. The BoG acted on several requests for co-sponsorship of meetings:

- A request from Vijay Bhargava for co-sponsorship of the IEEE International Conference on Personal Wireless Communication to be held December 2000 in Hyderabad, India was considered. The Board voted to offer "Technical Co-Sponsorship" and will consider co-sponsorship at the next BoG meeting if a conference budget is available.
- The Board declined to provide financial support for the International Conference on Distributed Comupter Communication Networks (DCCN '99), to be held in November 1999 in Israel. This decision was made in light of longstanding BoG policy that conferences should be self-supporting and the belief that DCCN '98 seemed to be marginal to the interests of the Society.
- The Board voted to offer Technical Co-Sponsorship to the organizers of the 3rd ITG Conference on Source and Channel Coding, to be held January 2000 in Munich.

14. Joachim Hagenauer presented a brief report from the Membership and Chapters Committee. It was noted that IEEE membership went up approximately 5% last year, while IT Society membership has gone down. The BoG members were asked to consider ways that this trend might be reversed.

15. The following names were placed in nomination for Society officers for 2000:

- Vijay Bhargava for President.
- Joachim Hagenauer for First Vice-President.

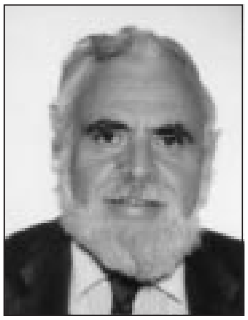
The nominees for each of the above offices were unanimously approved by the BoG. The nominations for Second Vice President were not complete at the time of the meeting and will be handled by mail before the Chicago meeting.

16. The meeting was adjourned.

Golomb's Puzzle Column^{TM} Number 48:

Solving for the Unknowns

Solomon W. Golomb



1. There were n players in a round-robin chess tournament (i.e. each player was paired with every other player exactly once). As is customary in chess tournainents, the winner of each game got one point, and the loser got 0 points; in case of a draw, each player got ½ of a point. Two of the players were masters, and they completed the tournament with respective total scores of 3 points and 4 ½ points. The other $n-2$ players were all grandmasters, and surprisingly they all finished in a tie, each having the same total score as the other GMs. How many players participated in the tournament, and what was the final score of each grandmaster?

2. Five picnickers decided to calculate the sums of their ages two at a time. These ten sums turned out to be 19, 25, 28, 37, 40, 46, 49, 52, 58, and 70. What were their individual ages? (You may assume that all ages are whole numbers.)

3. Given that $x(y+z)=A$, $y(x+z)=B$, and $z(x+y)=C$, express x, y, and z explicitly in terms of A, B, and C. (Assume that A, B, and C are positive real numbers.)

4. Suppose that $f(x)=x^n+a_1x^{n-1}+a_2x^{n-2}+\cdots+a_{n-1}x+a_n$ is a polynomial of degree $n>3$ with real coefficients, having roots $a_1, a_2, \ldots, a_\mathrm{n}$. Let $S_t=\sum_{j=1}^{n}\alpha_j^t$ for $t = 1, 2, 3, \ldots$. Express S_1, S_2, and S_3 explicitly in terms of the coefficients of $f(x)$.

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 Fellow

The grade of Fellow is the highest membership grade in the IEEE. The Information Theory Society has many distinguished members who are potential candidates for this honor. Of those members who are evaluated by the IT Society, a good percentage are usually elected.

Fellow elections reflect honor not only on the individuals elected but also on the Society as a whole, and the Board of Governors advocates an aggressive search for nominations. The Society also has an interest in identifying candidates from historically underrepresented subfields, regions, and institutions.

The basic qualification for election to Fellow is "unusual distinction in the profession." About 250 IEEE members are elected each year. A list of the 1999 class of IEEE Fellows appeared in the January 1999 issue of *The Institute*, and can also be accessed through the IEEE Website (http://www.ieee.org/awards/).

Preparation of the nomination form is important. Any person may serve as nominator (except IEEE staff or volunteers involved in the Fellow selection process). The basic responsibility of the nominator is to prepare a complete and accurate four-page nomination form that clearly identifies the unique contributions of the candidate. The other principal task of the nominator is to obtain the agreement of five to eight IEEE Fellows who are qualified to judge the candidate's work to serve as references.

Detailed instructions and forms may be found in the IEEE Fellow Nomination Kit, which may be obtained from the IEEE homepage at http://www.ieee.org/awards/table1.htm. Hardcopy may be requested by sending email to fellow-kit@ieee.org. Email inquiries about the Fellow process may be addressed to fellows@ieee.org.

Vincent Poor (email: poor@princeton.edu) is Chair of the IT Fellow Evaluation Committee and is also available for help.

The deadline for the nomination form and all reference letters is March 15, 2000. Your Society asks you to:

- Think about identifying a qualified candidate;
- Ask for a Fellow nomination kit;
- Get started early!

Encore, Encore! ISIT'98 Scoops the Opera World

Those who were fortunate enough to attend the closing ceremonies of the IEEE International Symposium on Information Theory (ISIT'98) in Cambridge, MA, in August 1998, witnessed a diva in the making. Barbara Quintiliani, a 22-year-old soprano from Boston, who graduated in May 1999 from the New England Conservatory, performed at ISIT'98 at the invitation of Dave Forney, Anthony Ephremides, Ezio Biglieri, and Sergio Verdú. The program of the evening included arias by Quintiliani, a rendition of a composition by Ephremides of the poem "Casey at Bat," and a canconetta "Torna a Sorriento."

In August 1999, Quintiliani won the prestigious Marian Anderson International Vocal Competition at the Kennedy Center Concert Hall. The prize includes $20,000 and concert engagements throughout the United States. This is the second major competition Quintiliani has won this year, the other being the national finals of the Metropolitan Opera Auditions, which awarded five winners prizes of $16,000 each. Quintiliani is currently singing roles with the Boston Lyric Opera, and will be doing further auditions at the Met later this year. Evidently, Information Theory is a vehicle for excellence in many different endeavors!

Workshop Report:

Information Theory and Networking Workshop

Metsovo, Greece,
June 27 — July 1, 1999

The 1999 Information Theory and Networking Workshop took place from June 27 to July 1st, 1999 in the beautiful mountain village of Metsovo in northwestern Greece. Metsovo perched in the magnificent mountain range of Pindos at an altitude of 1115 meters offered a tranquil and comfortable environment for the workshop. Metsovo is not far away from Meteora area. Many attendees took the opportunity to visit these famous monasteries.

The workshop itself was located in the new Metsovo conference center that is managed by members of Averov family, a very prominent Greek family. The workshop was organized by Anthony Ephremides (U. Maryland), Leonidas Georgiadis (U. Thessaloniki), Philippe Jacquet (INRIA), Wojciech Szpankowski (Purdue U.), and Apostolos Traganitis (U. Crete) who was a local organizer. The organizers received a generous help from the session organizers: A. Anantharam, C. Cachin, C. Courcoubetis, D. Forney, I. Kontoyiannis, N. Merhav, A. Lapidoth, B. Prabhakar, R. Rao, G. Seroussi, L. Tassiluas, D. Tse, H. van Tilborg, A. Vardy, M. Weinberger, Z. Zhang. There were three plenary speakers: John Kieffer talked on universal data compression via grammatical inference, P. Flajolet presented tools to analyze digital search trees and other data structures that often arise in information theory, and P. Varayia spoke about the pricing problem of modern communication networks. Finally, there were three panels (two on networking and one on multimedia), recent result session and a poster session. The organizers and participants seem to enjoy a lively discussion during the panels and the poster session.

More than 80 participants attend the workshop. It started with a reception, and ended with a banquet during which folklore bands and participants enjoyed traditional Greek dances. The final visit to Zagorohoria region offered a very appreciated relaxation moment after the successful meeting.

The technical program follows:

Monday June 28

PLENARY SPEAKER
John Kieffer
Universal Lossless Data Compression via Grammatical Inference.

NETWORKS AND SHANNON THEORY
Organizers: A. Lapidoth and Z. Zhang

Toby Berger:
Tight Typicality and the Generalized Billiard Ball Channel

Thomas M. Cover:
Conflicts between state information, side information and intended information.

Te-sun Han:
Weak variable-length source coding theorems

S. Shamai and Emre Telatar:
Some information theoretic aspects of decentralized power control in multiple access fading channels

S. Verdu:
Capacity of CDMA Fading Channels
(Joint work with S. Shamai)

R. Yeung:
Linear codes for network information flow
(joint work with S.-Y. Robert Li)

COMMUNICATION / CODING

Organizers: D. Forney, A. Vardy.

Tom Hoeholdt:
Advances in algebraic-geometry codes

Claude Berrou:
Multidimensional turbo codes

Ralf Koetter:
Factor graphs and iterative decoding

Dan Costello:
On the packet error rate performance of convolutional codes

Ronny Roth:
Constrained codes and systems

PANEL: ROLE OF IT in MULTIMEDIA
Panelists: Jacov Ziv and N. Farvardin

Tuesday June 29

PLENARY SPEAKER
Philippe Flajolet:
Analytic Aspects of the Digital Tree Process

SOURCE CODING
Organizers: Y. Kontoyiannis and N. Merhav

Tamas Linder and Ram Zamir:
High-Resolution Rate-Distortion Theory

Gil Shamir and Daniel J. Costello:
Asymptotically Optimal Threshold Based Low Complexity Sequential Lossless Coding for Piecewise Stationary Memoryless Sources

Tjalling Tjalkens and Frans Willems:
Variable-to-Fixed length source codes: a geometrical approach to low complexity codes

S. Savari:
Variable-to-fixed length codes and plurally parsable dictionaries.

Bin Yu and Mark Hansen:
Assessing MDL in Wavelet Compression and Denoising

FUNDAMENTALS OF COMMUNICATION NETWORKS

Organizers: L. Tassiulas

C. Courcoubetis, V. Siris and R. Weber:
Cell and Burst Scale Effects in Multiplexing Periodic Sources

James Giles and Bruce Hajek:
The Jamming Game for Timing Channels

R. Poovendran, J. S. Baras:
An Information Theoretic Approach to Secure Multicast Key Management

Kihong Park:
Noncooperative network games for multi-class QoS provision

PANEL: ROLE OF IT IN NETWORKING

Organizers: R. Rao and T. Ephremides

Panelists: Venkat Anantharam, Toby Berger, Bob Gallager, Bruce Hajek, Jack Wolf

Wednesday June 30

PLENARY SPEAKER

Pravin Varaiya:
Pricing and Provisioning of Quality-Differentiated Interent Access.

CRYPTOGRAPHY AND INFORMATION SECURITY

Organizers: Henk van Tilborg and C. Cachin

Henk van Tilborg:
Survey on Cryptography.

Don Beaver:
Imperfections in Perfectly Secure Key Exchange

Christian Cachin:
Security Against Memory-bounded Adversaries,

Claude Crepeau:
Cryptography in the Quantum World.

IT AND QUEUEING NETWORKS

Organizers: V. Anantharam and D. Tse

Bob Gallager and Balaji Prabhakar:
The Entropies of Queue Arrivals and Queue Departures

Lewis, J.T. Pfister, C.-E., Sullivan, W.G.:
Information Theory and Large Deviation Theory

George Kesidis and Takis Konstantopoulos:
Extremal behavior and bounds for a network buffer fed by deterministically shaped random processes

Balaji Prabhakar:
A two-bit scheme for address lookup

PANEL: PRICING IN NETWORKS

Organizers: C. Courcoubetis and B. Prabhakar:

Panelists: John Tsitsiklis, Pravin Varaiya, Richard Weber.

RECENT RESULT SESSIONS

“On the design of Space-Time codes,’’ H. El Gamal.

“On the modified Niederreiter cryptosystem,’’ E. Gabidulin, A. Ourivski, V. Pavlouchkov.

``Performance of the turbo hybrid automatic repeat request system type II,’’ Jozef Hamorsky, Lajos Hanzo.

``Constructing low parity-checkcodes with circulant matrices,’’ S. Hui, J. Bond, H. Schmidt.

``Representing group codes as permutation codes,'' J. Karlof, E. Biglieri, E. Viterbo.

``Strong converse theorems in the quantum information theory,'' Tomohiro Ogawa Hiroshi Nagaoka.

``Traffic multiplexing networks,'' M. Shalmon.

``Overflow and underflow probabilities of fixed-to-variable codeword lengths for general sources,'' O. Uchida, T. Han.

``Interleaver design for turbo codes based on divisibility,'' M. Wang, A. Sheikh, F. Qi.

``Basic properties of fix-free codes,'' R. Yeung, C. Ye.

``Noise prediction for channels with side information at the transmitter: error exponents,'' R. Zamir, U. Erez.

POSTER SESSION

``A combinatorial approach to information inequalities,'' H. Chan, R. W. Yeung.

``On a BEP of a generalised concatenated code,'' X. Feng.

``An information-spectrum approach to degraded broadcast channels,'' K. Iwata, M. Morii.

``Asymptotic properties on codeword length distribution of FV codes for general sources,'' H. Koga, H. Yamamoto, N. Yamaguchi.

``Near optimal voice-data integration over third generation wireless TDMA channel,'' P. Koutsakis, M. Paterakis.

``Algorithms for finding good column permutation of codes,'' C. Papadopoulos.

``Stack algorithms for random multiple access in the presence of asymmetric channel feedback erasures,'' M. Paterakis, C. Harizakis.

``Zigzag codes and concatenated Zigzag codes,'' Li Ping,

Nam Phamdo.

``The behavior of stochastic process arising in window

protocols,'' S. Savari, E. Telatar.

``Efficient hierarchical broadcasting using multilevel codes,'' D. Schill, D. Yuan, J. Huber.

``A separation principle of communication network,'' L. Song, R. Yeung.

``The kth order nonhomomorphicity of S-boxes,'' Y. Zheng, X. Zhang.

``Multiparty videoconferencing on multi-drop VP based SONET-ATM rings performance analysis,'' G. Feng, T. Yum.

``The method of statistical hypothesis testing based on stochastic polynomial use,'' Y. Kuchenko.

Symposium Report

Fifth International Symposium on Communication Theory and Applications

Ambleside, Lake District, UK
11-16 July 1999

The fifth International Symposium on Communication Theory and Applications was held at the Charlotte Mason College, Ambleside, in the English Lake District, from Sunday 11th July until Friday 16th July, 1999. The Symposium was supported by the Communications Research Centre of the University of Lancaster, the Institute of Integrated Information Systems of the University of Leeds and HW Communications Ltd, and was sponsored by the IEE and the IEEE Communications and Information Theory Chapters (UKRI Section).

The first Symposium took place at the Crief Hydro, Crief, Scotland in 1991, but all subsequent symposia have been at Ambleside, a venue which both new and regular participants seem to be very pleased to visit. The scenery is magnificent (whatever the weather!), and can be enjoyed by everyone at all levels from hiking to sightseeing. On this occasion the weather was kind to us, and on the free Wednesday afternoon groups of participants were able to climb several peaks, including Blencathra, Helm Crag and Steel Fell.

The technical programme was equally varied and interesting, with four days of sessions on a range of topics (see list below). It is a feature of these Symposia that most sessions are plenary, which the delegates find makes for good discussion and cross-fertilisation of ideas. Only four sessions were presented in parallel, in two pairs. An innovation on this occasion was a special invited session on Digital Broadcast Below 30MHz, organised by Prof. Dr. Jurgen Lindner (University of Ulm, Germany), a rapidly developing topic of much current interest. A total of 77 papers was presented, of which 13 were invited (see list below), and in addition there was a general interest evening talk by Dr. Mark Rayne (SIMOCO Europe Ltd, UK) on Tetra Mobile Communications for Professionals. About 90 delegates attended, from 20 different countries, making about 120 participants in all when including relatives and friends. A reception on the Monday evening, a barbecue and ceilidh band on the Wednesday evening and the banquet on the Thursday evening completed the programme.

Copies of the Proceedings of the Symposium (£50) can be obtained from Jayne Chippendale, CRC, Department of Communication Systems, Faculty of Applied Sciences,

Speech by Paddy Farrell.

University of Lancaster, Lancaster LA1 4YR, UK. A book containing about half of the presentations is in the process of being published by Research Studies Press, a division of Wiley.

Organising Committee

Prof. L. W. Barclay, Lancaster University, UK

Prof. M. Darnell, University of Leeds, UK

Prof. P. G. Farrell, Lancaster University, UK

Prof. B. Honary, Lancaster University, UK

Prof. J. Lindner, University of Ulm, Germany

Dr. G. Markarian, NDS Ltd, UK

Mr. M. Maundrell, DERA Malvern, UK

Prof. R. J. McEliece, Caltech, USA

Prof. S. Wicker, Cornell University, USA

Sessions

Error control Coding (4 sessions)

Posters (2)

Modulation, Detection and Synchronisation (3)

Mobile Systems (1)

Networks and Protocols (1)

Digital Broadcast Below 30MHz (2)

Source Coding (2)

Modelling and Simulation (1)

Signal Processing (2)

Code Division Multiple Access (1)

Sequences (1)

Security (1)

Celida band.

Invited Presentations

D. Mackay (Cambridge, UK): Gallager Codes: Recent Results

Y. Kaji, E. Kasai (Nara, Japan), T. Fujiwara (Osaka, Japan), T. Kasami (Hiroshima, Japan): Suboptimum Decoding Based on the Recursive Maximum Likelihood Decoding Algorithm

R. Y. Shao, S. Lin, M. Fossorier (Hawaii, USA): Decoding of Tailbiting Codes

M. Blaum, B. Kabelac, S. Hetzler (IBM Almaden, USA): An Efficient Method for Servo-ID Synchronization with Error-Correcting Properties

S. Coffey, H. Chen (Michigan, USA): Bit Error Probability and Encoder Structure, and the First Iteration in Decoding

I. Dumer (Riverside, USA): Decoding of Reed-Muller Codes on Pascal Triangles

M. E. Buckley, S. Wicker (Cornell, USA): Neural Networks for Predicting Turbo Decoder Error and Convergence

A. Mason, G. Markarian, K. Pickavance, S. Waddington (NDS, UK): Channel Coding in Digital Video Broadcasting: State-of-the-Art and Future Developments

A. Khandekar, R. J. McEliece, E. Rodemich (Caltech, USA): The Discrete Noiseless Channel Revisited

V. C. da Rocha (Pernambuco, Brazil): Some Information-Theoretic Aspects of Uniquely Decodable Codes

T. Gneiting, H. Khakzar (Stuttgart, Germany): Modelling and Simulation of High Pincount Connector Systems

V. Levenshtein (Academy of Sciences, Russia): Graph-Theoretical Approach to Efficient Reconstruction of Sequences

E. M. Gabidulin, A. V. Ourivski (Moscow, Russia): Improved GPT Public Key Cryptosystems

Scientific Meeting Report

German IEEE Chapter on Information Theory Meeting on "Developments in Information and Communication Theory"

Essen, Germany
September 16 -17, 1999

This scientific meeting was organized by the Ph.D. School "CINEMA" in cooperation with the IEEE German Chapter on Information Theory at the Institute for Experimental Mathematics, IEM, in Essen. An international audience of 40 researchers participated. The meeting contained the following contributions:

Dirk Timmermann, University of Rostock, Germany
Current Developments in VLSI-Design and in Hardware Verfication

Olaf Drögehorn, University of Duisburg, Germany
Translation of formal cTLA+ - specifications in VHDL based on formal semantics transformation

Vijay Barghava, University of Victoria, Canada
Code Division Multiple-Access for Satellite Communication

Peter Gober, IEM, University of Essen, Germany
Coding for the M-Frequency Multiple-Access Channel

Vladimir Balakirsky, St. Petersburg, Russia
A Direct Approach to Searching with Lies

Hendrik Ferreira, Rand Afrikaanse University of Johannesburg, South Africa
Markov Models for GSM-channels

Martin Bossert, University of Ulm, Germany
Overview on Concatenated Coding

Christoph Haslach, IEM, University of Essen, Germany
Array Codes based on Interleaved Linear Block Codes

Peter Sweeney, University of Surrey, U.K.
Watermarking and Encryption for Digital Video

Bernhard Dorsch, University of Mannheim, Germany
Coding for DS - CDMA - Systems

A.J. Han Vinck, IEM, University of Essen, Germany
Recent Results on Powerline Communications

Peter de With, University of Mannheim, Germany
Picture Coding Algorithms and their Implementation

Hui Li, University of Duisburg, Germany
Multiscale Matching Pursuit Application for Image Compression

Rolf Johannesson, University of Lund, Sweden
Something on Convolutional Codes

Tadashi Wadayama, University of Okayama, Japan
Trellis-Based Algorithms for Performance Analysis on Bounded Distance

Vijay Bhargava presenting a lecture on access techniques.

Hendrik Ferreira presenting a certificate to Han Vinck during the banquet.

During the banquet Vijay Bhargava and Hendrik Ferreira honored the chairman Han Vinck with a certificate for his contributions to the developing countries in Africa and Asia. The organizers of the workshop succeeded in creating ideal circumstances for an inspiring workshop which offered many possibilities for informal discussions. After the workshop the participants took the opportunity to visit a "classical" German chemical industry and to taste the local products. For more information, please contact the workshop chairman: Han Vinck, vinck@exp-math.uni-essen.de.

Call for Papers – ISITA2000

The 2000 International Symposium on
Information Theory and its Applications
Sheraton Waikiki Hotel, Honolulu, Hawaii, U.S.A.
November 5–8, 2000

http://isita2000.soft.iwate-pu.ac.jp/

Sponsored by *the Society for Information Theory and Its Applications*
With the technical co-sponsorship of *the IEEE Information Theory Society* and
the IEICE Fundamentals on Information and Communication Sub-Society

International Advisory Committee

Chair
Hideki Imai

Members
Behnaam Aazhang
Tomonori Aoyama
Suguru Arimoto
Shigeru Asakawa
Andrew R. Barron
Vijay K. Bhargava
Ezio Biglieri
A. Robert Calderbank
Agnes Chan
Chin-Chen Chang
Michelle Effros
Anthony Ephremides
Thomas Ericson
Thomas R. Fischer
Tom Fuja
Jerry D. Gibson
Joachim Hagenauer
Bruce Hajek
Te Sun Han
Hiroshi Harashima
Chris Heegard
Shigeichi Hirasawa
Yasuo Hirata
Kazuo Horiuchi
Kees A. Schouhamer Immink
Yoshihiro Iwadare
Fumio Kanaya
Masao Kasahara
Tadao Kasami
Saleem A. Kassam
Kwok-Yan Lam
Steven W. McLaughlin
Hector Perez Meana
Urbashi Mitra
Sang Jae Moon
Katsuhiro Nakamura
Masao Nakagawa
Greg Pottie
Ramesh Rao
Shojiro Sakata
Shlomo Shamai (Shitz)
Paul H. Siegel
Hatsukazu Tanaka
Saburo Tazaki
Henk Van Tilborg
Shigeo Tsujii
Vijay Varadharajan
Sergio Verdu
Stephen B. Wicker
Guozhen Xiao
Serena Zabin

Symposium General Chairs
Shu Lin
Eiji Okamoto

Technical Program Committee

Chairs
Toru Fujiwara
Marc Fossorier

Members
Martin Bossert
Joseph Boutros
Chi-chao Chao
Michelle Effros
Tom Fuja
Atsushi Fujioka
Johannes Huber
Hiroyuki Inaba
Makoto Itami
Keiichi Iwamura
Hajime Jinushi
Ralf Koetter
Hiroki Koga
Toshiyuki Kohnosu
Mao-Chao Lin
Wei Lin
Andi Loeliger
Upamanyu Madhow
Toshiyasu Matsushima
Steven McLaughlin
Misa Mihaljevic
Urbashi Mitra
Robert Morelos-Zaragoza
Masakatsu Morii
Wai Ho Mow
Jun Muramatsu
Toshihiro Niinomi
Masayoshi Ohashi
Yasutada Oohama
Steven Pietrobon
Takahiko Saba
Kazue Sako
Hiroshi Sasano
Iwao Sasase
Tomoharu Shibuya
Patrick Solé
Hisashi Suzuki
Joe Suzuki
Oscar Takeshita
Ichi Takumi
Toshio Tokita
Kin-ichiroh Tokiwa
Tomohiko Uyematsu
Mahesh Varanasi
Emanuele Viterbo
Koichiro Wakasugi
Lei Wei
Isao Yamada
Hirosuke Yamamoto
Raymond Yeung
Ken Zeger
Yuliang Zheng

Treasurer
Kaoru Arakawa
Shoichiro Yamasaki

Local Arrangement
Marc Fossorier

Publicity
Toyoo Takata

Registration
Kazuhiko Yamaguchi

Secretariat
Atsuko Miyaji
Kanta Matsuura

The first International Symposium on Information Theory and its Applications (ISITA) was held in Honolulu in November 1990. Ten years later, the sixth ISITA symposium is back to its birthplace, in conjunction with the 2000 IEEE International Symposium on Intelligent Signal Processing and Communication Systems (ISPACS 2000, http://www.mk.ecei.tohoku.ac.jp/ISPACS2000/).
Authors are invited to submit original papers to the 2000 International Symposium on Information Theory and its Applications, to be held in Honolulu, Hawaii, U.S.A., November 5–8, 2000.

Categories of Interest include (but are not limited to) the following:

- Error Control Coding
- Communication Systems
- Detection and Estimation
- Spread Spectrum Systems
- Signal Processing
- Source Coding
- Neural Networks
- Data Networks
- Data Security
- Chaos and Fractals
- Coded Modulation
- Optical Communications
- Mobile Communications
- Pattern Recognition
- Speech/Image Processing
- Shannon Theory
- Distributed Information Networks
- Stochastic Processes
- Cryptography
- VLSI Communications

Important Dates

- Extended summaries due: March 15, 2000
- Notification of acceptance: June 1, 2000
- Camera ready papers due: August 1, 2000

Author Information

Prospective authors should submit 5 copies of an extended summary (500–1000 words) of their manuscript by postal submission. Also, it is preferable to send an email containing the title of the paper, and the authors' names and affiliation at the address: *isita@basyou.ics.es.osaka-u.ac.jp*.
The details of the submission will appear in the web page of the symposium by the end of 1999. The manuscripts should be submitted to:

Prof. Toru Fujiwara
Department of Informatics and Mathematical Science
Graduate School of Engineering Science
Osaka University
1-3 Machikaneyama, Toyonaka, Osaka 560-8531 JAPAN
E-mail: *fujiwara@ics.es.osaka-u.ac.jp*

For further information please contact

Prof. Eiji Okamoto
Center for Cryptography, Computer and Network Security
University of Wisconsin, Milwaukee
Milwaukee, WI 53201, U.S.A.
Tel: +1-414-229-5731 Fax: +1-414-229-6958
E-mail: *okamoto@cs.uwm.edu*

2000 IEEE INTERNATIONAL CONFERENCE ON PERSONAL WIRELESS COMMUNICATIONS (ICPWC'2000)

December 17–20, 2000 Grand Kakatiya Sheraton Hotel, Hyderabad, India

Sponsored by IEEE AES/COM/LEOS India Council Chapter
Co-sponsored by: IEEE Hyderabad Section and IEEE Information Theory Society

It is our pleasure to invite you to the Fifth IEEE International Conference on Personal Wireless Communications, to be held in Hyderabad, India. The climate in December will be warm and comfortable.

It is estimated that 40% to 60% of the future telephones in India will be based on wireless technologies, not including the demands from mobile communications. Their successful deployment will require the cooperation of a host of players such as wireline, wireless and satellite providers, manufactures and researchers. Therefore the scope of ICPWC'2000 encompasses but is not limited to:

- Narrow-/Broadband Mobile Radio
- Wireless Local Loop: LMDS/LMCS, MMDS
- Mobile and Personal Satellite Communications
- CDMA and Related Techniques
- Internet and IP for Wireless
- Fixed and Mobile Convergence
- RF and Spectrum Issues
- Coding, Modulation and Equalization
- Wireless Network Architectures
- Adaptive and Intelligent Antennas
- IMT - 2000 Deployment
- Software Radios

In addition to technical presentations, panel discussions and pre-conference short courses by leading authorities in the field are planned. Please submit a 300 word summary by **June 15, 2000** to:

In India
Dr. Kumar Sivarajan
Indian Institute of Science
Dept. of Electrical Communications Engineering
Bangalore, India 560 012
Tel: +91-80-309-2658 Fax: +91-80-334-7991
E-mail: kumar@ece.iisc.ernet.in

Outside India
Dr. Rajamani Ganesh
Network Planning and Engineering
GTE Laboratories Inc.
40 Sylvan Road Waltham, MA 02451-1128 USA
Tel: +781-466-3275 Fax: +781-466-2846
E-mail: rganesh@labs.gte.com

Notification of acceptance or rejection will be sent by **July 15, 2000**. Accepted papers will be published by the IEEE in the conference Proceedings. A camera-ready version of the paper must be received by **August 30, 2000**. Corporations desiring to sponsor conference exhibition: please read the ICPWC'2000 Patron Program on the World Wide Web or contact any one of the following:

Dr. Vijay K. Bhargava
Dept. of Elec. & comp. Eng.
University of Victoria,
P.O. Box 3055, STN CSC
Victoria, BC, Canada V8W 3P6
Tel: +1-250-721-8617
Fax: +1-250-721-6048
E-mail: bhargava@ece.uvic.ca

Dr. Ram Gopal Gupta
Dept. of Electronics,
Govt. of India
6 CGO Complex, Lodhi Road
New Delhi 110 003 India
Tel: +91-11-436-3095
Fax: +91-11-436-3079
E-mail: guptarg@xm.doe.ernet.in

Dr. Ramjee Prasad
Aalborg University
Institute of Electronic Systems
Fredrik Bajers VEJ 7A5
DK-9220 Aalborg, Denmark
Tel Sec.: +45-9635-8671
Fax: +45-9615-1583
E-mail: prasad@cpk.auc.dk

http://www.citr.ece.uvic.ca/icpwc2000

Conference Report

First International Conference on Concatenated Codes German Chapter of the IEEE Information Theory Society

Reisensburg Castle, Günzberg Germany
October 3, 1999

The German chapter of the IEEE Information Theory Society hosted its first annual conference on concatenated codes on October 3rd, 1999. The event took place at the medieval castle Reisensburg located in Günzberg, about 40 km outside of Ulm.

Concatenated coding is a technique which combines two or more codes in serial or parallel to give one single overall code. In general, long codes perform well, but suffer from a high decoding complexity. The concatenation paradigm allows individual component codes to be decoded using low complexity methods while still having the advantages of long codes. Some of the topics addressed during the forum included iterative decoding techniques, generalized concatenation, woven codes, and coded modulation.

The conference attracted 40 participants from all over the world including Japan, Italy, Russia, Sweden, Canada, and as far north as Bremen in Germany. Key note speakers included Professor Hagenauer from the Technical University of München, Germany, Professor Benedetto from the Politecnico di Torino, Italy, and Professor Bossert from the University of Ulm, Germany.

The comfortable mileau of Castle Reisensburg, and the relatively small number of participants allowed many opportunities for the personal exchange of information and ideas. It was an excellent conference, and the beginning of a great tradition. Plans are already underway for the next conference in 2000.

Advance Program for the 2000 IEEE International Symposium on Information Theory (ISIT 2000)

Please note that the paper form of the Advance Program of ISIT 2000 will only be mailed to those who submitted a paper. All others may find the relevant information on the Symposium's web site at http://www.unisa.it/isit2000/.

Reflections. . .

continued from page 1

III. La Dolce Vita

The paper "Bits through Queues" is the result of thinking along the preceding lines. Like a lot of research, it is largely "curiosity-driven." We decided to formulate a sharply defined problem about timing channel capacity and attempt to solve it, mostly for the fun of it. Among the random phenomena that blur timing information, queueing is one of the most important, practically and theoretically. Indeed, queues are the fundamental building blocks of packet communication networks. Moreover, with an arrow going in, an arrow going out, and randomness inside, we saw the simple single-server queue as an irresistible Shannon-theoretic target. This was particularly true in the aftermath of [4] which found a non-communication characterization of channel capacity as the rate of random bits that needs to be generated to simulate the output of the system, for any desired input process.

The opportunity for attacking the capacity of the queue presented itself in the Spring of 1992, when one of us (VA) visited the other (SV) on sabbatical leave at Princeton for a couple of months. The rough outlines of the results were clear to us before too long, but nailing down all the details took more time. We retrieved the paper from the back burner with a visit by SV to Cornell in the Summer of 1993 and in March of 1994 the manuscript was ready.

IV. Teorema

Despite its simplicity, the single-server queue quickly showed sharp teeth: nonnegative inputs, infinite memory, nonlinearity, difficult analysis outside the steady-state which the capacity analysis cannot assume, etc. However, we were fortunate to encounter striking parallels between the information theoretic roles of the exponential distribution and the Gaussian distribution. The reversibility of the M/M/1 queue played an important role in guiding our insight and conjectures.

We showed that the capacity of the single-server queue is equal to e^{-1} nats (0.531 bits) per average service time if the server is exponential, and can only be larger for any other service distribution. Thus, the exponential server is the "noisiest" of all. In several ways, exponential is to queuing channels what Gaussian is to additive-noise power-constrained channels. Another result shown in [1] is that even though the queue is a channel with memory, noiseless instantaneous feedback does not improve capacity. If the service rate is μ and the input rate to the queue is constrained to be $\lambda \leq \mu$ arrivals per second, then the capacity is equal to

$$\lambda \log_2 \left(\frac{\mu}{\lambda}\right)$$

bits per second. Thus, the maximum information transfer is achieved at $\lambda = e^{-1}\mu$.

The capacity of the telephone signaling channel and associated problems alluded to in Section I turned out to be much easier to analyze than the queue. In addition to proving the information theoretic results we also carried out an experiment in long-distance telephony, which indicated that AT&T is the right choice when it comes to cheating the phone company.

V. The Six Percent Solution

Network people frequently refer to the service rate μ of the queue as its “capacity.” When we considered information transmission both in packet contents and in timing, we discovered that the capacity of a single-server queue (where bits arrive individually) is equal to at least six percent more than μ, with this lower bound achieved by the exponential server. As the service time becomes less random, the bandwidth-boosting capabilities of timing information grow without bound.

Not only timing information can be used to boost throughput but also to reduce delay. For example, to transmit one bit every $1/\mu$ sec the average queueing delay with timing information is no more than $2/\mu$ sec versus ∞ sec without timing information.

VI. The Sequels

Several papers have built upon “Bits through Queues.” Highlighting the elegant information-theoretic properties satisfied by the exponential distribution, [5] obtained formulas for rate-distortion functions and capacities of several problems dealing with Markov processes. In particular, [5] found a simple rate-distortion function formula for the Poisson process, by introducing a distortion measure different from those considered earlier [6], [7].

The discrete-time counterpart of the single-server channel considered in [1] is a binary asymmetric channel with infinite memory. Its capacity, in the case of geometrically distributed service time with mean $1/\mu$ slots, was shown by Bedekar and Azizoglu [8] (and, independently by Thomas [9]) to equal

$$\log\left(1 + \mu(1-\mu)^{(1-\mu)/\mu}\right).$$

Coding theory for queuing channels is virtually nonexistent. The capabilities of sequential decoding for the exponential server were analyzed in Sundaresan’s dissertation [10], [11] in conjunction with a suboptimal tree code. Another way in which the exponential distribution turns out to play the role of the Gaussian distribution in additive-noise channels is on the issue of decoding robustness. Lapidoth [12] has shown that the maximum-likelihood decoder for the Gaussian channel can still achieve Gaussian capacity in the presence of non-Gaussian noise provided the encoder takes the suboptimality of the decoder into account. Sundaresan [10], [13] obtained parallel results for the exponential-server maximum-likelihood decoder (which selects the message that can be explained with the rninimum sum of service times and no negative service times).

As we may expect from Section I (and will elaborate in VIII), it is natural to consider various jammed timing channels. Information theoretic analysis of those channels has begun along the two classical avenues of arbitrarily varying channels [10], [13] and jamming games [14].

Burke’s output theorem (e.g. [15]) was instrumental in the proof of the main achievability result in [1]. The part of Burke’s theorem that establishes that the equilibrium departure process of a Poisson-driven exponential server is Poisson, can be apparently sharpened using information theory [16], [17] so as to show that the queue is an entropy-increasing operation. However, using the divergence data-processing theorem this is in fact a simple corollary to Burke’s theorem itself. It would be interesting to see if information theory can provide new versions of Burke’s theorem (for other queuing systems).

VII. The Bonfire Of The Vanities

Theoretically important as it is, the exponential service distribution is not as ubiquitous as the Gaussian noise distribution. Indeed, in many cases timing information is worth exploiting only if the sevice times are much less random. [1] gave an upper bound on the capacity of non-exponential servers based on the divergence of the service distribution relative to the exponential. However, general lower bounding techniques are lacking.

Any first course on queueing networks shows that multi-server exponential queues are not much harder to analyze than than single-server queues. That has certainly not proven to be the case regarding their capacity. We know the answer for one server and infinite servers (infinite capacity) but even the capacity of the two-server exponential queue remains unknown. The capacity of a simple tandem of two single-server exponential queues is also unknown. Thus, the capacity region of Jackson networks is nowhere in sight.

The capacity of queues with finite buffers has also proved to be notoriously difficult. In particular the fact that dropped packets translate into deleted codeword symbols makes the problem rather challenging.

We have shown that timing can improve the delay-throughput characteristic substantially, but even for the exponential server we do not know the optimal delay-throughput curve.

VIII. The Silence Of The Lambs

Covert information leakage across security boundaries using timing information is of interest to intelligence, law enforcement, and law-breaking organizations. The signaling channel studied in "Bits through Queues" can be used to model covert information transmission with packets that consist entirely of unclassified material or material that is publicly available (the news, jokes, etc.). There have been past attempts to study the information theoretic capacity of other covert channels. For instance a covert resource scheduling channel has been studied in [18], [19], [20], [21], [22], [23], [24], [25]. In this channel, Clarice shares a resource (say a CPU) with Hannibal. Hannibal never sends information to Clarice directly, but at certain (message-conveying) times Hannibal overloads the resource thus increasing the response time Clarice observes for her own resource requests. The analyses found in the literature are quite restricted in scope, as they assume that the channel will be used by Hannibal and Clarice in a very simple manner: all Clarice can do is to determine if the response to her requests is "slow" or "fast". This simplification leads to the "timed channel" discussed in [20], [21]. Analysis of the capacity of a covert channel associated to an acknowledgement-based communication protocol is carried out in [26], [27]. The focus is on reducing the capacity of this channel by introducing a buffer of fixed size in the ack channel from Hannibal to Clarice. In this channel, Hannibal leaks information to Clarice by modulating the times at which it releases the acknowledgments to packets sent by Clarice. The buffering scheme serves to reduce the timing channel capacity by releasing acknowledgments to Clarice as a moving average of a fixed number of past acknowledgement times sent by Hannibal. In general it is of great interest to study the tradeoff between network performance and timing channel capacity when re-timing schemes are used to reduce the capacity of covert timing channels.

Fundamental questions regarding the capacity of such timing channels, the extent to which they can compromise the goals of the protocol designed for the interaction between the agents involved (e.g. how much hidden collusion is possible in a negotiation) and of the tradeoffs between timing channel capacity and performance (if mechanisms are implemented to reduce timing channel capacity, how much do they degrade the performance of the network) naturally present themselves to the information theorist.

IX. Final Analysis

We conclude by quoting from the masterful review of the interface between information theory and communication networks [28, p.2429]:

[[1]] may prove to have a catalytical role in creating a common platform for the joint study of information-theoretic and queuing-theoretic systems. It may represent a pivotal moment in the history of the two fields." But more to the point, [28] states:

"Viewing a service system as a channel may prove to be nothing more than a whimsical, cute exercise."

References

[1] V. Anantharam and S. Verdu, "Bits through queues," *IEEE Trans. Information Theory*, vol. 42: (1), pp. 4-18, Jan. 1996.

[2] R. B. Stein, "The information capacity of nerve cells using a frequency code," *Biophysical Journal*, vol. 7, pp. 797-826, 1967.

[3] F. Rieke, D. Warland, R. de Ruyter von Steveninck, and W. Bialek, *Spikes*, MIT Press, Cambridge, MA, 1997.

[41 T. S. Han and S. Verdú, "Approximation theory of output statistics," *IEEE Trans. Information Theory*, vol. 39, pp. 752-772, May 1993.

[5] S. Verdú, "The exponential distribution in information theory," *Problemy Peredachi Informatsii*, vol. 32, no.1, pp. 100-111, Jan. - Mar. 1996.

[6] I. Rubin, "Information rates and data-compression for posson processes," *IEEE Trans. Information Theory*, vol. 20, pp. 200210, March 1974.

[7] R. G. Gallager, "Basic limits on protocol information in data communication networks," *IEEE Trans. Information Theory*, vol. 22, pp. 385-398, July 1976.

[8] A. S. Bedekar and M. Azizoglu, "The information-theoretic capacity of discrete-time queues," *IEEE Trans. Information Theory*, vol. 44: (2), pp. 446-461, Mar. 1998.

[9] J. A. Thomas, "On the Shannon capacity of discrete-time queues," *Proc. 1997 IEEE Int. Symp. Information Theory- Ulm*, p. 333, July 1997.

[10] R. Sundaresan, *Coded Communication over timing channels*, Ph.D. thesis, Princeton University, Princeton, NJ, 1999.

[11] R. Sundaresan and S. Verdú, "Sequential decoding for the exponential server timing channel," *IEEE Trans. Information Theory*, to appear.

[12] A. Lapidoth, "Nearest neighbor decoding for additive non-Gaussian noise channels," *IEEE Trans. Information Theory*, vol. 42, pp. 1520-1529, Sept. 1996.

[13] R. Sundaresan and S. Verdú, "Robust decoding for timing channels," *IEEE Trans. Information Theory*, to appear.

[14] J. R. Giles and B. Hajek, "The jamming game for timing channels," *1999 IEEE Workshop on Information Theory*, Metsovo, Greece, p. 35, June 27-July 1, 1999.

[15] D. Bertsekas and R. Gallager, *Data Networks, Second Edition*, Prentice-Hall, Englewood-Cliffs, NJ, 1992.

[16] R. G. Gallager and B. Prabhakar, "Entropy and the shannon capacity of queueing systems," *1999 IEEE Workshop on*

Information Theory, Kruger, South Africa, p. 1, June 20-25, 1999.

[17] R. G. Gallager and B. Prabhakar, “The entropies of queue arrivals and queue departures,” *1999 IEEE Workshop on Information Theory*, Metsovo, Greece, p. 42, June 27-July 1, 1999.

[18] B.W. Lampson, “A note on the confinement problem,” *CA CM*, vol. 16 (1), pp. 613-615, October 1973.

[19] J.C. Huskamp, *Covert Communication Channels in Timesharing Systems*, Ph.D. thesis, University of California, Berkeley, Berkeley, CA, 1978.

[20] I.S. Moskowitz, S.J. Greenwald, and M.H. Kang, “An analysis of the times z-channel,” *Proceedings of the 1996 IEEE Computer Society Symposium on Security and Privacy*, pp. 2-11, 1996.

[21] I.S. Moskowitz and A.R. Muller, “The channel capacity of a certain noisy timing channel,” *IEEE Transactions on Information Theory*, vol. 38, No. 4, pp. 1339-1344, July 1992.

[22] W.M. Hu, “Reducing timing channels with fuzzy time,” *Proceedings 1991 IEEE Computer Society Symposium on Security and Privacy*, pp. 8-20, 1991.

[23] B. R. Venkatraman and R. E. Newman-Wolfe, “Capacity estimation and auditability of network covert channels,” *Proceedings of the 1995 IEEE Computer Society Symposium on Security and Privacy*, pp. 186-198,1995.

[24] J. W. Gray III, “On introducing noise into the bus-contention channel,” *Proc. 1993 IEEE Computer Society Symposium on Research in Security and Privacy*, pp. 90-98, May 24-26, 1993.

[25] I. S. Moskowitz and A. R. Miller, “The influence of delay upon an idealized channel’s bandwidth,” *Proc. 1992 IEEE Computer Society Symposium on Research in Security and Privacy*, pp. 62-67, May 4-6, 1992.

[26] M.H. Kang, I.S. Moskowitz, and D.C. Lee, “A network pump,” *IEEE Transactions on Software Engineering*, vol. 22, No. 5, pp. 329-338, May 1996.

[27] I.S. Moskowitz and M.H. Kang, “Discussion of a sabbatical channel,” *Proc. 1996 IEEE-IMS Workshop on Information Theory and Statistics*, p. 95, 1996.

[28] A. Ephremides and B. Hajek, “Information theory and communication networks: An unconsummated union,” *IEEE Trans. Information Theory*, vol. 44: (6), pp. 2416-2434, Oct. 1998, Reprinted in “Information Theory: Fifty Years of Discovery,” IEEE Press, 1999.

GOLOMB’S PUZZLE COLUMN^{TM} PUZZLE NO. 47:

Solutions to “Find the Simple Solution”

l. a. Two trains start 100 miles apart, heading toward each other at respective speeds of 60 mph and 40 mph. Clearly they will meet in exactly one hour. A fly travelling back and forth between the two trains at 75 mph, until they meet, will travel exactly one hour, and therefore a distance of 75 miles.

(There is a well-known story that when John von Neumann was first asked some version of this problem, he gave the correct answer very quickly. “Oh, you saw the trick,” said the questioner. “What trick? It was an easy series to sum”, was von Neumann’s reply.)

b. The fly who starts at 50 miles per hour from the front of the train going at 60 miles per hour won’t get very far on his own. Most likely he will be pushed along at 60 mph until the two trains collide an hour later, for a distance of 60 miles rather than 50. (You give this variant to people who are familiar with 1.a. hoping to catch them off guard.)

2. The problem about the fifteen billiard balls is most easily solved by viewing it in reverse. The *last* ball off the table will be either No. 1 or No. 15. The next-to-last ball will also be a binary choice, at either end of the shortened numerical sequence of length 14 (either 1 to 14 or 2 to 15). Proceeding backward, there is a binary choice at each stage, except when only the *first* ball remains, so there are 2^{14} = 16,384 possible sequences.

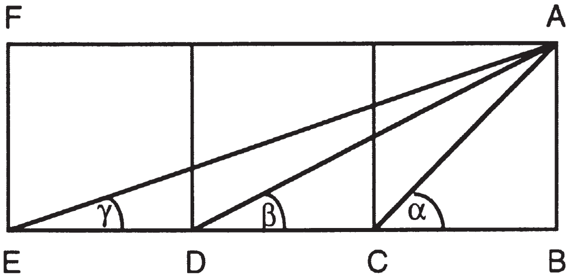
I was first asked this problem by a fellow graduate student at Harvard, around 1952. 1 thought less than half a minute, and answered “2^{14},,. ”Oh, you saw the trick," he said. “What trick?”, I replied. “It’s the sum of the fourteenth row of Pascal’s triangle.” (That’s the solution if you ask how many sequences are there if the first ball to go is No. 1, or No. 2, or No. 3, etc.) For a discussion of different viewpoints that lead to solutions, see “The Problem of the Fifteen Billiard Balls”, S.W. Golomb, *Mathematics Magazine*, vol. 58, no. 3, May, 1985, pp. 156-160.

3. The *average* game lasts *two* tosses, because every game contains *exactly* one "tail" (the game-ender), and the perfect coin produces heads and tails equally often.

The uninspired solution calculates the *expectation* as

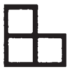
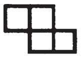
$$\sum_{n=-1}^{\infty} nPr(n) = \sum_{n=1}^{\infty} \frac{n}{2^n} = 2, \text{ using } \sum_{n=-1}^{\infty} np^n = \frac{p}{(1-p)^2}, \text{ evaluated at } p = \tfrac{1}{2}$$

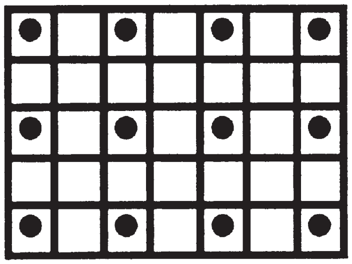
4. The really clever solution (spotted almost instantly by the late Leon Bankoff, the first time he was shown this problem) starts by observing that the triangles ACD and ECA are similar! They have the angle ACE in common, and the including sides, for the smaller triangle, are in the ratio $\overline{AC}/\overline{CD} = \frac{\sqrt{2}}{1} = \sqrt{2}$, and for the larger triangle, in the ratio $\overline{EC}/\overline{CA} = \frac{2}{\sqrt{2}} = \sqrt{2}$. Hence the triangles are similar, and their corresponding angles are equal, so that ∠CAE=β. We have ∠EAF=γ (by alternate interior angles of parallel lines), and ∠FAC=∠BCA=∝ (again by alternate interior angles). Since ∠FAC= ∠FAE + ∠CAE, we have α = γ+β. (This problem appeared many years ago in Martin Gardner's *Scientific American* column, "Mathematical Games".)



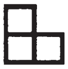
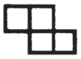
5. We started with 1000 lbs. of watermelons which were 99% water (by weight). That means 1% or 10 lbs., was *not* water. At the destination, water was only 98%, which means that the 10 lbs. of non-water was now 2%, or one-fiftieth, for an ending weight of 500 lbs.

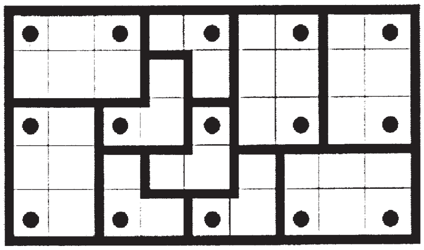
The first guess of most people, on hearing the problem, is 990 lbs., since only 1% was lost". (I learned of this problem from Dick Hess.)

6.a. It is impossible to tile a 5 × 7 rectangle using any combination of the tiling shapes  and . The easy way to see this is to place twelve dots among the 35 squares of the rectangle:

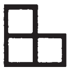


Each tile shape can cover at most one dot, and each tile consists of at least three squares. Since there are twelve dots, and 12 × 3 = 36, the tiles needed to cover all dots have a total area of at least 36, but the area of the rectangle is only 35.

b. For the 5 × 9 rectangle, the same approach places 15 dots, and 3 × 15 = 45, the area of the rectangle. Thus, if a tiling is possible, it must use fifteen of the  -tiles and none of the  -tiles; and each tile used must cover a dot. With these constraints, a successful tiling is not hard to find. (A 2 × 3 rectangle can obviously be



covered using two of the tiles, in either of the two ways.)

This method can easily be used to show that fifteen is the smallest *odd* number of copies of  which will tile a rectangle. (See, e.g., my book *Polyominoes*, Second Edition, Princeton University Press, 1994, especially Chapter 8.) To use the late Paul Erdös's terminology, the simple solutions to this set of problems are almost certainly the ones from The Book.

Conference Calendar

DATE	CONFERENCE	LOCATION	CONTACT/INFORMATION	DUE DATE
January 17-19, 2000	3rd ITG Conference on Source and Channel Coding	Munich, Germany	Joachim Hagenauer Institute for Communications Engineering Technische Universitaet Muenchen D-80290 Muenchen, Germany Web: http://www.LNT.ei.tum.de/itg/itg_main.html	
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)	
June 5-9, 2000	IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP 2000)	Istanbul, Turkey	Conference Management Services 3109 Westchester Ave. College Station, TX, USA 77845-7919 Email: mercer@conf-mgmt.com Web: http://icassp2000.sdsu.edu	

Conference Calendar

DATE	CONFERENCE	LOCATION	CONTACT/INFORMATION	DUE DATE
June 18-19, 2000	7th International Workshop on Algebraic and Combinatorial Coding Theory	Blagoevgrad, Bulgaria	S. M. Dodunekov Institute of Mathematics and Informatics Bulgarian Academy of Sciences 8 G. Bonchev Str. 1113 Sofia, Bulgaria Email: stedo@moi.math.bas.bg	March 31, 2000
June 25-30, 2000	**ISIT 2000**	Sorrento, Italy	Professor Ezio Biglieri Dipartimento di Elettronica Politecnico di Torino Corso Duca Degli Abruzzi, 24 I-10129, Torino, Italy email: biglieri@polito.it Tel: +39 011 5644030 Fax: +39 011 5644099 Web: http://www.unisa.it/isit2000	
March 15-17, 2000	34th Annual Conference on Information Sciences and Systems	Princeton University	CISS 2000 Dept. of Electrical Engineering Princeton University Princeton, NJ 08544-5263 Email: ciss@ee.princeton.edu Web: http://www.ee.princeton.edu/CISS/cfp.html	January 14, 2000
May 15-18, 2000	IEEE Annual Vehicular Technology Conference (VTC2000-Spring)	Tokyo, Japan	Tadashi Matsumoto Secretary for VTC2000-Spring Wireless Laboratories, NTT DoCoMo Tel: +81-468-40-3552 Fax: +81-468-40-3790 Email: matumoto@mars.yrp.nttdocomo.co.jp Web: http://www.convention.co.jp/vtc2000s	
May 22-25, 2000	International Conference on Telecommuncations (ICT 2000)	Acapulco, Mexico	Salvador Landeros Electrical Engineering Division Faculty of Engineering National University of Mexico Mexico City, 04510 P.O. Box 20-694, San Angel Tel: 52(5) 622-3116 Fax: 52(5) 616-1855 Email: roset@speech.fi-p.unam.mx Web: http://telecom.fi-b.unam.mx/ict	December 15, 1999

Conference Calendar

DATE	CONFERENCE	LOCATION	CONTACT/INFORMATION	DUE DATE
November 5-8, 2000	International Symposium on Information Theory and Its Applications (ISITA 2000)	Honolulu, Hawaii	Prof. Eiji Okamoto Center for Cryptography, Computer and Network Security University of Wisconsin, Milwaukee Milwaukee, WI 53201 Tel: +1-414-229-5731 Fax: +1-414-229-6958 Email: okamoto@cs.uwm.edu Web: http://isita2000.soft.iwate-pu.ac.jp/	March 15, 1999

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

Information Theory
Society Newsletter