IEEE Information Theory Society Newsletter

Vol. 49, No. 1, March 1999 Editor: Kimberly Wasserman ISSN 1059-2362

ISIT'98 Plenary Lecture Report: Variations on the Theme of 'Twenty Questions'

Richard M. Karp

Introduction

This article is based on my plenary talk at the IEEE International Symposium on Information Theory held at M.I.T. in August, 1998. The talk concerned a family of identification problems exemplified by the familiar game of Twenty Questions. The article is intended to stimulate interest in the subject by briefly presenting a number of attractive examples; the discussion will be informal, with no claim to rigor or completeness. The literature on this subject is vast, and only a handful of the many relevant papers will be referenced.

Identification Problems

An *identification problem* is specified by:

1. A finite universe U of objects.

2. A probability distribution $p(\cdot)$ over U, in which $p(a)$ denotes the *a priori* probability of object a.

3. A set T of *tests*. For any test $t \in T$ and any object a, $t(a)$, the *outcome* of test t on object a, is either 0 or 1; thus each test t partitions the universe U into the two sets $t^{-1}(0)$ and $t^{-1}(1)$.

An *identification algorithm* performs a sequence of tests in order to identify an initially unknown object drawn from the probability distribution p. The algorithm is *adaptive* if the choice of each test may depend on the outcomes of all previous tests, and *oblivious* if the sequence of tests is fixed in advance. We also consider randomized algorithms, in which each successive test is drawn from a probability distribution over T determined by the outcomes of previous tests.

A (deterministic) adaptive identification algorithm can be represented by a binary decision tree in which the nodes represent tests and the possible executions of the algorithm correspond to paths from the root of the tree to a leaf.

The main problem is to find an adaptive algorithm which minimizes the expected number of tests performed. The *information theory bound* states that, for any algorithm, the expected number of tests is at least the entropy of the distribution p; *i.e.*, $-\Sigma_{a \in U} p(a) \log_2 p(a)$. In particular, when the distribution p is uniform, the expected number of tests (and hence *a fortiori* the maximum number of tests) is at least $\log_2(|U|)$, where $|U|$ denotes the cardinality of U. Thus a perfect strategy for Twenty Questions is possible only if the number of objects in the universe does not exceed 2^{20}.

The classic *prefix coding problem* corresponds to the case where every function t from U into $\{0,1\}$ (*i.e.*, every two-way partition of the universe) is available as a test. Huffman codes [9] provide an elegant optimal solution to this problem. The *alphabetic coding problem* corresponds to the case where the universe is linearly ordered, and all tests of the form $x < a$? are available, where x is the unknown object, a is a specific object, and $<$ is the linear ordering. The Gilbert-Moore code [6] requires an expected number of tests that does not exceed the information theory bound by more than 2. An efficient algorithm for solving this problem optimally was given by Hu and Tucker [8].

Several variations on the identification problem are of interest. A test may have more than two possible out-

Continued on page 3

From the Editor

Kimberly Wasserman

It is with great pleasure (and only a small amount of trepidation), that I assume editorship of the IEEE Information Theory Society Newsletter. As we move into the second fifty years of the field of Information Theory, I look forward to the fun and challenging task of keeping you up-to-date on the announcements, seminars, papers, and reports that bring us together as a true academic —and social — community. In this issue, I hope you'll enjoy the report by Richard Karp on his ISIT'98 plenary lecture, and the columns from the society President Ezio Biglieri and society Historian Anthony Ephremides. There are also announcements of prestigious awards and medals recently won by members of our Society. I owe a tremendous debt of gratitude to outgoing editor Michelle Effros, who has been of invaluable assistance to me in this transition, and extend an invitation to you to stay in touch, offer suggestions for future columns, proffer tips, advice and the like that will truly make this our newsletter. The deadlines for the next few issues are as follows:

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

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

Kimberly Wasserman

Kimberly Wasserman
Electrical Engineering and Computer Science Department
University of Michigan
Ann Arbor, MI 48109-2122
USA

Tel: +1 (734) 647-3524
Fax: +1 (734) 763-8041
e-mail: wass@eecs.umich.edu

IEEE
Information Theory Society Newsletter

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

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

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

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

Table of Contents

ISIT'98 Plenary Lecture Report . . .

continued from front cover

comes. A small probability of erroneous identification may be permitted. Instead of minimizing the expected number of tests we may wish to determine the *worst-case complexity* of the problem, defined as the minimum over all adaptive deterministic algorithms of the maximum number of tests executed. Different tests may have different execution costs. The objects may be partitioned into classes, and the goal may be to identify the class to which an unknown object belongs; such a problem is called a *classification problem*.

The applications of identification and classification problems range from serious applications arising in medical diagnosis, pattern classification, machine learning and the design of scientific experiments to mathematical recreations such as determining which of n coins is lighter or heavier than the others by a series of weighings on a balance scale.

The examples discussed in this article will be of three types: mathematical recreations, problems arising in the design of efficient algorithms, and problems related to experimental design in the field of genomics. Several of the examples are intimately connected with coding theory.

Ulam's Problem

In 1979 S. Ulam proposed the problem of 'Twenty Questions with Lies.' Here the universe is an arbitrary set of m elements, and all possible tests are permitted. However, in any run of the algorithm, the outcomes of up to e tests may be incorrect. The problem is to minimize the maximum number of tests executed by an adaptive algorithm that is guaranteed to identify an unknown object. Let $f(m,e)$ denote this minimax number of tests.

It turns out that Ulam's problem had already been investigated in disguised form in a 1968 paper by Berlekamp [3]. Berlekamp described it as the problem of transmitting messages reliably across a noisy binary symmetric channel which is accompanied by a noiseless, delayless feedback channel. In this formulation there are m possible messages, each of which is encoded by n bits, of which up to e may be corrupted by the binary symmetric channel. The bits are transmitted sequentially, and, after receiving each bit, the receiver sends it back to the transmitter using the feedback channel. It is easy to see that there is a way to ensure that the receiver learns the message if and only if $n \geq f(m,e)$.

Berlekamp derived lower bounds on $f(m,e)$ using two bounding techniques, which he referred to as the volume bound and the translation bound. We limit ourselves to presenting the following inequality, which is a special case of the volume bound: if $n \geq f(m,e)$ then $2^n \geq m\Sigma_{i=0}^{e}\binom{n}{i}$. The proof is simple. We may assume that the algorithm always asks exactly n questions. There are 2^n possible values for the sequence of answers, and each sequence of answers must uniquely identify an element of the universe. Since any set of up to e of the answers may be erroneous, each element of the universe must be identified by any of at least $\Sigma_{i=0}^{e}\binom{n}{i}$ different sequences of answers. The desired inequality follows.

Berlekamp's original paper gave rather tight bounds on the function $f(m,e)$, but the quest to determine $f(m,e)$ exactly for larger and larger values of m and e goes on to this day.

Group Testing

The concept of group testing originated during World War II, when blood samples were being taken from hundreds of thousands of draftees in order to screen them for syphilis. To avoid the labor of testing each blood sample separately in order to identify the relatively small set of individuals who tested positive, someone suggested testing pools of blood samples. It was assumed that a pool would test positive if and only if it contained an individual positive for syphilis. Thus, if a pool tested negative there would be no need for further testing of the individuals in the pool.

Abstractly, the group testing problem is as follows: given a universe U of patients, each of whom is either *positive* or *negative*, identify the set P of positive patients by an adaptive algorithm that uses tests of the following form: does S, a subset of U, contain a positive patient? A good general reference on group testing is [4].

Let us consider the somewhat artificial case in which the number of patients is known to be d. Since there are $\binom{n}{d}$ possibilities for the set P, the information theory bound tells us that the worst-case complexity is at least $\left\lceil \log_2 \binom{n}{d} \right\rceil$. F. Hwang [10] has given a simple algorithm with worst-case complexity bounded above by $\left\lceil \log_2 \binom{n}{d} \right\rceil + d - 1$.

Interestingly, oblivious algorithms for the group testing problem are inherently more expensive than the best adaptive algorithms for the problem. It can be shown that the minimum worst case number of tests for an oblivious group testing algorithm is at least $\frac{d^2}{2}(1+o(1))\log_2 n$. However, if one is willing to accept a small probability of error, then a very simple randomized oblivious algorithm performs reasonably well [2]. The algorithm simply constructs a set of N tests randomly, such that, independently for every test S and every patient a, the probability that $a \in S$ is $\frac{1}{d+1}$. It is easily shown that the number of tests required to ensure that, with probability greater than or equal to $1-\varepsilon$, every patient is correctly designated as positive or negative, is $(1+o(1))(d+1)e\ln(\frac{n}{\varepsilon})$, which exceeds the information theory bound by a small constant factor when ε is a constant and d is bounded above by a fractional power of n. This result can be improved signficantly by placing each patient randomly in exactly $\frac{N}{d+1}$ of the N tests, rather than letting the number of tests containing a given patient be a random variable.

This oblivious algorithm is easily extended to an interesting generalization of group testing that we call the *Multi-Disease*

Problem. In this problem we have a universe U of n patients, and each patient may be positive for any of m diseases. A test $S \subseteq U$ determines, for each disease j, whether S includes a patient positive for disease j. The goal is to determine, for each disease j, the set of patients positive for that disease. Adaptive algorithms for the single-disease case are not easily extended to the multi-disease problem, but the oblivious algorithm works; it is only necessary to choose the number of tests appropriately. If the number of positive patients for each disease is at most d then the number of tests required to ensure that, with probability greater than or equal to $1-\varepsilon$, every patient is correctly designated as positive or negative for every disease, is $(1+o(1))(d+1)e\ln(\frac{nm}{\varepsilon})$.

A Genomics Example: Identifying Splice Sites

A generic problem in experimental science and medicine is the design of an efficient experimental protocol for determining properties of a specimen, molecule or patient. One such example is the detection of splice sites within a gene [15]. The genes of an organism occur within each of its cells, and lie within linear DNA molecules (the chromosomes) composed of tens of millions of subunits called nucleotides which are of four types: A,C, T and G. Genes get transcribed into an intermediate form called mRNA, which in turn is translated into protein. In the laboratory one can perform a process called reverse transcription, which converts the mRNA back to DNA.

For present purposes we can adopt a simplified model in which a DNA molecule is treated as a string x of nucleotides and a gene consists of several disjoint substrings of x, usually fairly close together. These substrings are called *exons*, and the substrings between consecutive exons are called *introns*. The point where an exon ends and an intron begins is called a *splice site*. When a gene is transcribed to mRNA the introns are removed and the mRNA versions of the exons are spliced together. If we then perform reverse transcription we get a single string y which is the concatenation of all the exons, and we can then use standard experimental procedures to determine the nucleotide sequence of y. Given this sequence we would like to determine the splice sites. Using an experimental procedure called PCR (polymerase chain reaction) we can pick any two positions in y that are not too far apart and determine whether these two positions are further apart in x than they are in y; this is the criterion for the existence of a splice site between the two positions.

The problem of splice site detection involves three parameters: n, the length of the string y, m, an upper bound on the number of splice sites, and d, the maximum possible distance in y between the two end positions of a PCR experiment. In terms of these parameters the splice site detection problem can be stated as follows. We are given a sequence of n positions (corresponding to the occurrences of nucleotides in y), of which at most m (the splice sites) are marked. For any two positions i and j such that $|j-i| \le d$ we can perform a test to determine whether there is a marked position between i and j. We wish to minimize the maximum number of tests needed to determine the marked positions. It is clear that this number is roughly of the order $max(n/d, m\log n)$, but its exact dependence on n, m and d is unknown.

Sorting

Let $(x_1, x_2, \ldots, x_n)$ be a sequence of n elements that are linearly ordered by the relation $<$. Then there is exactly one permutation π such that $x_{\pi(1)} < x_{\pi(2)} < \ldots < x_{\pi(n)}$. The process of discovering this permutation is called *sorting*. We are interested in algorithms for sorting by performing comparisons between pairs of elements. By the information theory bound, the expected number of comparisons needed to determine the correct permutation is $\log_2 n!$ if all $n!$ permutations are equally likely to be the correct one; by Stirling's formula, $\log_2 n! = n\log_2 n - \frac{n}{\ln 2} + \frac{1}{2}\log_2 n + O(1)$. Several sorting methods are known which have a worst-case complexity of $n\lceil \log_2 n \rceil - 2^{\lceil \log_2 n \rceil} + o(1)$, and thus are nearly optimal [13].

It is an interesting challenge to find an algorithm that sorts five elements in seven comparisons.

In practice, the choice of a sorting method depends on its simplicity, the amount of bookkeeping and data movement it requires, its performance when the amount of data is too large to fit into main memory, and a number of other factors in addition to its worst-case and expected number of comparisons.

Sorting Networks

A *sorting network* is a special type of sorting algorithm suitable for realization in hardware. The network has n registers. At any stage during the execution of the algorithm the n elements to be sorted occupy separate registers. The sorting is performed by a fixed sequence of comparators. An $i-j$ *comparator*, where $1 \le i < j \le n$, compares the elements in registers i and j, and returns the smaller of the two to register i and the larger to register j. At the end of the computation the elements are required to be sorted; *i.e.*, for each i between 1 and n, the ith-smallest element is in register i.

For many years there was a gap between the known upper and lower bounds on the minimum number of comparators in a sorting network. By the information theory bound the number of comparators must be $\Omega(n\log n)$, but the best construction known used about $n\log^2 n$ comparators. In a 1983 paper Ajtai, Komlós and Szemerédi [1] showed that $O(n\log n)$ comparators suffice, using a remarkable construction based on expander graphs. Their algorithm has the additional feature that it can be parallelized; the parallel version runs in $O(logn)$ rounds, with each element entering into at most one comparison in each round.

Sorting Given a Partial Order

A natural extension of the sorting problem is the problem of sorting when some *a priori* information is available about the ordering of the n elements. Suppose we are given a partial ordering p of the n elements, such that the true linear ordering < is a linear extension of p; *i.e.*. if x_i p x_i then $x_i < x_j$. Let $N(\text{p})$ be the number of linear extensions of p; then, by the information theory bound, the worst-case number of comparisons required to sort the n elements given the partial order p is at least $\lceil \log_2 N(\text{p}) \rceil$.

Fredman [5] showed that the worst-case number of comparisons needed to sort n elements given the partial order p is at most $\lceil \log_2 N(\text{p}) \rceil + 2n$. Fredman's construction makes clever use of the Gilbert-Moore code for the alphabetic coding problem. The Gilbert-Moore code can be viewed as solving the following search problem. Given an ordered sequence $a = (a_0, a_1, a_2, \text{L}, a_n)$, a sequence p_0, p_1, L, p_n of positive reals summing to 1, and an unknown element x such that $a_0 < x < a_n$ and $x \notin \{a_0, a_1, \text{L}, a_n\}$, insert x into the ordered sequence a by an adaptive algorithm which compares x with elements of a, such that, if $a_{i-1} < x < a_i$, the number of comparisons performed does not exceed $\lceil -\log_2 p_i \rceil + 1$.

Fredman's construction is based on insertion sorting. At a general step, the first k elements of the sequence a have been sorted, and the goal is to insert the $(k+1)$th element. Let the ordered sequence of elements obtained so far be $(a_0, a_1, \text{L}, a_{k-1})$ and let b be the next element to be inserted. Let $a_k = \infty$. Among all the linear extensions of p satisfying $a_0 < a_1 < a_2 \text{L} < a_{k-1}$ let p_i be the fraction that satisfy $a_{i-1} < b < a_i$. Using the Gilbert-Moore code, the construction inserts b into the ordered sequence in such a way that, if $a_{i-1} < b < a_i$, the number of comparisons performed does not exceed $\lceil -\log_2 p_i \rceil + 1$. A short calculation then shows that the total number of comparisons to sort given the partial order p does not exceed $N(\text{p}) + 2n$.

Fredman's construction establishes an upper bound on the worst-case number of comparisons required to sort given p. It is not suitable for practical use because of the extensive computation needed to determine the quantities p_i at each step; this work is not counted in the complexity bound, since it does not involve comparisons between the elements to be sorted.

Suppose we wish to sort n elements given a partial order p. For any two elements u and v, let $\Pr[u < v]$ be the fraction of linear extensions of p in which $u < v$; $\Pr[u < v]$ gives the probability that $u < v$ if all linear extensions of p are equally likely. Call the comparison a *perfect comparison* if $Pr[u < v] = \frac{1}{2}$. A perfect comparison eliminates exactly half of the linear extensions of p, regardless of its outcome. If, at every step of our algorithm, we execute a comparison which is perfect with respect to the current partial order (*i.e.*, the partial order determined by the initial partial order p together with the results of all the comparisons performed thus far), then the number of comparisons performed by the algorithm will be exactly equal to the information theory bound.

Unfortunately, there are situations where no perfect comparison exists. As an example, consider a partial order on the set $\{x_1, x_2, x_3\}$ such that $x_1 < x_2$ and x_3 is comparable to neither x_1 nor x_2. In this case $\Pr[x_1 < x_{3]} = 2/3$ and Pr $[x_2 < x_3] = 1/3$. Fredman conjectured that, for every partial order that is not a total order, there exist two elements u and v such that $1/3 \le Pr[u < v] \le 2/3$. This conjecture remains open, but in 1984 Kahn and Saks [11] proved that, for every partial order that is not a total order, there exist two elements u and v such that $3/11 \le Pr[u < v] \le 8/11$. To prove this, they define $h(x)$ as the average rank of element x in the linear extensions of p. If p is not a total order, then there exist two elements, u and v, such that $|h(u) - h(v)| < 1$. They give an elegant geometric argument showing that, if $|h(u) - h(v)| < 1$, then $3/11 \le Pr[u < v] \le 8/11$.

It follows that, at every stage in the process of sorting given a partial order, a comparison will be available which causes at least a fraction $3/11$ of the eligible linear extensions to be discarded, regardless of the outcome of the comparison. thus the worst-case number of comparisons to sort, given the partial order p, is at most $\lceil log_{11/8} N(\text{p}) \rceil$. This result is an improvement over Fredman's upper bound when $N(\text{p}) < c^n$, where c is a certain constant greater than 1. However, this result, like Fredman's, while useful for deriving an upper bound on worst-case complexity, does not give a usable algorithm, as the labor required to find the desired comparison at each step is unreasonably large.

Local Sorting

In [7] Goddard, King and Schulman consider the following problem. Let G be an undirected graph, and let distinct elements of a linearly ordered set be assigned to its vertices; let $x(u)$ denote the element assigned to vertex u. For each edge $\{u, v\}$ of G, determine whether $u < v$.

An *acyclic orientation* of G is an assignment of directions to the edges such that the resulting directed graph is acyclic. Let $\alpha(G)$ be the number of acyclic orientations of G. Local sorting yields an acyclic orientation of G by the following rule: orient edge $\{u, v\}$ from u to v if $x(u) < x(v)$, and from v to u if $x(v) < x(u)$. Conversely, every acyclic orientation of G is induced by this rule from some assignment of distinct elements to the vertices of G. Thus local sorting can be viewed as the problem of determining the acyclic orientation induced by a given assignment of distinct elements to the vertices of G. It follows that the information theory bound for local sorting is $\lceil \log_2 \alpha(G) \rceil$. The paper [7] gives a randomized local sorting algorithm such that, for every assignment of distinct elements to the vertices, the expected number of comparisons is $O(\log_2 \alpha(G))$.

Continued on page 21

Awards

Kees A. Schouhamer Immink wins the 1999 Edison Medal

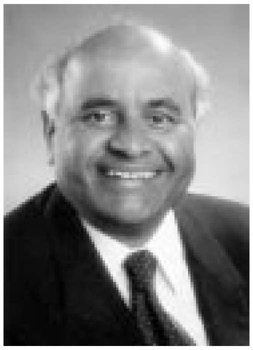
The IEEE Board of Directors has named Kees A. Schouhamer Immink the recipient of the 1999 Edison Medal "for a career of creative contributions to the technologies of digital video, audio, and data recording."

The Edison medal, named after the renowned inventor, was established in 1904 by the AIEE, one of the constituent societies of the IEEE. The Edison Medal is IEEE's principal medal presented for a career of meritorious achievement in electrical science, electrical engineering, or the electrical arts. The prize, sponsored by Hitachi Ltd, Mitsubishi Electric Corporation, and Toshiba Corporation of Japan, consists of a gold medal, small gold replica, certificate and $10,000.

A native of The Netherlands, Kees Schouhamer Immink was born in Rotterdam on December 18, 1946. He obtained the M.S. and Ph.D. degrees at the Eindhoven University of Technology. He worked in industry from 1968 till 1998, and is, since 1995, an adjunct professor at the Institute for Experimental Mathematics, Essen University, Germany.

An article on Professor Schouhamer Immink in honor of his receipt of the medal will appear in a future issue of the newsletter.

Vijay K. Bhargava Receives the 1999 Haraden Pratt Award



The IEEE has announced that Vijay K. Bhargava is the recepient of the 1999 IEEE Haraden Pratt Award "for meritorious service to the Institute, particularly in regional and section activities, and for his efforts to improve relationships with technical and professional organizations worldwide." The Haraden Pratt is sponsored by the IEEE Foundation and recognizes outstanding service to the Institute. It consists of a bronze medal, an illuminated certificate and $5,000. Professor Bhargava is with the department of Electrical and Computer Engineering at the University of Victoria in Canada, and will receive the award at the IEEE Awards and Honours Ceremony to be held at the White Hall Palace in London on Saturday, June 12, 1999.

W. Wesley Peterson wins the 1999 Japan Prize

The Science and Technology Foundation of Japan has selected Dr. W. Wesley Peterson as a laureate of the 1999 Japan Prize for his establishment of coding theory for reliable digital communication, broadcasting and storage.

The Japan Prize 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. The first prizes were awarded in 1985.

Each year, the Science and Technology Foundation of Japan chooses the two prize categories, which are information technology and life sciences for 1999. Peterson is the laureate for information technology and will receive Y50 million (about US$450,000) at the 15th Japan Prize award ceremony scheduled for April 28, 1999. The ceremony will be held in the presence of Their Majesties, the Emperor and Empress in Tokyo. The event will also be attended by the Prime Minister, the Speaker of the House of Councilors, the Chief Justice of the Supreme Court, foreign ambassadors to Japan and well over a thousand other guests, including eminent academics, researchers and representatives of political, business and press circles. The week in which the Japan Prize is awarded is designated as "Japan

Prize Week". During this period, Peterson will attend commemorative lectures and an academic discussion meeting.

Peterson, a professor of the Information and Computer Sciences at the University of Hawaii at Manoa, is particularly well known for his book *Error-Correcting Codes*, the "bible" for algebraic coding theory, which had a profound effect on the evolution of the digital communication and storage field. In this book, he created the conceptual framework of coding theory on the basis of modern algebra and described practical realization for error-detection and error-correction of his own invention. This led to an outstanding contribution in the industrial applications. An article on Professor Peterson in honor of his receipt of the prize will appear in a future issue of the newsletter.

Electronic Submission of Manuscripts to the IEEE Transactions on Information Theory

INFORMATION FOR AUTHORS

Overview:

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

Submission Procedure:

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

submit@it.csl.uiuc.edu

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

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

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

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

ftp.it.csl.uiuc.edu

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

Copyright:

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

Review Procedures:

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

Hard Copies:

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

President's Column

Ezio Biglieri

Ezio Biglieri

As Isaac Newton (or was it Didacus Stella? The most "Shandean" among our readers know the answer) wrote in his letter to Thomas Hooke, "If we have seen further, it is because we have stood on the shoulders of giants." So, it was altogether fitting and proper to celebrate these giants of Information Theory in 1998, our Golden Jubilee year. The year 1998, which has just come to an end while I am writing this column, was indeed a very exciting one for all of us having interest in this field. Our celebrations gave us in fact, at a time, the occasion of reflecting on the accomplishments of our discipline, of learning from those who embody in their work what is deemed worthwhile in our discipline ("You must earn what you inherit from your fathers; you must make it your own"; Goethe), and of looking forward to the challenges of the second fifty years of Information Theory.

A number of events, intended to celebrate the 50 years of Information Theory, were arranged, most of them occurring in the occasion of the IEEE Information Theory Symposium at MIT. The organizers of ISIT'98, led by Dave Forney and Bob Gallager, were successful in making this symposium the special event the fiftieth anniversary of Information Theory deserved. The sheer number of participants to this Symposium—-around 900—-documents at the same time the success of their efforts and the vitality of our Society. Among the many other initiatives, the October 1998 issue of our Transactions, guest-edited by Sergio Verdú, was a commemorative issue containing perspective papers intended for a wide audience. A book version of it, called "Information Theory: Fifty Years of Discovery" and published by the IEEE Press, is in the final stages of production. It should be in the bookshops shortly after you read this column.

Following a longstanding tradition, our members continue to collect awards and distinctions. To name some of the more prominent recent awards, W. Wesley Peterson won the Japan Prize, Kees A. Schouhamer Immink the IEEE Edison Medal, and Vijay Bhargava the IEEE Haraden Pratt Award. You will read more on these elsewhere in this Magazine.

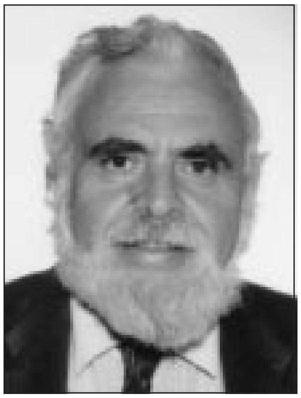
We welcome and congratulate our newly elected and re-elected members of the Board of Governors: Anthony Ephremides, Johannes Huber, Vincent Poor, Stephen Wicker, Raymond Yeung, Bin Yu, and Jacob Ziv. The lineup of our 1999 officers reflects the increasing internationalization of the IT Society: first Past President, first and second VP, and the President all work outside of the United States. The other key positions in the Society are in the best of hands: Alexander Vardy leads, as Transactions Editor-in-Chief, a dedicated and talented group of Associate Editors; Steve McLaughlin, Transactions Publications Editor, ensures a smooth interface with IEEE Publications; Kimberly Wasserman shoulders the task of editing this Newsletter; and our Secretary, Greg Pottie, is in charge of the Minutes of Board Meetings. Behnaam Aazhang, our former Treasurer, has just stepped down after serving the Society extremely well for three years. He leaves the Society on a firm financial footing. Marc Fossorier is now replacing Behnaam. Thanks to Ramesh Rao, who continues his service to the Society as Web Editor, our World Wide Web site (http://www.itsoc.org) is reaching its full potential. Please help us make our site the valuable tool that it can be in the promotion of information theory around the world. You can do this by sending your suggestions and feedback to <rrao@uscd.edu>. Other committees are in the process of being formed or reconfirmed. I shall report on these in my next column.

In future issues of this Newsletter I will also expand on some of the new initiatives in preparation. Until then, I would like to hear any questions, comments or suggestions you may have. You can reach me at biglieri@polito.it. I would also like to see an increased participation of the members of the Society in its affairs. For example, the voting-member turnout in the Board of Governors elections is typically around 10%, a percentage lower than that of the participants to International Symposia. I repeat here what my predecessor Jerry Gibson wrote in his column a few years ago: for the Society to continue to provide high-quality services to our members and to the technical community at large, we need to recruit new members, new volunteers, and new leaders. Other IEEE Societies have staff members who aid in many of the technical details, work on organizing conferences, edit publications, and author Web pages. So far, we have been a completely volunteer society, a choice which requires capable individuals who can and will devote a substantial portion of their time. A good way to learn more about the Society activities and to get involved in them is to attend the meetings of its Board of Governors. The three 1999 meetings will be held on February 27 after the IT Workshop on Detection, Estimation, Classification and Imaging in Santa Fe, NM, on June 20 before the IT Workshop to be held in the Kruger National Park in South Africa, and in the occasion of the Allerton Conference, to be held in Allerton House, Monticello, IL, on September 22—24, 1999. Please plan to participate.

As I am running out of space, I notice that I could only delve into organizational issues in this first column of mine, and that I am forced to leave out some of the "philosophical" points I had in mind to discuss with our readers. One of them, which I consider especially important, has to deal with our ability of conveying the significance of our work to the community of people with no technical background. Today, we are experiencing a process in which the place of a "diffuse culture" is being taken by a "diffuse information:" apparently, the "user of culture," in reading books or magazines, does not look for scientific concepts expressed in a legible yet rigorous form. He is rather in search for quick, easy, curiosity-laced information. I see the result of this process as the trivialization of the way non-technical people see our work. A good example of this could be experienced a few months ago, when the New York Times ran an obituary of the distinguished Information Theorist Aaron D. Wyner: it presented him as a scientist who "helped speed data around the globe." Are we happy with such a reductive view of our profession? Is there anything we can do to reverse this trend? I would like to open a dialogue with our members on this and related points, which I plan to deal with in later columns, less concerned with organizational details and perhaps containing "more art with less matter."

Golomb's Puzzle Column™ Number 45:
0-1 Matrices

Solomon W. Golomb



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

   a. Prove that it is possible to remove a column from M in such a way that the shortened rows remain distinct.

   b. Show, for every $n \geq 3$, that there exists an $n \times n$ matrix M of 0's and 1's for which no two columns can be removed in such a way that all the (shortened) rows remain distinct.

2. *A* (v, k, λ)-design D is a set $S = \{x_1, x_2, \ldots, x_v\}$ with v k-element subsets $S_1, S_2, \ldots, S_k$, such that S_i I S_j contains λ elements for all $i \neq j$, each element is in k subsets, and each pair of elements x_i, x_j is contained in λ of the subsets. The $v \times v$ incidence matrix M of the design D has a 1 at m_{ij} if $x_j \in S_i$, and 0's everywhere else.

   If we call the elements x_i ,K , x_v, "points" and the subsets S_i,..., S_v "lines", then each line contains k points, each point lies on k lines, each pair of lines have λ common points, and each pair of points lie on λ common lines. The rows of the incidence matrix M correspond to the lines, and the columns to the points, and there is a 1 in the matrix wherever a point (column x_j) lies on a line (row S_i). (All other matrix entries are 0.)

   Let I be the $v \times v$ identity matrix, and let J be the $v \times v$ matrix *all* of whose entries are 1's. Express MM^t in terms of I and J, where M^t is the *transpose* of M, and prove that $k(k - 1) = \lambda(v - 1)$.

3. We want to form an $m \times n$ matrix of 0's, 1's, and *'s (you can think of *'s as erasures), where m is as large as possible for the given value of n, and where the m rows must satisfy the following two constraints:

   i) Every pair of rows is *comparable;* i.e. regarded as vectors, there is at least one position where they differ, and where neither has the value "*" in that position.

   ii) Each pair of rows is *consistent;* i.e. if there is one position where row R_i has a "0" and row R_j has a "1", there must not be another position where row R_i has a "1" and row R_j has a "0".

   a. Note that the *consistency* property does not lead to a transitive linear ordering of the rows. That is, if we say that $R_i < R_j$ if R_i has 0's where R_j has 1's in all the positions where these two rows differ and where neither has the value "*", it is possible to have three rows R_i, R_j, R_k where $R_i < R_j$, $R_j < R_k$, and $R_k < R_i$. Find an example of this with the smallest value of n for which it can occur.

   b. Construct $m \times n$ matrices of 0's, 1's, and *'s, subject to the rules of *comparability* and *consistency*, with m as large as possible for the given n, for each of the following values of n:

$$n = 3, \quad n = 7, \quad n = 13, \quad n = 21.$$

The Historian's Column

A. Ephremides

With the celebration of the Golden Anniversary of the founding of Information theory that took place last year fading gently into the past, I felt motivated to take a look at the much more modest celebration of the Silver Anniversary of the field that took place back in 1973. The most vivid of the celebration events last year was of course the Symposium last August in Cambridge, MA (although the most scholarly and durable one was beyond question the publication of the commemorative issues of the Transactions). Thus, I'd like you to join me in a mental journal twenty five years into the past in an effort to replay the highlights of what was the most vivid celebration event then, the 1973 ISIT.

A. Ephremides

Although present at that Symposium I had to refresh my memory by reviewing files and records that historians, among others, tend to keep. In doing so, I saw unfolding in my mind a wonderful event that, in retrospect, was just as important as the Golden Jubilee Symposium, although nowhere as glorious.

It was really another era and another world. The venue was Ashkelon, a seaside resort in Israel, and the time was just months before the 1973 middle-east war and oil embargo that in many ways shaped the last quarter of the expiring century. In terms of numbers it was a much smaller event. There were a total of 18 sessions arranged over five half-day periods in groups of 3 or 4 parallel ones, plus four plenary sessions, in one of which, the first Shannon lecture was delivered by Claude Shannon, himself.

The Symposium opened Monday, June 25, at the civilized hour of 10:30 am with a plenary session in which Bob Gallager delivered a keynote address on the first 25 years of Information Theory. The tenor of the talk was that the field had led to some modest technological advances by that time, but, far more importantly, it had led to a cohesive framework for viewing problems on communications and related areas. These words ring so true today as well, except that "concrete and substantive" should be substituted for "modest" as a qualifier of the nature of technology advances that Information Theory has led to. In that same talk, Bob predicted the emergence of networking as the challenge of the future for Information Theory.

The other plenary talks, spread over the rest of the week (except for Wednesday, the 27th, that was reserved for a memorable excursion to Jerusalem, the Masada, and the Dead Sea — in which some of us made the mistake of taking a swim after a fresh shave) were by R. Varshamov (on asymmetric coding systems and irreducible polynomials over Galois fields), S. Winograd (on arithmetic complexity of bilinear forms), M. Rabin (on complexity of computations), I. Jacobs - the same one who gave a plenary talk in the 1998 ISIT — (on the fanciful subject of "coding for a real, but resistant, world"), and, of course, Claude E. Shannon, whose lecture was titled: "The Wonderful World of Feedback." Although, I have no record document of that talk, my recollection is one of awe as many of us were seeing the Founder of the field for the first time. Whimsical pictures of feedback illustrated by means of infinite reflections on mirrors that face each other or in terms of a person pictured on a beer can who holds a can of that beer (with that person on it holding the beer can that has on it the person with the beer can that .... etc., etc.) were the highlights of a talk that showed the lighter side of Shannon's intellect and that, perhaps, intended to downplay the reverence with which everyone worshiped the impact of his work — a sign of modesty that was another one of Shannon's traits.

How different the composition of the Program was then, compared to what we are accustomed to today. There were 4 sessions on Shannon theory (it was just about the time that the term was first coined by A. Wyner), 3 sessions each on Coding, Communications, and Detection/Estimation, 2 sessions on Stochastic Processes, and 1 session each on Radar (!), Pattern Recognition, and Complexity/Learning.

Here is a sample of semi-randomly selected papers that convey the flavor of that Symposium. Jim Massey talked about Error Bounds for Random Tree Codes; Dick Blahut discussed the connection between Hypothesis Testing and Information Theory; Dave Forney presented an Information-Theoretic Inference Principle; Dave Slepian and Jack Wolf presented their famous work on Noiseless Coding of Correlated Information Sources; Peter Elias gave a talk on a Generalization of the Kraft Inequality; Lee Davisson discussed Universal Source Coding (by the way, there were no Source Coding sessions at that time; the subject was subsumed in general coding or, mostly, Shannon theory sessions); Andy Viterbi and Jim Omura coauthored a paper on Convolutional Encoding of Memoryless, Discrete-Time Sources with a Fidelity Criterion (how "standard" it sounds today!). The late David Sakrison and Stamatis Cambanis talked about Psycho-Physical Measurements of the Visual System and Continuity/Differentiability of Gaussian Processes, respectively (how ... different(!)); Ted Kadota and Jack Salz discussed Optimal Detections for M known signals in Impulsive Noise (yes, this was still virgin research territory then); and John Savage talked about signal sets that permit interference rejection with matched-filter detectors (those were pre-multi-user-detection days). Last but not least, the Historian himself, just two years out of Graduate School, showed that the spectral multiplicity of random processes was unimportant in the sampling and reconstruction of random processes (a result that essentially reduced his Ph.D. dissertion to an ... academic exercise, as many Ph.D. dissertations are!).

Most sessions were really crammed with papers. Some had as many as thirteen (13!) papers. Each paper presentation was given twelve (12!) minutes, except for a handful of asterisk-marked papers, designated as "long papers" that were given 25 minutes each. And there was a paper, right in the middle of a regular session on Communications, that was presented by Elias Schutzman, on the NSF Program supporting optical communications! Elias was a "regular" figure at IT events. He was a career employee at NSF who basically directed the Program that supported the research of many Information Theorists. He was feared, revered, befriended, and, in many ways, a part of the IT community. Having him listen to your paper was an omen that might bring funding bliss or funding blues.

Another highlight of the program was a special session on the status of Decision Theory. This was part of the total of the 18 sessions but it was an all-invited session with only six speakers: Carl Helstrom (on Quantum Detection and Estimation Theory - so much ahead of its time(!)), J. Capon (on Seismic Detection), L. Kurz (on Non-Parametric Methodologies), M. Hellman (on Finite-Memory Decision Theory), T. Kailath (on the Use of Martingales - a "hot" topic at the time (!)), and T. Fine (on Qualitative Decision Making - even then ... he knew(!)).

The Symposium cochairs were Jacob Ziv with the late Aaron Wyner and the Program Chair was Neil Sloane. There were many moments (some light, some serious, some personal, some landmark) that were memorable. One of those happened during one of the talks by a speaker who will not be named but who was hard of hearing. One person in the audience asked him to elaborate on a technical point that the speaker had made. The speaker, who had already asked previous questioners to repeat their questions louder, looked puzzled and annoyed, then stared at the audience blankly and answered, "yes"(!), and quickly returned busily to his viewgraphs.

What times, what world, what memories! If you look at the silver anniversary, the contents of the program, the size of the Symposium, and the "culture" of the community then and you compare it to the one we just experienced twenty-five years later, the question begs itself: "which was the better of the two?". My answer, like that of the aforementioned speaker, is "yes"! On to the diamond anniversary in the year 2023!

CALL FOR NOMINATIONS:

IEEE Medals, Service Awards, and Prize Papers

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

Below you will find a list of awards with a short description and recent winners. A complete list of 1998 awards appeared in the December 1998 issue of *The Institute*. All of the awards listed have a NOMINATION DEADLINE of JULY 1, 1999. We strongly encourage suggestions and or nominations, which can be directed to Vijay Bharagava at bhargava@ece.uvic.ca. More information on awards and the nomination procedure is also available on the Web at http://www.ieee.org/awards/, or directly from IEEE Awards Department, 445 Hoes Lane, Piscataway, NJ, USA 08855-1331, Tel: (732) 562-3840, Fax: (732) 981-9019, email: awards@ieee.org.

IEEE Medals

The IEEE Medals most appropriate to the IT society are:

IEEE Medal of Honor:
For a particular contribution which forms a clearly exceptional addition to the science and technology of concern to the Institute. The award shall normally be given within a few years after the recognition of the exceptional nature of such contribution. (Should have won at least a field award previously.)

Recent recipients:
1998—Donald O. Pederson,
1997—George A. Heilmeier,
1996—Robert M. Metcalfe,
1995—Lotfi A. Zadeh,
1994—Alfred Y. Cho,
1993—Karl Johan Aström,

1992—Amos E. Joel, Jr.,
1991—Leo Esaki,
1990—Robert G. Gallager,
1989—C. Kumar Patel,
1988—Calvin F. Quate.

The Alexander Graham Bell Medal:
For exceptional contributions to the advancement of communications sciences and engineering.

Recent recipients:
1998—Richard E. Blahut,
1997—Vinton E. Cerf & Robert E. Kahn,
1996—Tadahiro Sekimoto,
1995—Irwin M. Jocobs,
1994—Hiroshi Inose,
1993—Donald C. Cox,
1992—James L. Massey,
1991—C. Chapin Cutler, John O. Limb & Arun N. Netravali,
1990—Paul Baran,
1989—Gerald R. Ash,
1988—Robert M. Metcalfe.

The Richard W. Hamming Medal:
For exceptional contributions to information sciences and systems.

Recent recipients:
1998—David D. Clark,
1997—Thomas M. Cover,
1996—Mark S. Pinsker,
1995—Jacob Ziv,
1994—Gottfried Ungerboeck,
1993—Jorma J. Rissanen,
1992—Lotfi A. Zadeh,
1991—Elwyn R. Berlekamp,
1990—Dennis M. Ritchie & Kenneth L. Thompson,
1989—Irving S. Reed,
1988—Richard W. Hamming.

The Edison Medal:
For a career of meritorious achievement in electrical science or electrical engineering or the electrical arts.

Recent recipients:
1998—Rolf Landauer,
1997—Ester M. Conwell,
1996—Floyd Dunn,
1995—Robert W. Lucky,
1994—Leslie A. Geddes,
1993—James H. Pomerene,
1992—G. David Forney, Jr.,
1991—John Louis Moll,
1990—Archie W. Straiton,
1989—Nick Holonyak, Jr.,
1988—James Ross MacDonald.

The Medal for Engineering Excellence:
For excellence in teaching and ability to inspire students; leadership in electrical engineering education through publication of textbooks and writings on engineering education; innovations in curricula and teaching methodology; contributions to the teaching and engineering profession through research, engineering achievements, technical papers, and participation in the education activities of professional societies. All four requirements must be met.

Recent recipients:
1998—C. James Erickson,
1997—John G. Anderson,
1996—J.R. Dunki-Jacobs,
1995—Masasuke Morita,
1994—Heiner Sussner,
1993—Bernard C. Deloach, Jr., Richard W. Dixon, & Robert L. Hartman,
1992—Charles Elachi,
1991—Alexander Feiner,
1990—John A. Pierce,
1989—Walter A. Elmore,
1988—Karl E. Martersteck, Jr.

The John Von Neumann Medal:
For outstanding achievements in computer-related science and technology.

Recent recipients:
1998—Ivan Edward Sutherland,
1997—Maurice V. Wilkes,
1996—Carver A. Mead,
1995—Donald E. Knuth,
1994—John Cocke,
1993—Frederick P. Brooks, Jr.,
1992—C. Gordon Bell.

The Founders Medal:
For major contributions in the leadership, planning, and administration of affairs of great value to the electrical and electronics engineering profession.

Recent recipients:
1998—Alan W. Rudge,
1997—Gordon E. Moore,
1996—Norman R. Augustine,
1995—Malcom Currie,
1994—Akio Morita,
1993—Kenneth H. Olsen,
1992—Roland W. Schmitt,
1991—Irwin Dorros,
1990—Erich Bloch,
1989—Ivan A. Getting,
1988—Ian M. Ross.

The James H. Mulligan, Jr. Education Medal:
For a career of meritorious achievement in education as ex-

emplified by inspirational and innovative teaching; publication of texts, course material, and writings on education; creativity in curricula and teaching methodology; and other contributions to the teaching and engineering profession.

Recent recipients:
1998—Stephen W. Director,
1997—David A. Hodges,
1996—Adel S. Sedra,
1995—Thomas Kailath,
1994—Chung Laung Liu,
1993—Ronald A. Rohrer,
1992—Ronald W. Schafer,
1991—Hermann A. Haus,
1990—James D. Meindl,
1989—Ben G. Streetman,
1988—Alan V. Oppenheim.

IEEE Service Awards

Haraden Pratt Award:
For outstanding service to the Institute.

Recent recipients:
1998—Frederick T. Andrews,
1997—Robert A. Rivers,
1996—Walter E. Proebster,
1995—Henry L. Bachman,
1994—Ronald G. Hoelzeman,
1993—Harold S. Goldberg,
1992—Richard J. Backe,
1991—Thelma Estrin,
1990—Robert M. Saunders,
1989—Edward J. Doyle,
1988—Irene C. Peden.

Richard M. Emberson Award:
For distinguished service to the development, viability, advancement, and pursuit of the technical objectives of the IEEE.

Recent recipients:
1998—H. Troy Nagle, Jr.,
1997—Friedolf M. Smits,
1996—Theodore S. Sand,
1995—Theodore W. Hissey, Jr.,
1994—Oscar N. Garcia,
1993—William R. Tackaberry,
1992—Bruno O. Weinschel,
1991—Stephen J. Kahne,
1990—Harold Chestnut,
1989—Jose B. Cruz, Jr.,
1988—Merlin G. Smith.

IEEE Prize Paper Awards

W.R.G. Baker Prize Award:
For an outstanding paper reporting original work in the *Proceedings of the IEEE* or any of the IEEE Transactions, journals or magazines issued during the previous calendar year.

Recent recipients:
1998—Paul F. Mcmanamon, Terry A. Dorschner, David L. Corkum, Larry J. Friedman, Douglas S. Hobbs, Michaeil Holz, Sergey Liberman, Huy Q. Nguyen, Daniel P. Resler, Richard C. Sharp & Edward A. Watson,
1997—Rajiv Ramaswami & Kumar N. Sivarajan,
1996—Will E. Leland, Walter Willinger, Daniel V. Wilson, & Murad S. Taqqu,
1995—Petros Maragos, James F. Kaiser, & Thomas F. Quatieri,
1994—Michael M. Green & Alan N. Willson, Jr.,
1993—Narasimham Vempati, Ilya W. Slutsker, & William F. Tinney,
1992—Alon Orlitsky,
1991—John C. Doyle, Keith Clover, Bruce A. Francis, Pramod P. Khargonekar,
1990—Allen C. Newell,
1989— Randal E. Bryant,
1988—Benjamin Kedem.

Donald G. Fink Prize Award:
For an outstanding survey, review, or tutorial paper in the *Proceedings of the IEEE* or any of the IEEE Transactions, journals, or magazines issued during the previous calendar year.

Recent recipients:
1998—Francis T. S. Yu & Don A. Gregory,
1997—Asad A. Abidi,
1996—Ali H. Sayed & Thomas Kailath,
1995—Nikil Jayant, James D. Johnston, Robert J. Safranek,
1994—Andrew P. Sage,
1993—Pravas R. Mahapatra & Dusan S. Zrnic,
1992— Anthony Ephremides & Sergio Verdú,
1991—Tadao Murata,
1990—G. David Forney, Jr.,
1989—Karl Johan Aström,
1988—Raymond L. Murray

Leon K. Kirchmayer Prize Paper Award (successor to the Browder J. Thompson Memorial Prize Award):
For an outstanding paper by authors(s) under 30 years of age in an IEEE publication issued during the previous calendar year.

Recent recipients:
1998—Andrew R. Teel.

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@ee.princeton.edu) is Chair of the IT Fellow Evaluation Committee and is also available for help, particularly in identifying potential references.

The deadline for the nomination form and all reference letters is March 15, 1999. Your Society asks you to:

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

CALL FOR NOMINATIONS:

IEEE Information Theory Society Paper Award

Nominations are invited for the IEEE Information Theory Society Paper Award. Outstanding publications in the field of interest to the Society appearing anywhere during 1997 and 1998 are eligible. The purpose of this Award is to recognize exceptional publications in the field and to stimulate interest in and encourage contributions to the fields of interest of the Society.

The Award consists of an appropriately worded certificate(s) and an honorarium of US$5000 for single author papers, or honoraria of US$2500 to each of the authors of multiply authored papers.

NOMINATION PROCEDURE: Please send a brief rationale (limited to 300 words) for each nominated paper explaining its contributions to the field by April 15, 1999 to the Society's First Vice President: Professor Vijay K. Bhargava via e-mail (bhargava@ece.uvic.ca) or by post addressed as: Vijay K. Bhargava, Dept. of Elec. and Comp. Eng., Univ. of Victoria, P.O. Box 3055, Victoria BC Canada V8W 3P6.

CALL FOR PAPERS

Thirty-seventh Annual Allerton Conference on Communication, Control, and Computing

*Wednesday-Friday,
September 22-24, 1999*

The Thirty-Seventh Annual Allerton Conference on Communication, Control, and Computing will be held from Wednesday, September 22 through Friday, September 24, 1999, at the Allerton House, the conference center of the University of Illinois. Allerton House is located twenty-six miles southwest of the Urbana-Champaign campus of the University, in a wooded area on the Sangamon River. It is part of the fifteen-hundred acre Robert Allerton Park, a complex of natural and man-made beauty designated as a National natural landmark. The Allerton Park has twenty miles of well-maintained trails and a living gallery of formal gardens, studded with sculptures collected from around the world.

Papers presenting original research are solicited for the conference in the areas of communication systems, communication and computer networks, detection and estimation, information theory and error-correcting codes, source coding and data compression, multiple-access communications, queueing networks, control systems, robust and nonlinear control, adaptive control, optimization, dynamic games, large scale systems, robotics and automation, manufacturing systems, discrete event systems, intelligent control, multivariable control, adaptive signal processing, numerical methods for signals and systems, learning theory, neural networks, combinatorial and geometric algorithms, parallel and distributed computation, computational complexity, VLSI design algorithms, VLSI architectures for communications and signal processing, and automated highway systems. Also solicited are organized sessions for the Conference; prospective organizers should discuss their plans with the Conference co-chairmen before sending a form.

This year the plenary lecture will be delivered by Professor Frank Kelly of Cambridge University, England.

Information for authors: Regular papers, suitable for presentation in twenty minutes, as well as short papers, suitable for presentation in ten minutes, are solicited. The purpose of the short paper category is to encourage authors to present preliminary results of their work. Regular papers will be published in full (subject to a maximum length of ten 8.5" x 11" pages) in the Conference Proceedings, while short papers will be limited to two-page summaries in the Proceedings.

For regular papers, a title and a five-to-ten page extended abstract, including references and sufficient detail to permit careful reviewing, are required. For short papers, a title and a three-to-five page summary are required. Manuscripts that are submitted as regular papers but cannot be accommodated in that category will be considered in the short paper category, unless the authors indicate otherwise in their letter of submission.

Three copies of the manuscript should be mailed to 37th Annual Allerton Conference, Coordinated Science Laboratory, University of Illinois, 1308 West Main Street, Urbana, Illinois 61801-2307, USA, in time to be received by July 14, 1999. Submissions by email or fax will not be accepted.

Submissions should specify the name, email address, and postal address of the author who is to receive all subsequent correspondence. Authors will be notified of acceptance via email by August 14, 1999, at which time they will also be sent detailed instructions for the preparation of their papers for the Proceedings. Full camera-ready versions of accepted papers will be due the last day of the Conference. Only the papers presented at the Conference will be included in the Proceedings.

Further information on the Conference can be found on the Conference Web site whose URL address is given below.

Conference Co-Chairmen: Bruce Hajek and R.S. Sreenivas
Email: allerton@csl.uiuc.edu
URL: http://www.comm.csl.uiuc.edu/allerton/
COORDINATED SCIENCE LABORATORY AND
THE DEPARTMENT OF ELECTRICAL AND
COMPUTER ENGINEERING
University of Illinois at Urbana-Champaign

CALL FOR PAPERS

ISIT 2000
2000 IEEE International Symposium on Information Theory
SORRENTO (ITALY) JUNE 25-30, 2000

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

Papers presenting contributions to the following areas are solicited:

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

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

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

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

http://www.unisa.it/isit2000

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

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

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

Workshop Report

Scientific Meeting on Convolutional Codes and their Applications

November 4 - 6, 1998
Casino im Park,
Kamp-Lintfort, Germany

Ole Harmjanz IEM, University Essen
harmjanz@exp-math.uni-essen.de

The IEEE German chapter on Information Theory and the PhD School CINEMA organized the Scientific Meeting on "Convolutional Codes and their Applications". Bringing together senior experts and young researchers in the field, the workshop presented many interesting aspects of convolutional codes. More than 40 participants from groups working in Germany, the Netherlands, Russia, Sweden, and Switzerland enjoyed the opportunity to exchange new results during the talks and lively discussions. The nice location, where Churchill and Eisenhower met, invited participants to get to know each other during the breaks and the banquet. The final visit to the nearby Cistercian monastery Kamp offered welcomed relaxation after an interesting meeting.

Proceedings of the workshop can be obtained by sending an email to the chairman of the workshop Han Vinck (vinck@exp-math.uni-essen.de). A list of the presentations follows:

Rolf Johannesson (University of Lund): Convolutional Codes, Encoders and Syndrome Formers: Old and New

A. J. Han Vinck (University Essen): The Inverse Problem

Armin Häutle, H. Dietrich, Martin Bossert, S. Shavgulidze (University of Ulm): Generalized Concatenated Convolutional Codes with Systematic Encoding of Partitioned Subcodes

Ewa Hekstra-Nowacka, Ludo Tolhuizen (Philips Research Eindhoven): Some Results on Serially Concatenated Codes

Jossy Sayir (ETH Zürich): Arithmetic Channel Coding

Per Stahl, Rolf Johannesson, John B. Anderson (University of Lund): Some Results on Tailbiting Encoders

John B. Anderson (University of Lund): A BCJR Method for Finding Tailbiting Convolutional Encoders with Minimum Bit Error Rate

Arie Koppelaar, Stan Baggen, Ewa Hekstra-Nowacka (Philips Research Eindhoven): A GSM Adaptive Multi-Rate System

Rolf Johannesson, John B. Anderson, and Per Stahl

Stan Baggen, Martin Bossert, Ludo Tolhuizen, Ulrich Sorger

Birgit Kull (IMST, Kamp-Lintfort): Coding for a Broadband Multicarrier Wireless LAN

Marat V. Burnashev (IPPI, Moskau): On some Inequalities Useful for Decoding Error Performance Evaluation

Yuri V. Svirid (University of Ulm): How Close are Convolutional Codes to Random Codes

Vladimir Balalkirski (St. Petersburg): Some Distance Properties of Mixed Convolutional Codes

Stefan Host, Rolf Johannesson, Victor V. Zyablov (University of Lund): Decoding of Woven Convolutional Codes with Outer Warp - Preliminary Results

Ulrich Sorger, Jürgen Winter (University Darmstadt): Block-Matrix Representation of Convolutional Codes

Walter Schnug, Michael Lentmaier (University of Ulm and Lund): Generalized Low-Density Parity-Check Convolutional Codes with Hamming Component Codes

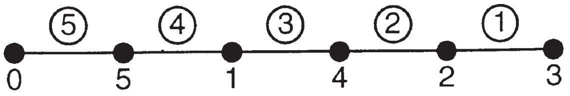
GOLOMB'S PUZZLE COLUMN™

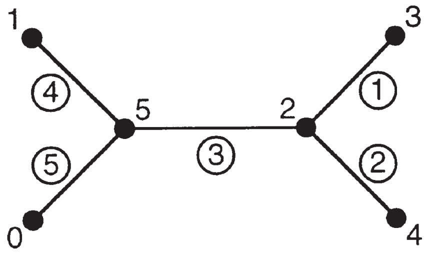
Solutions to "Graceful Graphs"

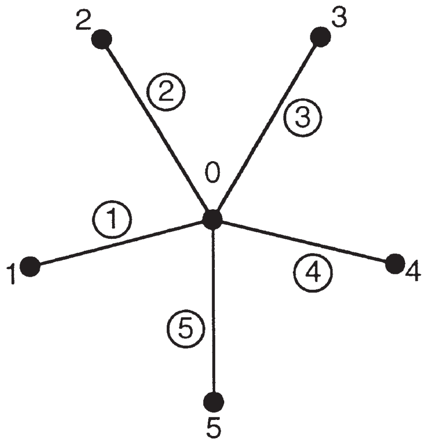
Solomon W. Golomb

Problems 1, 2, and 3 asked for "graceful numberings" of specified graphs.

1.

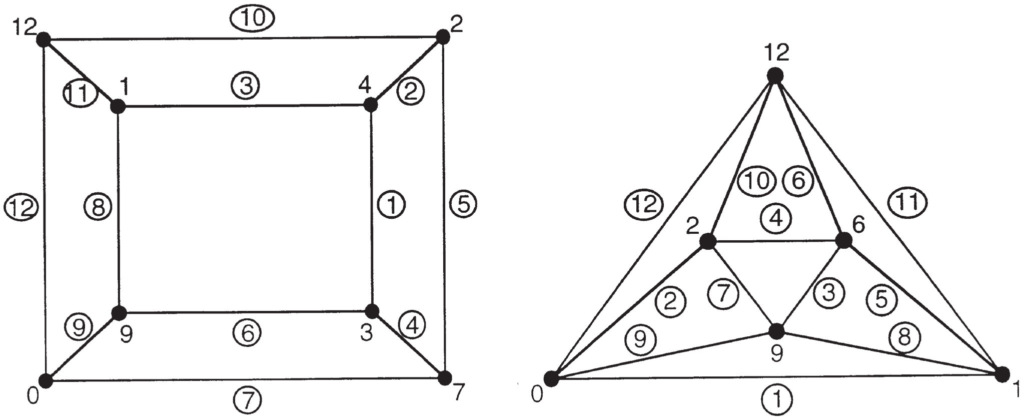






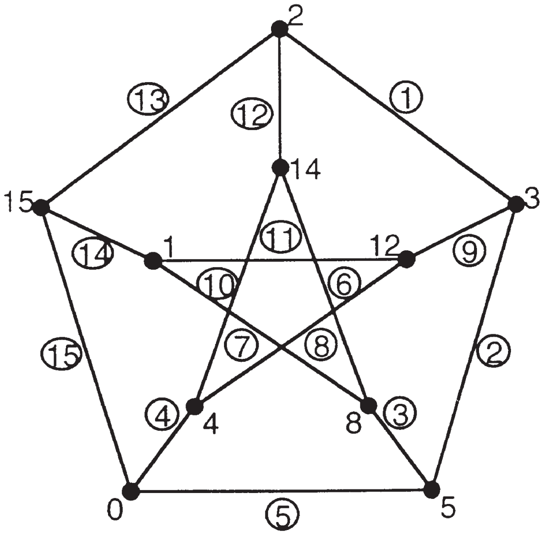
Note: It is widely conjectured that all trees are graceful.

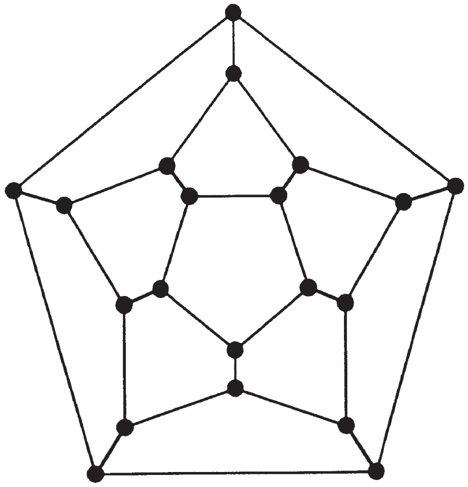
2.



Graceful numberings of the cube and the octahedron.

3.

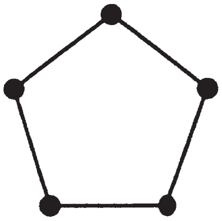
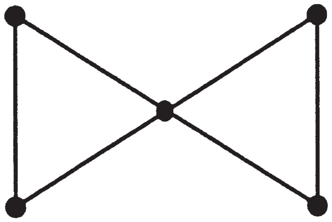
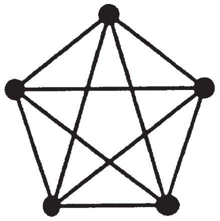




The Peterson Graph is graceful. Is the regular (pentagonal) dodecahedron?

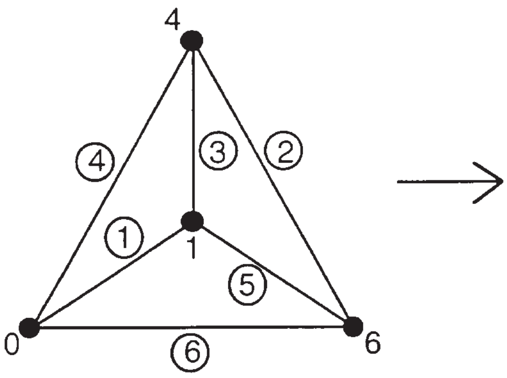
4. Suppose G has an Euler circuit, and as we traverse it we encounter the successive vertex numbers $a_1, a_2, a_3, \ldots, a_e$, where a, will be followed by a_1. (Some vertices may occur more than once in an Euler circuit.) Then the successive edge labels will be $b_1 = |a_1 - a_2|$, $b_2 = |a_2 - a_3|, \ldots, b_{e-1} = |a_{e-1} - a_e|$, and $b_e = |a_e - a_1|$. If G is graceful, then $\{b_1, b_2, \ldots, b_e\}$ must be the numbers $\{1,2,\ldots, e\}$ in some order. Hence, $b_1 + b_2 + \ldots + b_e = 1 + 2 + \ldots + e = \binom{e+1}{2} = e(e+1)/2$. Now, we have $|x - y| \equiv x - y \pmod{2}$, so that $\binom{e+1}{2} \equiv b_1 + b_2 + \ldots + b_e \equiv (a_1 - a_2) + (a_2 - a_3) + \ldots + (a_{e-1} - a_e) + (a_e - a_1) \equiv 0 \pmod{2}$, from which $\binom{e+1}{2}$ must be *even*. However, if either $e \equiv 1 \pmod{4}$ or $e \equiv 2 \pmod{4}$, then $\binom{e+1}{2}$ is *odd*, and G cannot be graceful.

5. The three graphs with ≤ 5 vertices which cannot be graceful by the previous result are:

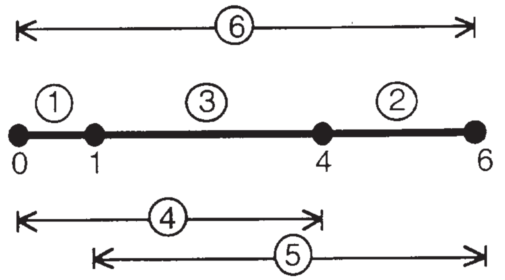
 ,  ,  .

(It turns out that all other connected simple graphs with≤ 5 vertices *are* graceful.)

6. To prove that K_n, the complete graph on n vertices, cannot be graceful if n ≥ 5, we first observe that a graceful numbering of K_n is equivalent to a "perfect ruler" with n marks. A *perfect ruler with n marks* is a sequence of integers $0 = m_1 < m_2 < m_3 < \ldots < m_n = L = \binom{n}{2}$ where the differences $m_j - m_i$, with $1 \le i < j \le n$, take every value from 1 to $\binom{n}{2}$ exactly once. The numbers $m_1, m_2, \ldots, m_n$ correspond to the vertex numbers on K_n, and the "measured distances" $m_j - m_i$ correspond to the edge labels on K_n. This correspondence is illustrated with $n = 4$, the longest n for which K_n has a graceful numbering:



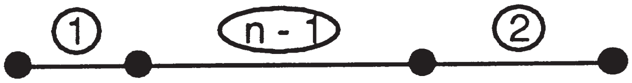
A graceful numbering of K_4.



The "perfect ruler" measures every distance from 1 to $\binom{4}{2}$ =6 in exactly one way.

To prove that a perfect ruler has at most $n = 4$ marks, we call the lengths between consecutive marks "intervals." (In the illustration, the intervals of the ruler are 1, 3, and 2.) For a perfect ruler, these *interval*s must be 1, 2, ... $n - 1$ in some order, because they are $n - 1$ distinct positive integers which sum to $L = \binom{n}{2}$, the length of the ruler. Where can the interval "1" occur? If it is next to an interval "k", then $k + 1$ is a measured distance on the ruler which is not an interval. But every length from 1 to $n - 1$ already occurs as an interval, so $k + 1$ must exceed $n - 1$, which means $k \geq n - 1$. But the *longest* interval is $n - 1$, so the only interval neighbor for "1" is "$n - 1$ ", which also requires the interval "1" to be at one end of the ruler.

Next, we ask what neighbors the interval "2" can have. If "k" is a neighbor of "2", then $k + 2 > n - 1$, because every length from 1 to $n - 1$ is already measured as an interval. But the length "n" is also already measured as $1 + (n - 1)$, a sum of two adjacent intervals. Therefore $k + 2 > n$, and again $k \geq n - 1$, which means that the only possible neighbor of the interval "2" is the interval "$n - 1$" , and "2" is also at an end of the ruler.
This reduces to:



as the entire ruler. (For $n = 4$, it is the perfect ruler corresponding to the graceful numbering of K_4, already illustrated.) For $n > 4$, no perfect ruler, and no graceful numbering of K_n, can exist.

References

1. S.W. Golomb, How to number a graph", in *Graph Theory and Computing*, Academic Press, Inc., New York, 1972, pp. 23-37.

2. G.S. Bloom and S.W. Golomb, " Applications of numbered undirected graphs", *Proc. IEEE*, vol. 65, no. 4, April, 1977, pp. 562-570.

ISIT'98 Plenary Lecture Report . . .

continued from page 5

Evasive Boolean Functions

Deterministic and Randomized Decision Trees

In this section we consider the problem of evaluating a boolean function F of n variables. Each variable x_i ranges over the set {0,1}, and the range of the function is {0,1}. We are interested in adaptive algorithms which evaluate F by questions of the form `$x_i = 1$?'. Such an algorithm is called a *decision tree*. The complexity of a decision tree is the worst-case number of questions asked. The complexity of F is the least complexity of any decision tree for F. The function $F(x_1, x_2, \ldots, x_n)$ is called *evasive* if it has complexity n; i.e., if, for every decision tree T for F, there is an input $(x_1, x_2, \ldots, x_n) \in \{0,1\}^n$ which causes all possible questions to be asked.

We also consider randomized decision trees, in which random coin tosses can be used to determine the next question to ask. The complexity of a randomized decision tree for F is the maximum, over all inputs $(x_1, x_2, \ldots, x_n) \in \{0,1\}^n$, of the expected number of questions required to determine $F(x_1, x_2, \ldots, x_n)$. The randomized complexity of F is the least complexity of any randomized decision tree for F.

There are evasive boolean functions whose randomized complexity is much smaller than n; in this sense, randomized decision trees are more powerful than deterministic ones. As an example, consider the sequence of functions $\{M_t\}$ defined inductively as follows:

1. M_t is a function of 3^t variables.
2. M_1 is the majority function; *i.e.*, $M_1(x, y, z)$ is equal to 1 if at least two of its inputs are equal to 1, and is equal to 0 otherwise.
3. For $t = 2, 3, \ldots$, $M_t(\vec{x}, \vec{y}, \vec{z}) = M_1(M_{t-1}(\vec{x}), M_{t-1}(\vec{y}), M_{t-1}(\vec{z}))$, where $\vec{x}$, $\vec{y}$ and $\vec{z}$ are sequences of 3^{t-1} boolean variables.

Let us show that M_1 is evasive. To do so, we construct an *adversary*; *i.e.*, a rule for answering the questions which forces the algorithm to ask all possible questions. This is quite easy: the adversary answers 'Yes' to the first question and 'No' to the second; these answers do not determine the function value, and thus force the algorithm to ask a third question. On the other hand, if the algorithm presents the questions in a random order then, for every input (x_1, x_2, x_3), there is at least a 1/3 chance that the first two inputs queried will be equal, in which case the third question is unnecessary. Thus the randomized complexity of M_1 is 8/3, rather than 3.

By constructing a suitable adversary one can show that, for every t, M_t is evasive; *i.e.*, its complexity is 3^t. On the other hand, we shall show by induction on t that the randomized complexity of M_t is at most 8/3. Assume the result for $t-1$. To evaluate $M_t(\vec{x}, \vec{y}, \vec{z})$, consider the subfunctions $M_{t-1}(\vec{x})$, $M_{t-1}(\vec{y})$ and $M_{t-1}(\vec{z})$ in a random order and, recursively, evaluate the first two of these subfunctions; with probability at least 1/3, the third subfunction will not need to be evaluated. Thus the expected number of subfunction evaluations is at most $(8/3)^{t-1}$, and the expected number of questions to evaluate a subfunction is at most $(8/3)^{t-1}$ by induction hypothesis.

Evasive Graph Properties

We consider the problem of testing whether a graph G has some property such as being connected, planar or eulerian by asking questions of the form 'Is there an edge between vertices u and v ?'. If we fix the number of vertices at n then each graph G can be represented by a characteristic vector $\chi(G) \in \{0,1\}^{\binom{n}{2}}$. This vector has a component for each pair of distinct vertices; the component is 1 if the vertices are joined by an edge, and 0 if they are not. The graph property thus determines a boolean function F of $\binom{n}{2}$ variables defined as follows: $F(\chi(G)) = 1$ if G has the property, and $F(\chi(G)) = 0$ otherwise. A graph property is called *evasive* if F is evasive. Thus a property of n-vertex graphs is evasive if, in the worst case, it is necessary to test all $\binom{n}{2}$ potential edges in order to determine whether the property holds.

A graph property is called *intrinsic* if it remains invariant under permutations of vertex names; (i.e., it depends only on the isomorphism type of the graph. The property is called *monotone* if, whenever the property holds for a graph G, it continues to hold when G is augmented by the addition of a new edge. The property is called *nontrivial* if it holds for at least one graph and fails to hold for at least one graph. Some years ago I made the reckless conjecture that every intrinsic, monotone, nontrivial graph property is evasive. The conjecture remains open; it has been shown to hold when the number of vertices is a prime power [12].

Communication Complexity

Communication complexity measures the number of bits that must be transmitted when k parties must share information in order to solve a computational problem. The subject was founded by Andrew Yao in 1979 [18]. The monograph [14] gives an excellent survey of the subject.

Here we restrict ourselves to two-party communication complexity. Suppose Alice knows x, Bob knows y, and together they must determine $f(x, y)$, where f is a function known to both. They communicate in rounds, where, in each round, Alice sends a bit to Bob and, simultaneously, Bob sends a bit to Alice. How many rounds are required in order for both parties to know the function value? The subject is largely concerned with deriving lower bounds on the number of rounds required by deterministic and randomized protocols for such problems.

The following example illustrates that communication complexity problems sometimes have surprisingly efficient solutions. Each party has a multiset consisting of n k-bit numbers, where n is a power of 2. Their goal is to determine the n th-smallest element of the union of the two multisets. It is not too difficult to find a protocol that terminates within $k+O(log^2 n)$ rounds. Surprisingly, there is a protocol that requires only $k+\log_2 n$ rounds.In the first round each party sends the most significant bit of the $(n/2)$ th smallest of his or her numbers. If the bits agree then the most significant bit of the answer is known and the parties proceed to determine the remaining $k-1$ bits of the answer. If the bits disagree then the party who transmitted a 0 discards his or her smallest $n/2$ numbers, the party who transmitted a 1 discards his or her largest $n/2$ numbers, and they proceed to determine the $(n/2)$th smallest of the remaining numbers. Continuing in this way, each round either determines one more bit of the answer or eliminates half the numbers.

Schulman [16] extended the two-party communication complexity model to the case where the parties communicate over a noisy channel. Given a noiseless t -round protocol, it is easy to see that $O(t\log t)$ rounds suffice to simulate the protocol over a binary symmetric channel with exponentially small probability of error; each bit is sent $O(logt)$ times, and the receiver takes the more frequently occurring value. Using a subtle construction based on tree codes, Schulman shows that $O(t)$ bits suffice. This result generalizes a fundamental result of Shannon [17] for the case of one-way communication.

References

1. M. Ajtai, J. Komlós and Szemerédi, “An $O(n\log n)$ sorting network,” Proc. of 15th ACM Symposium on Theory of Computing, pp. 1-9, 1983.

2. D.J. Balding, W.J. Bruno, E. Knill and D.C. Torney, “A Comparative Survey of Non-Adaptive Pooling Designs,” Institute for Mathematics and its Applications, Vol. 81, pp. 133-154, 1996.

3. E.R. Berlekamp, “Block coding for the binary symmetric channel with noiseless, delayless feedback,” Error-Correcting Codes, edited by H.B. Mann, Wiley and Sons, pp. 61-88, 1968.

4. D.-Z. Du and F.K. Hwang, Combinatorial Group Testing and its Applications, World Scientific, 1993.

5. M. L. Fredman, “How good is the information theory bound in sorting,” Theoretical Computer Science, Vol. 1, pp. 355-361, 1976.

6. E.N. Gilbert and E.F. Moore, “Variable-length binary encodings,” Bell System Technical Journal, Vol. 38, pp. 933-967, 1959.

7. W. Goddard, V. King and L. Schulman, “Optimal randomized algorithm for local sorting and set maxima,” Proc. of 22nd ACM Symposium on Theory of Computing, pp. 45-53, 1990.

8. T.C. Hu and A.C. Tucker, “Optimal computer search trees and variable-length alphabetical codes,” SIAM J. Appl. Math., Vol. 21, No. 4, pp. 514-523, 1971.

9. D.A. Huffman, “A method for the construction of minimum-redundancy codes,” Proc. of the IRE, Vol. 40, pp. 1098-1101, 1952.

10, F.K. Hwang, “A method for detecting all defective members in a population by group testing,” J. Amer. Statist. Assoc., Vol. 67, pp. 605-608, 1972.

11. J. Kahn and M. Saks, “Balancing poset extensions,” Order, Vol. 1, pp. 113-126, 1984.

12. J. Kahn, M. Saks and D. Sturtevant, “A topological approach to evasiveness,” Combinatorica, Vol. 4, pp. 297-306, 1984.

13. D.E. Knuth, The Art of Computer Programming, Vol. 3, Sorting and Searching, Addison Wesley, 1973.

14. E. Kushilevitz and N. Nisan, Communication Complexity, Cambridge University Press, 1997.

15. P.A. Pevzner, personal communication, 1998.

16. L.J. Schulman, “Deterministic coding for interactive communication,” Proc. of 25th ACM Symposium on Theory of Computing, pp. 747-756, 1993.

17. C.E. Shannon, “A mathematical theory of communication,” Bell System Technical Journal, Vol. 27, 379-423, 623-656, 1948.

18. A.C. Yao, “Some complexity questions related to distributed computing,” Proc. of 11th ACM Symposium on Thory of Computing, pp. 209-213, 1979.

Conference Calendar

DATE	CONFERENCE	LOCATION	CONTACT/INFORMATION	DUE DATE
March 15–19 1999:	IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP)	Phoenix, Arizona	Conference Management Services 3109 Westchester Ave. College Station, Texas 77845-7919 Tel: (409) 693-6000 email: mercer@conf-mgmt.com http://icassp99.asu.edu	
March 17-19, 1999	CISS '99 Conference on Information Sciences and Systems	Johns Hopkins University, Baltimore, MD	1999 CISS 105 Barton Hall Dept. of Electrical and Computer Engineering Johns Hopkins University Baltimore, MD 21218 Tel: (410)516-7033, Fax: (410)516-5566 Web: http://www.ece.jhu.edu/ciss99/.	
March 29-31, 1999	1999 Data Compression Conference (DCC'99)	Snow Bird, Utah USA	http://www.cs.brandeis.edu/~dcc/	
March 30 - April 1, 1999	PLC'99: 3rd International Symposium on Power-Line Communications	Lancaster House Hotel, Lancaster, UK,	Dr Nader Zein Communications Research Centre Lancaster University Lancaster, LA1 4YR Fax: 44 1524 594207 E-mail: n.zein@lancaster.ac.uk	
June 14-16, 1999	IEEE Signal Processing Workshop on Higher-Order Statistics	Ceasarea, Israel.	Hagit Messer-Yaron Dept. of EE - Systems Tel-Aviv University Tel-Aviv 69978, ISRAEL e-mail: messer@eng.tau.ac.il URL: http://sig.enst.fr/ ~hos99/	
June 15-18, 1999	1999 Canadian Workshop on Information Theory	Kingston, Ontario, Canada	Prof. F. Alajaji Dept. of Mathematics & Statistics Queen's University Kingston, Ontario K7L 3N6, Canada Tel: (613) 545-2423, Fax: (613) 545-2964 Email: fady@polya.mast.queensu.ca Web: http://markov.mast.queensu.ca/~fady/ CWIT99/cwit99.html	
June 20–25, 1999	1999 Information Theory Workshop Kruger National Park, South Africa	Kruger National Park, South Africa	Prof. Hendrik C. Ferreira Dept. of Electrical Engineering Rand Afrikaans University P.O. Box 524 Auckland Park, 2006, South Africa E-mail: hcf@ing1.rau.ac.za Web page: http://www.wits.ac.za/ITW99	
June 27– July 1, 1999	1999 Information Theory and Networking Workshop	Metsovo, Greece	Prof. Wojciech Szpankowski Department of Computer Science Purdue University W. Lafayette, IN 47907, USA Email: spa@cs.purdue.edu Tel: (765) 494 6703, Fax: (765) 494 0739 Web: http://www.cs.purdue.edu/ homes/spa/itw99.html	

Conference Calendar

DATE	CONFERENCE	LOCATION	CONTACT/INFORMATION	DUE DATE
July 11-16, 1999 :	5-th International Symposium on Communication Theory and Applications (ISCTA’99)	Charlotte Mason College, Ambleside, Lake District, UK	P. G. Farrell Communications Research Centre Faculty of Applied Sciences Lancaster University Lancaster LA1 4YR UK Tel: 44 1524 593427/594141 Fax: 44 1524 594207 Email: p.g.farrell@lancaster.ac.uk	
August 2–13, 1999	Workshop on “Codes, Systems and Graphical Models”	Minneapolis, Minnesota, USA	http://www.ima.umn.edu/csg	
September 22-24, 1999	37-th Annual Allerton Conference on Communication, Control, and Computing	Monticello, Illinois, USA	37-th Annual Allerton Conference Coordinated Science Laboratory University of Illinois 1308 W. Main Street Urbana, Illinois 61801-2307 USA Email: allerton@csl.uiuc.edu Web: http://www.comm.csl.uiuc.edu/allerton/	July 14, 1999
November 14-19, 1999.	13th AAECC Symposium on Applied Algebra, Algebraic Algorithms, and Error-Correcting Codes	Honolulu, Hawaii, USA	Prof. Marc Fossorier University of Hawaii Dept. of Electrical Engineering 2540 Dole St., # 483 Honolulu, HI 96822, USA E-mail: marc@spectra.eng.hawaii.edu Web: http://www.irit.fr/ACTIVITES/ AAECC/aaecc13.htm	
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	September 15, 1999

IEEE

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

Information Theory
Society Newsletter