IEEE Information Theory Society Newsletter

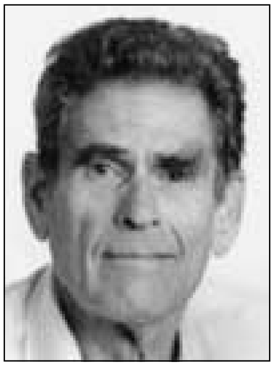
Vol. 52, No. 1, March 2002 Editor: Lance C. Pérez ISSN 1059-2362

OBITUARY

Peter Elias, 1923–2001

By James L. Massey

On December 7, 2001, the field of information theory lost another of its true giants, Peter Elias, who passed away at his home in Cambridge, Massachusetts, a victim of the mysterious and dreadful ailment, Creutzfeld-Jakob Disease.


Peter Elias

Five years ago in his tribute to Shannon in this *Newsletter*, Peter described his initiation into information theory in this way. "Fifty years ago I had completed a Master's program in computation and further coursework at Harvard and was looking for a doctoral thesis topic when Shannon's paper came out. It was an amazing piece of work. ... I was fascinated, finished a thesis in information theory in 1950 and have continued working in the domain ever since, the first three years as a Harvard postdoc and since 1953 at MIT. I joined a group that Bob Fano, who had explored some of the same questions, was starting in Jerry Wiesner's Research Laboratory of Electronics. Shannon came to MIT from Bell Labs for a visit in 1956, and came to stay in 1958: he gave a wonderful advanced topics course, opening new topics in many of the sessions, and was always open for discussion. It was a wonderful environment for graduate students and faculty."

In those fifty-plus years of immersion therein, Peter contributed a wealth of fundamental results to information theory. When one looks into any of the breakthrough developments in communications over the past 50 years, one is almost sure to find one of his contributions at its base. We cite here only a few instances.

One of Peter's most remarkable papers is "Coding for Noisy Channels," which he published in the 1955 IRE Convention Record–and nowhere else, Peter was never one to artificially enlarge his publication list. This paper has the honor of appearing in both 1974 IEEE Press books, *Key Papers in the Development of Information Theory* (Ed. D. Slepian) and *Key Papers in the Development of Coding Theory* (Ed. E. R. Berlekamp) [but unfortunately its very insightful figures are missing in the latter].

Hamming had already introduced "parity-check codes," but Peter went a giant step farther by showing for the binary symmetric channel that such *linear codes* suffice to exploit a channel to its fullest. In particular, he showed that "error probability as a function of delay is bounded above and below by exponentials, whose exponents agree for a considerable range of values of the channel and the code parameters" and that these same results apply to linear codes. These exponential error bounds presaged those obtained for general channels ten years later by Gallager. In this same paper Peter introduced and named "convolutional codes". His motivation was to show that it was in principle possible, by using a convolutional code with infinite constraint length, "to transmit information at a rate equal to channel capacity with probability one that no decoded symbol will be in error."

In his error-free coding, Peter exploited the fact that the codewords in a convolutional code have a tree structure that allows the decoder to use as much or as little of the code length as it wishes to reduce decoding effort to what is needed for a desired error probability. This real-

continued on page 3

From the Editor

Lance C. Pérez

In this issue of the *IEEE Information Theory Society Newsletter* we must once again mark the passing of a Society luminary, Peter Elias. Jim Massey has written an obituary for Peter recounting his numerous contributions as a scientist and a human being.

This issue also contains an article by Venkat Guruswami and Madhu Sudan on their paper "Improved Decoding of Reed-Solomon and Algebraic-Geometric Codes" which was awarded the 2000 IEEE Information Theory Society Prize Paper Award. It is fitting that this paper draws impetus from the work of Elias on list decoding.

Finally, while working on the Newsletter digital library, I noticed that the Society has discussed the notion of an Information Theory magazine for at least the past twenty years. The primary purpose of the magazine would be to feature more technical articles than the *IT Newsletter* has traditionally offered. The budget difficulties of the IEEE and the subsequent financial demands placed on the technical societies prohibits the creation of a magazine for now. In the meantime, I am interested in trying to increase the technical content of the *IT Newsletter* and would welcome any suggestions on the best way to accomplish this.

Lance C. Pérez

Please help 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**
June 2002	April 12, 2002
September 2002	July 16, 2002

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

I may be reached at the following address:

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

Sincerely,
Lance C. Pérez

IEEE

Information Theory Society Newsletter

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

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

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

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

Table of Contents

Letter to the Editor

Followup on ArXiv E-Print Service

In his announcement in the June 2001 issue of *IT Newsletter*, Joachim Hagenauer points out that in physics it is standard for people to place their papers on the ArXiv e-print server as soon as they are completed, and usually before they are submitted to a journal.

He urges members of the Information Theory Society to do the same, placing their papers in a subsection of the archive devoted to Information Theory. I fully support this suggestion.

Joachim concludes by saying that once a paper has appeared in the "IT Transactions" then it should be removed from the ArXiv server. In this context I should like to point out that this is not the practice in physics, mathematics or computer science; normally papers remain on the ArXiv (one hopes) forever. Indeed, the name of the ArXiv is the ArXiv E-print Server, not Preprint Server.

Furthermore, there is a growing movement among scientists to put pressure on publishers to allow papers that have appeared in their journals to be distributed freely by independent, online public libraries of science such as the ArXiv e-print library. This movement is spear-headed by a non-profit organization called the "Public Library of Science" (www.publiclibraryofscience.org). These developments have been reported in recent issues of "Nature" (see for example "Nature," Sept. 6, 2001, page 6). Already a number of publishers in medicine, physics, mathematics and computer science (e.g. the Association for Computing Machinery) have agreed.

For a more extensive discussion of these matters, see the "Nature" on-line forum on electronic access:

www.nature.com/nature/debates/e-access/.

The article by Steve Lawrence of NEC Research, Princeton, is especially compelling. It gives the results of a scientific study which shows that an article that is available on-line is 3 to 5 times as likely to be cited as an article that is only available in print. To quote my former colleague Andrew Odlyzko, "when more scholars become aware of this evidence, the move to make papers easily available will snowball."

Neil J.A. Sloane
Information Sciences Research
AT&T Shannon Laboratory
180 Park Avenue
Florham Park, NJ 07932

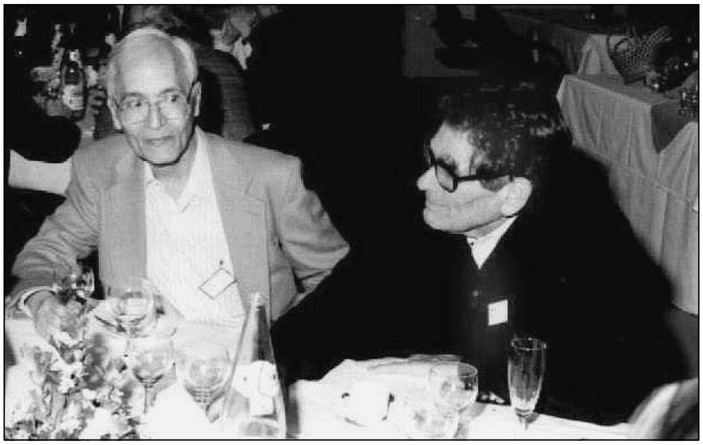
Peter Elias, 1923–2001

Continued from page 1

ization led directly to the invention of *sequential decoding* by J. M. Wozencraft in his 1957 MIT doctoral thesis. Sequential decoding of convolutional codes became the first coding system used on a deep-space mission (Pioneer 9 in 1969) and soon became the NASA standard coding system for deep-space.

Peter was also the inventor of product codes and interative decoding of such codes, which as he demonstrated in his 1954 paper [1] [which is also reprinted in *Key Papers in the Development of Coding Theory*] can obtain bit-error probability arbitrarily close to zero on the binary symmetric channel with practical decoding effort when a product of sufficiently many Hamming codes is used, provided the overall rate is less than a certain number smaller than channel capacity. Peter used iterative decoding in a single-pass fashion, but this provided the starting point for other developments such as low-density parity-check codes, developed by R. G. Gallager in his 1960 MIT doctoral thesis which Peter supervised, that iterate over multiple passes. The most recent and dramatic breakthrough in coding techniques, Berrou and Glavieux's turbo codes, is a further evolution of Peter's basic idea. Convolutional codes and iterative decoding are again used, but operation at rates very close to channel capacity is obtained by a very clever scheme for interleaving the codes.

Peter also contributed fundamental new concepts and techniques to source coding. His widely cited 1975 paper [11] introduced universal representations of the integers, showing that the integers could be coded with binary codewords hav-



Peter Elias (right) with Jacob Ziv at the Monte Verita Symposium in Ascona, Switzerland, February 1994.

ing the crucial property that no codeword is the prefix of another but with virtually no expansion of their length from that in standard binary coding. Peter was not the first to work on universal source coding, but his approach was so simple and insightful that it has influenced much, if not all, of subsequent research in universal source coding. One such further development came in Peter's own 1988 paper [14] that gave practical and ingenious methods for compressing any stationary source down to its entropy (essentially by coding how long it has been since the current source symbol was last observed rather than by coding the symbol itself) and that provided many ideas which have been incorporated into later universal coding schemes.

Peter was a fundamental contributor to communication networks as well. His 1967 paper [8] treated networks of Gaussian channels with enough depth and originality to merit inclusion in *Key Papers in the Development of Information Theory*. His 1956 brief note [4], joint with A. Feinstein and Shannon, is an acknowledged jewel of the field that gives the celebrated max-flow min-cut theorem for networks.

Peter received the highest honor of the IEEE Information Theory Society, the Shannon Award, in 1977 and was the Shannon Lecturer at the International Symposium on Information Theory (ISIT) that year. His Shannon Lecture was vintage Elias. He showed that the simple binary erasure channel incorporated all the essentials that are needed to understand coding for noisy channels. The IEEE Information Theory Society honored Peter for his invention of convolutional codes at the 1998 ISIT with a Golden Jubilee Award for Technological Innovation. Among his other honors, Peter was a Fellow of the IEEE and of the American Association for the Advancement of Science, and a member of the U. S. National Academy of Engineering, the U. S. National Academy of Science and the American Academy of Arts and Sciences. In one of those cruel ironies of fate, Peter has been awarded the 2002 IEEE Hamming Medal, one of the major medals of the IEEE. These medals cannot be awarded posthumously but Peter was still alive when the awards were confirmed by the IEEE Board of directors–it is uncertain whether Peter himself learned about this award before his death.

Peter is a past President of the IEEE Information Theory Society. Among his many other *pro bono* activities, Peter served on the President's Science Advisory Committee panel on Computers in Higher Education and as a member of the Education and Accreditation Committee of the Engineer's Council on Professional Development. In 1957 he was one of the three founding editors of *Information and Control* (now *Information and Computation*) and remained a member of its editorial board until his death. He also served on the editorial boards of the MIT Press, the *Proceedings of the IEEE* and the *IEEE Spectrum*.

Peter was born on Nov. 23, 1923 in New Brunswick, New Jersey. His father was an engineer in Thomas A. Edison's laboratory. Peter attended Swarthmore College for two years before transferring to MIT in 1942. Upon receiving a bachelor's degree in business and engineering management in 1944, Peter enlisted in the U. S. Navy where he served as a radio technician instructor. After his discharge in 1946, he earned two master's degrees and a doctorate from Harvard University, the latter in 1950. From 1950 to 1953, he was a Junior Fellow in the Society of Fellows at Harvard University. Peter joined the MIT faculty in 1953 as an assistant professor. He became an associate professor in 1956 and a full professor in 1960, the year he became the youngest person to head the electrical engineering department (he served until 1966). Peter assumed emeritus rank at MIT in 1991, but as one of his MIT colleagues, Victor Zue, remarks: "He was one of the most energetic emeritus professors I know–coming to work almost every day and continuing to advise undergraduate students." Peter recently took on the responsibility of organizing the electrical and computer science department's colloquium at MIT. "When he became ill, his son Daniel told me that he was particularly concerned about not being able to discharge his responsibilities," said Zue. "This tells you the kind of person he was."

Peter is survived by two sons, Daniel of Lincoln, Mass., and Paul of Cambridge; a daughter, Ellen Elias-Bursac of Cambridge; and six grandchildren. Peter's wife of 43 years, Marjorie (Forbes), whom we all knew better as "Midge", died suddenly in 1993 from a heart attack, a loss that had weighed heavily on Peter until his own death.

On a personal note, after forty years, I still remember Peter's assistance to me as an MIT doctoral student from 1959 to 1962. He was an eager and interested listener to what I said during examinations or presentations, which greatly bolstered my confidence and he always had some wise words for me. I suspect that it was this open and unselfish aspect of his character that caused the electrical engineering department at MIT to saddle him with the heavy burden of being Head during six years when his research skills were at their peak. He was a splendid Head, but I cannot help but wonder how much greater his technical contributions, remarkable as they are, would have been if he had not been so sidetracked. Throughout his career, Peter gave unstintingly of himself to MIT and to his profession.

Peter closed his above-cited tribute to Shannon with these words: "My favorite paper by Shannon since 1948 is 'Prediction and Entropy of Printed English'–a delightful example of the playful diversity of his approach, particularly in the identical twin coding scheme for estimating the entropy of English. ... I miss that playfully creative mind." Peter Elias's mind and person will be sorely missed by all of us who work in information theory.

James L. Massey

Publications by Peter Elias in the *IEEE Trans. Inform. Theory*

[1] Elias, P., "Error-free Coding," Sep. 1954, pp. 29 - 37.

[2] Elias, P., "Predictive Coding–I," Mar. 1955, pp. 16 - 24.

[3] Elias, P., "Predictive Coding–II," Mar. 1955, pp. 24 - 33.

[4] Elias, P., Feinstein, A. and Shannon, C. E., "A Note on the Maximum Flow through a Network," Dec. 1956, pp. 117 - 119.

[5] Elias, P., "Two famous papers" (Editorial), Sep. 1958, p. 99.

[6] Elias, P., "PGIT in 1960" (Editorial), Dec. 1959, p. 149.

[7] Elias, P., "Progress in Information Theory in the USA, 1957-1960," July 1961, pp. 128 - 144.

[8] Elias, P., "Networks of Gaussian Channels with Applications to Feedback Systems," July 1967, pp. 493 - 501.

[9] Elias, P., "Bounds on Performance of Optimum Quantizers," Mar. 1970, pp. 172 - 184.

[10] Elias, P., "Distinguishable Codeword Sets for Shared Memory," July 1975, pp. 392 - 399.

[11] Elias, P., "Universal Codeword Sets and Representations of the Integers," Mar. 1975, pp. 194 - 203.

[12] Brown, D. J. and Elias, P., "Complexity of Acceptors for Prefix Codes," May 1976, pp. 357 - 359.

[13] Elias, P., "Minimax Optimal Universal Codeword Sets," July 1983, pp. 491 - 502.

[14] Elias, P., "Interval and Recency Rank Source Coding: Two On-line Adaptive Variable-length Schemes," Jan. 1987, pp. 3 - 10.

[15] Elias, P., "Zero Error Capacity under List Decoding," Sep. 1988, pp. 1070 - 1074.

President's Column

Tom Fuja

It is my pleasure and honor to serve as president of the IEEE Information Theory Society for 2002. I joined this Society as a graduate student twenty years ago, and it's been my technical home ever since. The hallmarks of the IT Society have always been the highest technical standards and a welcoming environment for young researchers; it's a privilege to serve such a group.

Tom Fuja

I would like to begin my first President's Column by expressing my sincere thanks to my predecessor, Joachim Hagenauer. Joachim served as Society president during one of its most difficult years – a year that saw the death of the founder of information theory, Claude Shannon, as well as financial tribulations visited upon our society by the IEEE. (See below.) Joachim carried out the role of President with vigor and aplomb, and I am glad for having had the chance to watch and learn.

There are three items I will touch on in this column: the scheduling of symposia, the Society's ongoing financial concerns, and Society volunteers for 2002.

Symposium: An Annual Event?

Until the summer of 2001, the International Symposium on Information Theory was held twice every three years. Typically, this meant that our society's main conference was held:

- Outside North America in the summers of years equivalent to two modulo three. (E.g., Sorrento in 2000, Ulm in 1997, Trondheim in 1994, Budapest in 1991, etc.)
- In North America late in the years equivalent to zero modulo three or early in the years equivalent to one modulo three. (E.g., Cambridge in August 1998, Whistler in September 1995, San Antonio in January 1993, San Diego in January 1990, etc.)

However, beginning with the Washington DC symposium in 2001, we initiated an annual ISIT schedule. Currently, ISITs are planned for late-June or early-July for the next three summers – Lausanne in 2002, Yokohama in 2003, and Chicago in 2004.

The reasons for the change to a yearly schedule included these:

- There is enough good-quality work being generated to justify a yearly meeting.
- A yearly meeting would, presumably, mean each ISIT would be somewhat smaller, with fewer parallel sessions and a better chance to see the talks one really wanted to see.
- Having the ISIT (approximately) the same time every year – like most technical conferences – makes planning simpler, both for the ISIT and for other conferences seeking to attract some of the same audience.

The Board of Governors instituted this change on a provisional basis, with the understanding that the advisability of a yearly schedule would be reconsidered when we had enough experience to make an informed decision. Now that we've had one "cycle" to evaluate the yearly schedule, it's clear that there are some shortcomings. One complaint that was heard during the planning of ISIT '01 was that too little time elapsed between the end of ISIT '00 and the submission date for ISIT '01; certainly, a yearly schedule means a more compressed timetable for organizers and authors alike. In addition, it's not at all clear that the goal of a "smaller, gentler" ISIT was achieved; while ISIT '01 was the smallest ISIT in recent memory, the number of submissions to ISIT ’02 has skyrocketed to over 700. (Of course, how many submissions would the organizers have received if there were 18 months between ISIT ’01 and ISIT ’02?)

In any case, the Board plans to re-evaluate this policy at its meeting in Lausanne. We would like to hear from as many Information Theory Society members as possible on this issue; please feel free to contact me at tfuja@nd.edu with your input.

IT Society Paying for IEEE Mistakes

As Joachim Hagenauer and Marc Fossorier indicated in their September 2001 Newsletter columns, the Information Theory Society took a substantial financial “hit” in 2000/2001 at the hands of its parent organization, the Institute of Electrical and Electronics Engineers. IEEE Corporate, accustomed to the prodigious stock market gains of the mid-to-late 1990’s, grew to depend on such gains in their yearly budgets; when the market turned downward, they had substantial holes to fill, and they turned to the technical societies to fill them. Why? For the same reason Willy Sutton gave when he was asked why people rob banks – because that’s where the money is.

In early 2001 the Information Theory Society had “long term investments” totaling about $1.2 million dollars. These funds are invested for us by IEEE, and historically they have done quite well; they are used as a “rainy day” fund to let us carry out new initiatives (such as the digital library project) and to protect us during uncertain financial times.

In April 2001, IEEE Corporate appropriated $179,000 from our long-term investment account, made retroactive to December 2000. It is anticipated that they will appropriate at least that much (and quite likely more) in the current fiscal year. Moreover, IEEE is instituting a new financial model that will result in more money flowing from the societies to IEEE Corporate in the future. While the new model is still evolving, there have been analyses of some of the proposed models that show the smaller societies – including ours – could literally be soaked dry of their assets.

The technical societies, through the Technical Activities Board, have made clear to IEEE the need for the parent organization to get its financial house in order in a way that does *not* drive the societies into penury. This is an ongoing effort, and I will provide you with additional information in my next *IT Newsletter* column.

IT Society Volunteers for 2002

The Information Theory Society depends on volunteers to carry out its activities – to edit its publications, balance its budget, nominate and select its award winners, and plan its conferences. Chief among these volunteers for 2002 are our two “Past Presidents” – Vijay Bhargava and Joachim Hagenauer; I’m counting on the wisdom and experience of these two gentlemen in the year ahead. The Society’s two Vice Presidents – Han Vinck and Hideki Imai – chair various committees and will serve as President in 2003 and 2004, respectively. I am pleased that Marc Fossorier has agreed to continue as Society Treasurer; given the unusual state of the Society’s finances, we’re fortunate that Marc was willing to “re-enlist” for another year beyond what has traditionally been the treasurer’s three-year term. Similarly, Aaron Gulliver will continue his considerable duties as Society Secretary. And 2002 will be the first full year for the two recently appointed editors of the Society’s publications – Paul Siegel as editor-in-chief of the *Transactions* and Lance Pérez as editor of the *IT Newsletter.*

Finally, I’d like to welcome the five Society members recently elected (or, in some cases, re-elected) to a three-year term on the Board of Governors; they are Tony Ephremides, Marc Fossorier, Urbashi Mitra, David Neuhoff, H. Vincent Poor, and Bin Yu.

Reflections on “Improved Decoding of Reed-Solomon and Algebraic-Geometric Codes”

*Venkatesan Guruswami**
Madhu Sudan†

A t-error-correcting code over a q-ary alphabet $\mathbb{F}_q$ is a set $C \subseteq \mathbb{F}_q^n$ such that for any received vector $\mathbf{r} \in \mathbb{F}_q^n$ there is at most one $\mathbf{c} \in C$ that lies within a Hamming distance of t from $\mathbf{r}$. The minimum distance of the code C is the minimum Hamming distance between any pair of distinct vectors $\mathbf{c}_1,\mathbf{c}_2 \in C$. In his seminal work introducing these concepts, Hamming pointed out that a code of minimum distance $2t+1$ is a t-error-correcting code. It also pointed out the obvious fact that such a code is not a t'-error-correcting code for any $t'>t$. We conclude that a code can correct half as many errors as its distance and no more.

The mathematical correctness of the above statements are indisputable, yet the interpretation is quite debatable. If a message encoded with a t-error-correcting code ends up getting corrupted in $t'>t$ places, the decoder may simply throw its

*University of California at Berkeley, Computer Science Division, Berkeley, CA 94708. venkat@lcs.mit.edu
†MIT Laboratory for Computer Science, 200 Technology Square, Cambridge, MA 02139, USA. madhu@mit.edu.

hands up in the air and cite the above paragraph. Or, in an alternate notion of decoding, called *list decoding*, proposed in the late 1950s by Elias [10] and Wozencraft [43], the decoder could try to output a list of codewords within distance t' of the received vector. If t' is not much larger than t and the errors are caused by a probabilistic (non-malicious) channel, then most likely this list would have only one element — the transmitted codeword. Even if the errors are caused by a malicious jammer, the list cannot contain too many codewords provided t' is not too much larger than t. Thus, in either case, the receiver is in a better position to recover the transmitted codeword under the model of list decoding.

List decoding was initiated mainly as a mathematical tool that allowed for a better understanding of some of the classical parameters of interest in information and coding theory. Elias [10] used this notion to get a better handle on the error-exponent in the strong forms of Shannon's coding theorem. The notion also plays a dominant role in the Elias-Bassalygo [34, 4] upper bound on the rate of a code as a function of its relative distance.

Through the decades the notion has continued to be investigated in a combinatorial context; and more recently has seen a spurt of algorithmic results. The paper being reflected on [23] was motivated by a gap between the combinatorial understanding of Reed-Solomon codes, and the known algorithmic performance. Below we summarize the combinatorial state of knowledge, describe the main result of [23], and also use the opportunity to survey some of the rich body of algorithmic results on list decoding that have emerged in the recent past. We also muse upon some useful asymptotic perspectives that eased the way for some of this progress, and reflect on some possibilities for future work.

1.1 Combinatorics of list decoding

We start by defining the notion of the list decoding radius of an (infinite family of) codes. This notion is adapted from a definition in [20], who term it the "polynomial list decoding radius".

Definition 1 *A family of codes $\mathcal{C}$ has a* list decoding radius $L:\mathbb{Z}^+ \to \mathbb{Z}^+$ *if there exists a polynomial $p(\cdot)$ such that for every code $C \in \mathcal{C}$ of block length n, and every received vector* $\mathbf{r}$, *it is that case that there are at most $p(n)$ codewords in C that have Hamming distance at most $L(n)$ from* $\mathbf{r}$. *We say that the code has a* relative list decoding radius $\ell(n)$ *if it has list decoding radius $L(n) = n \cdot \ell(n)$.*

The primary thrust of the combinatorial study is the relationship between $\ell(n)$ and the more classical parameters $\delta(n)$,the relative distance of a code, and $R(n)$, the rate of a code. (A family of codes has rate $R(n)$ (relative distance $\delta(n)$) if every member of C of block length n has information length at least $n \cdot R(n)$ (minimum distance at least $n\delta(n)$.)

For a "well-designed" code C of relative distance $\delta(n)$, one should expect the list decoding radius $\ell(n)$ to be at most $\delta(n)$. And from the fact that a code can correct half as many errors as its distance it follows that a family of codes C of relative distance $\delta(n)$ has relative list decoding radius $\ell(n) \geq \delta(n)/2$. The real question here is where in between $\delta/2$ and δ does the list decoding radius actually lie in general. The classical Johnson bound (or at least, its proof) shows that $\ell(n) \geq 1 - \sqrt{1-\delta(n)}$ which turns out to be better than $\delta/2$ for all choices of δ. This bound motivates one of the principal algorithmic challenges associated with list decoding: For a code of relative distance $\delta(n)$, give a polynomial time algorithm to find a list of all codewords within a relative distance of $\left(1-\sqrt{1-\delta(n)}\right)$ from a given received word $\mathbf{r}$. This is the question that motivated the work [23] and was answered positively therein. Before describing the algorithmic results, we wrap up the section with a summary of the combinatorial state of knowledge.

The inequality $\ell(n) \geq 1 - \sqrt{1-\delta(n)}$ appears to be the best possible lower bound one can establish on the relative list decoding radius of a code as a function of its distance.[1] It is easy to prove the existence of non-linear codes which match this bound. The question of whether the bound is the best one can prove for linear codes remains open, though significant progress has been made towards resolving it in [25, 20, 18].

From the point of usage, it is more useful to compare the rate of a code with its list decoding radius. This question has been investigated over the years by [6, 7, 45, 11, 20]. It follows from the converse to Shannon's coding theorem that a q-ary code of relative list decoding radius $\ell(n)$ has rate at most $R(n) \approx 1 - H_q(\ell(n))$. The above mentioned works show that there exist codes approaching this bound. The associated algorithmic challenge, of constructing such codes explicitly and finding decoding algorithms for them remains wide open.

2 List decoding algorithms

Despite the obvious utility of list decoding algorithms, few results were obtained till the eighties. The first efficient list decoding algorithms, due to Dumer [9] and Sidelnikov [36] corrected a number of errors that were of the form $\ell(n) = \left(\frac{1}{2} + o(1)\right)\delta(n)$ for some families of Reed-Solomon codes. This problem was introduced to the computer science literature by Goldreich and Levin [14] who gave a highly efficient randomized list decoding algorithm for Hadamard codes, when the received vector was given implicitly. This work led to some extensions by Goldreich, Rubinfeld, and Sudan [16]. Yet no efficient list decoding algorithms were found for codes of decent rate (constant, or even slowly vanishing rate such as $R(n) = n^{-1+\varepsilon}$ for some $\varepsilon > 0$).

The first list decoding algorithm correcting $\delta(n)$ errors for $\alpha > \frac{1}{2}$ for codes of constant rate was due to Sudan [38], who gave such an algorithm for Reed-Solomon codes. The algo-

[1] This applies to bounds that apply for all codes, regardless of their alphabet size. For small alphabets, e.g. for binary codes, a better bound can be proven. Since our primary focus is Reed-Solomon codes, we do not elaborate on the improved bound on list decoding radius that takes into account the alphabet size.

rithm was subsequently extended to algebraic-geometric codes by Shokrollahi and Wasserman [35]. Yet these results did not decode up to the best known combinatorial bounds on list decoding radius; in fact, they did not correct more than $(n)/2$ errors for any code of rate greater than 1/3. The obvious gap between the combinatorial bound $\left(\ell(n) \geq 1-\sqrt{1-\delta(n)}\right)$ and the algorithmic results motivated the work [23], where this gap was bridged for Reed-Solomon codes and algebraic-geometric codes. Specifically, the following theorem was proven for the class of Reed-Solomon codes.

Theorem 2 ([23]) *There exists an algorithm that, given a received vector* **r** *and a description of a q-ary Reed-Solomon code of dimension* $(k+1)$ *and block length n, finds a list of all codewords within a distance of* $n\left(1-\sqrt{k/n}\right)$ *from the received vector. The running time of the algorithm is bounded by a polynomial in n and q.*

Below we give a brief overview of the algorithm and in particular, describe some of the history behind this algorithm.

2.1 Decoding Reed-Solomon Codes

It might help to recall the definition of Reed-Solomon codes. Let $\mathbb{F}_q$ denote a field of size q and let $\mathbb{F}_d^k[x]$ denote the vector space of polynomials of degree at most k over $\mathbb{F}_q$. Recall that the Generalized Reed Solomon code of dimension $(k + 1)$, is specified by distinct $x_1, \ldots, x_n \in \mathbb{F}_q$ and consists of the evaluations of all polynomials p of degree at most k at the points $x_1, \ldots, x_n$. More formally, letting $\mathbf{x} = \langle x_1, \ldots, x_n \rangle$ and letting $p(\mathbf{x})$ denote $\langle p(x_1), \ldots, p(x_n) \rangle$, we get that the associated code $\mathrm{RS}_{q,k,x}$ is given by

$$\mathrm{RS}_{q,k,x} = \left\{ p(\mathbf{x}) \middle| p \in \mathbb{F}_q^k[x] \right\}.$$

Viewed from this perspective (as opposed to the dual perspective, where the codewords of the Reed Solomon codes are coefficients of polynomials), the Reed Solomon decoding problem is really a "curve-fitting" problem: Given n-dimensional vectors **x** and **y**, find all polynomials $p \in \mathbb{F}_q^k[x]$ such that $\Delta(p(\mathbf{x}),\mathbf{y}) \leq e$, for some error parameter e. (Here and later, $\Delta(\cdot,\cdot)$ denotes the Hamming distance.) We now give a brief summary of the algorithmic ideas that led to the algorithm in [23]. This chain of ideas includes the Welch-Berlekamp algorithm [42, 5], an algorithm for a restricted decoding problem due to Ar et al. [1], and the list decoding algorithm of Sudan [38].

Traditional algorithms, starting with those of Peterson [32] attempt to "explain" **y** as a function of **x**. This part becomes explicit in the work of Welch & Berlekamp [42, 5] (see, in particular, the expositions in [13] or [37, Appendix A]) where **y** is interpolated as a rational function of **x**, and this leads to the efficient decoding. (Specifically, a rational function $a(x)/b(x)$ can be computed such that for every $i \in \{1, \ldots, n\}$we have $a(x_i) = y_i * b(x_i)$.)

Rational functions, however, are limited in their ability to extract the message from data with large amounts of error. In particular they fail to work when the data has exactly two explanations — i.e., there are two polynomials p_1 and p_2 such that for exactly half the points $y_i = p_1(x_i)$ and for the other half $y_i = p_2(x_i)$. In such a case it is still possible to find an algebraic explanation of the points $\left\{(x_i . y_i)\right\}_{i=1}^n$: we simply have that the polynomial $Q(x, y) = \left(y - p_1(x)\right) \cdot \left(y - p_2(x)\right)$ is zero on every given (x_i,y_i). Furthermore the polynomial $Q(x,y)$ can be found by simple interpolation (which amounts to solving a linear system), and the candidate polynomials $p_1(x)$ and $p_2(x)$ are the roots of the polynomial $Q(x,y)$. (Notice that the factoring will find two polynomials p_1 and p_2 and, if $\omega^2 \neq 1$, the true candidate is p_1 if it satisfies $p_2 = \omega p_1$.) This was the problem considered by Ar et al. [1] and the solution above is the one given by them.

The next step in this chain of ideas, due to Sudan [38], is the realization that the algorithm above already solves the Reed-Solomon list decoding problem for a non-trivial choice of parameters (rate vs. list decoding radius). In particular, a simple counting argument shows that there exists a non-zero polynomial $Q(x,y)$ of degree $\sqrt{n}$ each in x and y that is zero on *any* set of n points. Now, if a subset of more than $(k+1)\sqrt{n}$ of these points satisfy $y_i = p(x_i)$, then $y - p(x)$ is a factor of $Q(x,y)$. Thus, finding such a bivariate polynomials Q and factoring it, gives a small list of polynomial that includes all the candidates for output of the list decoding algorithm. By picking the degree of Q very carefully, one can improve its performance significantly to at least $n - \sqrt{2kn}$ errors (see [39] for a more complete analysis of the performance of this algorithm).

The interesting aspect of the above algorithm is that it takes some very elementary algebraic concepts, such as unique factorization, Bezout's theorem, and interpolation, and makes algorithmic use of these concepts in developing a decoding algorithm for an algebraic code. This may also be a good point to mention some of the significant advances made in the complexity of factoring multivariate polynomials that were made in the 1980's. These algorithms, discovered independently by Grigoriev [17], Kaltofen [26], and Lenstra [28], form the technical foundations of the decoding algorithm above. Modulo these algorithms, the decoding algorithm and its proof rely only on elementary algebraic concepts. Exploiting slightly more sophisticated concepts from commutative algebra leads to even stronger decoding results that we describe next.

The algorithm of Guruswami and Sudan [23] is best motivated by the following weighted curve fitting question: Suppose in addition to vectors **x** and **y**, one is also given a vector of positive integers **w** where w_i determines the "weight" or confidence associated with a given point (x_i,y_i). Specifically we would like to find all polynomials p such that $\sum_{i|p(x_i)=y_i} w_i \geq W$ (for as small a W as possible). How can one interpret the weights in the algebraic setting? A natural way at this stage is to find a "fit" for all the data points that corresponds to the weights: Specifically, find a polynomial $Q(x,y)$

that "passes" through the point (x_i,y_i) at least w_i times. The notion of a curve passing through a point multiple times is a well-studied one. Such points are called singularities. Over fields of characteristic zero, these are algebraically characterized by the fact that the partial derivatives of the curve (all such, up to the $(r-1)$th derivatives, if the point must be visited by the curve r times), vanish at the point. The relevant component of this observation is that insisting that a curve pass through a point r times is placing $\binom{r+1}{2}$ linear constraints on the coefficients. This fact remains true over finite fields, though the partial derivatives don't yield these linear constraints any more. Formalizing this algorithm carefully and optimizing the degree of Q appropriately, gives the following lemma:

Lemma 3 ([23]) *Given vectors* $\mathbf{x},\mathbf{y} \in \mathbb{F}_q^n$*, and* $\mathbf{w} \in (\mathbb{Z}^+)^n$*, a list of all polynomials* $p \in \mathbb{F}_q^k[x]$ *satisfying* $\sum_{i|p(x_i)=y_i} w_i > \left\lfloor \sqrt{k\sum_{i=1}^n w_i(w_i+1)} \right\rfloor$ *can be found in time polynomial in* $n, \sum_i w_i$*, provided all pairs* (x_i,y_i) *are distinct.*

The surprising element in the above lemma is that the performance is not invariant to scaling of the w_i's — and the requirement on the amount of agreement decreases as one scales the weights up. This holds even if all the weights are equal, in which case the problem being solved is just the Reed-Solomon list decoding problem in a disguised form. In particular, by setting the weights appropriately large gives the algorithm claimed in Theorem 2. Thus we have a better unweighted decoding algorithm, that uses the weighted version as an intermediate step! Of course, it is also possible to state what the algorithm achieves for a general set of weights. For this part, we will just assume that the weight vector is an arbitrary vector of non-negative reals, and get the following:

Theorem 4 ([23, 24]) *Given vectors* $\mathbf{x},\mathbf{y} \in \mathbb{F}_q^n$*, a weight vector* $\mathbf{w} \in \boldsymbol{R}_{\geq 0}^n$*, and a real number* > 0*, a list of all polynomials* $p \in \mathbb{F}_q^n[x]$ *satisfying* $\sum_{i|p(x_i)=y_i} w_i > \sqrt{k\left(\varepsilon + \sum_{i=1}^n w_i^2\right)}$ *can be found in time polynomial in* n *and* $\frac{1}{\varepsilon}$*, provided the pairs* (x_i,y_i) *are all distinct.*

This result summarizes the state of knowledge for list decoding of Reed Solomon codes, subject to the restriction that the decoding algorithm runs in polynomial time. However, this criterion, that the decoding algorithm runs in polynomial time, is a very loose one. The practical nature of the problem deserves a closer look at the components involved and efficient strategies to implement these components. This problem has been considered in the literature, with significant success. In particular, it is now known how to implement the interpolation step in $O(n^2)$ time, when the output list size is a constant [31, 33]. Similar running times are also known for the root finding problem (which suffices for the second step in the algorithms above) [3, 12, 29, 31, 33, 44]. Together these algorithms lead to the possibility that a good implementation of list decoding may actually even be able to compete with the classical Berlekamp-Massey decoding algorithm in terms of efficiency. A practical implementation of such an algorithm in C++, due to Rasmus Refslund Nielsen, is available from his homepage (http://www.student.dtu.Dk/~p938546/index.html).

The paper [23] also presents a generalization of the weighted decoding algorithm to the case of algebraic-geometric codes. Using it as an intermediate step with a suitable choice of weights, one gets an algorithm that decodes algebraic-geometric codes beyond half the minimum distance for every value of rate. In fact, as noted in [27], a careful choice of weights enables decoding up to the combinatorial bound on list decoding radius.

2.2 Other algorithmic results

A rich body of algorithmic results concerning list decoding have appeared following the publication of [23]. We have already mentioned the works that addressed the question of more efficient implementations of the list decoding algorithms for Reed-Solomon and algebraic-geometric codes from [23]. Goldreich, Ron, and Sudan [15] considered the question of list decoding a number-theoretic code called *the Chinese Remainder code* (henceforth, CRT code). Here, the messages are identified with integers m in the range $0 \leq m < K$ and a message m is encoded as: $m \rightarrow \langle m(\bmod p_1), \cdots, m(\bmod p_n) \rangle$ where $p_1 < p_2 < \cdots < p_n$ are n relatively prime integers. When $K = p_1 \cdot p_2 \cdots p_k$, the Chinese Remainder Theorem implies that the code thus defined has distance $(n-k+1)$. The combinatorial bounds then indicate that such a code can be list decoded with small lists up to about $n - \sqrt{kn}$ errors. Goldreich et al. [15] initiated the study of list decoding CRT codes and this was continued in Boneh [8]. However, these algorithms corrected only about $n - \Omega\left(\sqrt{kn\frac{\log p_n}{\log p_1}}\right)$ errors and therefore their performance was poor when the p_i's had widely different magnitudes.

Subsequently, in [22], it was realized that algebraic and number-theoretic codes can be unified under the umbrella of ideal-based codes. Loosely speaking, the messages of an *ideal-based* code are all elements of small "size" in a "nice" commutative ring, and a message is encoded by the sequence of its residues modulo a set of pairwise coprime *ideals* of the ring. Moreover, [22] also showed that the idea behind the list decoding scheme from [23] can be generalized to work for ideal-based codes as well. In addition to giving a "unified" approach to list decoding Reed-Solomon, algebraic-geometric and CRT codes, this also resulted in an improved algorithm for CRT codes that could list decode from up to $n - \sqrt{k(n+\varepsilon)}$ errors (for arbitrary $\varepsilon > 0$) and thus essentially up to the combinatorial list decoding radius.

The result of Theorem 4 has seen elegant applications in list decoding algorithms for concatenated codes with the outer code being Reed-Solomon or algebraic-geometric and with certain choices of inner code. Nielsen [30] considers the case of inner codes with small distance. Elegant analytic results for the case when the inner code is Hadamard are obtained in [24]. In [20], the authors use "tailor-made" inner codes that work very well in conjunction with the weighted Reed-Solomon decoding algorithm. In the latter two works, the inner codes are first decoded to provide, for each position i of the outer Reed-Solomon code, a "weight" $w_{i,\alpha}$ for each field element α. The weight $w_{i,\alpha}$ is a measure of the confidence that the i'th symbol of the Reed-Solomon codeword is α. These weights are then used to list decode the outer Reed-Solomon code as per Theorem 4. Analyzing such a decoding procedure with a careful choice of weights gives algorithms to list decode certain concatenated codes up to or reasonably close to their list decoding radius. We refer the reader to [24, 20], or [19, Chapter 8] for further details.

Besides algebraic-geometric codes, Reed-Solomon codes can be generalized in another way, by allowing polynomials on more than one variable to encode the message. This gives the class of *Reed-Muller* codes. The technique used in [23] unfortunately does not seem to generalize in any simple way to decode Reed-Muller codes up to their list decoding radius, or for that matter even beyond half the distance for all rates, and this remains an interesting open question. However, in [2, 40], using clever reductions to the univariate case, an algorithm to list decode Reed-Muller codes well beyond half the distance is presented for codes of low rate.

A consequence of Theorem 2 is that, for arbitrary $\varepsilon > 0$, efficient list decoding up to a fraction $(1 - \varepsilon)$ of errors can be performed using codes of rate ε^2. The only drawback of Reed-Solomon codes is their large alphabet size (which is at least their block length). While this is alleviated by algebraic-geometric codes and the generalization of Theorem 2 to them, the construction and decoding complexity becomes rather high. Using Reed-Solomon codes together with suitable highly expanding graphs, Guruswami and Indyk [21] present a simple construction of a code over a *fixed* alphabet size that achieves rate $\Omega(\varepsilon^2)$ and can be efficiently list decoded from a fraction $(1 - \varepsilon)$ of errors. They also present a construction with rate $\Omega(\varepsilon)$ (and thus is "better" than Reed-Solomon codes), though the decoding complexity becomes sub-exponential (2^{n^γ} for arbitrary $\gamma > 0$) in the block length [21]. This latter result raises the hope that even better codes and algorithms can be obtained by devising non-algebraic approaches to list decoding.

3 Future directions

It is well-known that the *capacity* of the binary symmetric channel with cross-over probability p equals $(1 - H(p))$. In other words, over the channel which flips each bit independently with probability p, one can achieve arbitrarily reliable communication at any rate less than $1 - H(p)$. Now consider the noise model where the channel *adversarially* corrupts up to a fraction p of positions. In such a case, "traditional" unique decoding is limited by the half the distance barrier, and thus one has to use codes of relative distance $2p$. In turn, this means one cannot achieve the capacity $1 - H(p)$. List decoding exhibits that this limitation is not entirely inherent to the adversarial error model, and can be overcome if one is allowed to output a small list of codewords as answers. In fact, a result due to [20] shows that one can get within ε of the capacity, even under the adversarial model, provided one is permitted list decoding with lists of size $1/\varepsilon$. This raises the intriguing possibility of a "worst-case" theory of information hinging upon list decoding as the basic notion of error-recovery.

The above-mentioned codes from [20] that achieve "capacity" under a worst-case setting are, however, highly non-explicit. An explicit construction of such codes together with efficient list decoding algorithms poses an enormous challenge for future work on list decoding, and constitutes in the authors' mind the single biggest open question in the area. There has been steady progress in this pursuit for the low-rate regime using clever concatenation schemes combined with the weighted Reed-Solomon list decoding algorithm (see, for example, [20]). Nevertheless, we are still very far from any construction of "capacity-approaching" codes that nearly achieve the optimal rate vs. list decoding radius trade-off. Algebraic codes possibly augmented with more sophisticated concatenation-like ideas still hold some promise. But, in light of the recent coding-theoretic developments using combinatorial objects such as "extractors" and "expanders" [41, 21], it is quite possible that non-algebraic approaches will be important in this pursuit.

References

[1] Sigal Ar, Richard Lipton, Ronitt Rubinfeld, and Madhu Sudan. Reconstructing algebraic functions from mixed data. *SIAM Journal on Computing*, 28(2):488-511, 1999.

[2] Sanjeev Arora and Madhu Sudan. Improved low-degree testing and its applications. *In Proceedings of the Twenty-Ninth Annual ACM Symposium on Theory of Computing*, pages 485-495, El Paso, Texas, 4-6 May 1997.

[3] Daniel Augot and Lancelot Pecquet. A Hensel lifting to replace factorization in list decoding of algebraic-geometric and Reed-Solomon codes. *IEEE Transactions on Information Theory*, 46:2605-2613, November 2000.

[4] L.A. Bassalygo. New upper boundes for error-correcting codes. *Problems of Information Transmission*, 1(1):32-35, 1965.

[5] Elwyn Berlekamp. Bounded distance +1 soft-decision Reed-Solomon decoding. *IEEE Transactions on Information Theory*, 42(3):704-720, 1996.

[6] Volodia M. Blinovsky. Bounds for codes in the case of list decoding of finite volume. *Problems of Information Transmission*, 22(1):7-19, 1986.

[7] Volodia M. Blinovsky. *Asymptotic Combinatorial Coding Theory*. Kluwer Academic Publishers, Boston, 1997.

[8] Dan Boneh. Finding smooth integers in short intervals using CRT decoding. *Proceedings of the 32nd Annual ACM Symposium on Theory of Computing*, pages 265-272, 2000.

[9] Ilya I. Dumer. Two algorithms for the decoding of linear codes. *Problems of Information Transmission*, 25(1):24-32, 1989.

[10] Peter Elias. List decoding for noisy channels. *Technical Report 335, Research Laboratory of Electronics, MIT*, 1957.

[11] Peter Elias. Error-correcting codes for list decoding. *IEEE Transactions on Information Theory*, 37:5-12, 1991.

[12] Shuhong Gao and M. Amin Shokrollahi. Computing roots of polynomials over function fields of curves. *Coding Theory and Cryptography: From Enigma and Geheimschreiber to Quantum Theory (D. Joyner, Ed.), Springer*, pages 214-228, 2000.

[13] Peter Gemmell and Madhu Sudan. Highly resilient correctors for multivariate polynomials. *Information Processing Letters*, 43(4):169-174, September 1992.

[14] Oded Goldreich and Leonid A. Levin. A hard-core predicate for all one-way functions. *In Proceedings of the Twenty First Annual ACM Symposium on Theory of Computing*, pages 25-32, Seattle, Washington, 15-17 May 1989.

[15] Oded Goldreich, Dana Ron, and Madhu Sudan. Chinese remaindering with errors. *IEEE Transactions on Information Theory*, 46(5):1330-1338, July 2000. Extended version appears as ECCC Technical Report TR98-062 (Revision 4), http://www.eccc.uni-trier.de/eccc.

[16] Oded Goldreich, Ronitt Rubinfeld, and Madhu Sudan. Learning polynomials with queries: The highly noisy case. *SIAM Journal on Discrete Mathematics*, 13(4):535-570, November 2000.

[17] Dima Grigoriev. Factorization of polynomials over a finite field and the solution of systems of algebraic equations. *Translated from Zapiski Nauchnykh Seminarov Lenningradskogo Otdeleniya Matematicheskogo Instituta im. V. A. Steklova AN SSSR*, 137:20-79, 1984.

[18] Venkatesan Guruswami. Limits to list decodability of linear codes. *Manuscript*, 2001.

[19] Venkatesan Guruswami. *List Decoding of Error-Correcting Codes*. PhD thesis, Massachusetts Institute of Technology, August 2001.

[20] Venkatesan Guruswami, Johan Håstad, Madhu Sudan, and David Zuckerman. Combinatorial bounds for list decoding. *Proceedings of the 38th Annual Allerton Conference on Communication, Control and Computing*, pages 603-612, October 2000.

[21] Venkatesan Guruswami and Piotr Indyk. Expander-based constructions of efficiently decodable codes. *Proceedings of the 42nd Annual Symposium on Foundations of Computer Science*, October 2001.

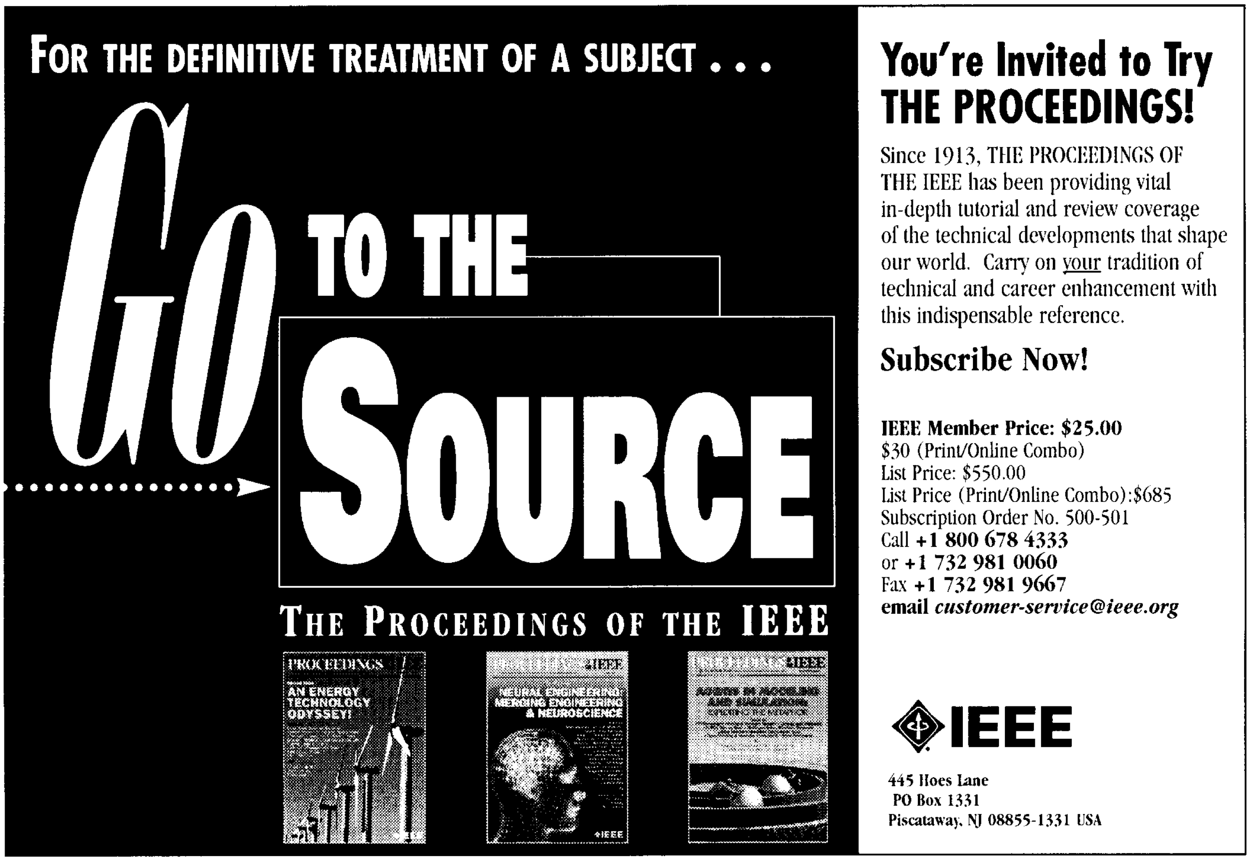
[22] Venkatesan Guruswami, Amit Sahai, and Madhu Sudan. Soft-decision decoding of Chinese Remainder codes. *In Proceedings of the 41st IEEE Symposium on Foundations of Computer Science*, pages 159-168, Redondo Beach, California, 12-14 November 2000.

[23] Venkatesan Guruswami and Madhu Sudan. Improved decoding of Reed-Solomon and algebraic-geometric codes. *IEEE Transactions on Information Theory*, 45:1757-1767, 1999.

[24] Venkatesan Guruswami and Madhu Sudan.List decoding algorithms for certain concatenated codes. *Proceedings of the 32nd Annual ACM Symposium on Theory of Computing*, pages 181-190, 2000.

[25] Jørn Justesen and Tom Høholdt. Bounds on list decoding of MDS codes. *IEEE Transactions on Information Theory*, 47(4):1604-1609, May 2001.

[26] Erich Kaltofen. Polynomial-time reductions from multivariate to bi- and univariate integral polynomial factorization. *SIAM Journal on Computing*, 14(2):469-489, 1985.


PROCEEDINGS
AN ENERGY TECHNOLOGY ODYSSEY!
NEURAL ENGINEERING MERGING ENGINEERING & NEUROSCIENCE
IEEE

[27] Ralf Koetter and Alexander Vardy. Algebraic soft-decision decoding of Reed-Solomon codes. *Proceedings of the 38th Annual Allerton Conference on Communication, Control and Computing*, October 2000.

[28] Hendrik W. Lenstra. Codes from algebraic number fields. In L.G.L.T. Meertens M. Hazewinkel, J.K. Lenstra, editor, *Mathematics and computer science II, Fundamental contributions in the Netherlands since 1945*, pages 95-104. North-Holland, Amsterdam, 1986.

[29] R. Matsumoto. On the second step in the Guruswami-Sudan list decoding algorithm for AG-codes. *Technical Report of the Institute of Electronics, Information and Communication Engineers (IEICE)*, pages 65-70, 1999.

[30] Rasmus R. Nielsen. Decoding concatenated codes using Sudan's algorithm. *Manuscript submitted for publication*, May 2000.

[31] Rasmus R. Nielsen and Tom Høholdt. Decoding Hermitian codes with Sudan's algorithm. *Proceedings of AAECC-13, LNCS 1719*, pages 260-270, 1999.

[32] W. Wesley Peterson. Encoding and error-correction procedures for Bose-Chaudhuri codes. *IEEE Transactions on Information Theory*, 6:459-470, 1960.

[33] Ronny Roth and Gitit Ruckenstein. EDcient decoding of Reed-Solomon codes beyond half the minimum distance. *IEEE Transactions on Information Theory*, 46(1):246-257, January 2000.

[34] Claude E. Shannon, Robert G. Gallager, and Elwyn R. Berlekamp. Lower bounds to error probability forcoding on discrete memoryless channels. *Information and Control*, 10:65-103 (Part I), 522-552 (Part II), 1967.

[35] M. Amin Shokrollahi and Hal Wasserman. List decoding of algebraic-geometric codes. *IEEE Transactions on Information Theory*, 45(2):432-437, 1999.

[36] V. M. Sidelnikov. Decoding Reed-Solomon codes beyond $(d-1)/2$ errors and zeros of multivariate polynomials. *Problems of Information Transmission*, 30(1):44-59, 1994.

[37] Madhu Sudan. *Efficient Checking of Polynomials and Proofs and the Hardness of Approximation Problems*. PhD thesis, University ofCalifornia at Berkeley, October 1992. Also appears as *Lecture Notes in Computer Science*, vol. 1001, Springer, 1996.

[38] Madhu Sudan.Decoding of Reed-Solomon codes beyond the error-correction bound. *Journal of Complexity*, 13(1):180-193, 1997.

[39] Madhu Sudan. Decoding of Reed-Solomon codes beyond the error-correction diameter. *Proceedings of the 35th Annual Allerton Conference on Communication, Control and Computing*, 1997.

[40] Madhu Sudan, Luca Trevisan, and Salil Vadhan. Pseudorandom generators without the XOR lemma. *Proceedings of the 31st Annual ACM Symposium on Theory of Computing*, pages 537-546, 1999.

[41] Amnon Ta-Shma and David Zuckerman. Extractor Codes. *Proceedings of the 33rd Annual ACM Symposium on Theory of Computing*, pages 193-199, July 2001.

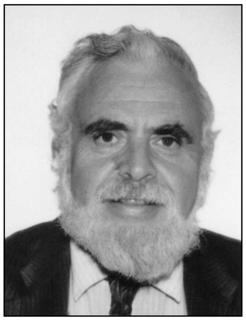
[42] Lloyd R. Welch and Elwyn R. Berlekamp. Error correction of algebraic block codes. *US Patent Number 4,633,470*, December 1986.

[43] John M. Wozencraft. List Decoding. *Quarterly Progress Report, Research Laboratory of Electronics, MIT*, 48:90-95, 1958.

[44] Xin-Wen Wu and Paul H. Siegel. Effcient list decoding of algebraic geometric codes beyond the error correction bound. *Proceedings of the International Symposium on Information Theory*, June 2000.

[45] Victor V. Zyablov and Mark S. Pinsker. List cascade decoding. *Problems of Information Transmission*, 17(4):29-34, 1981 (in Russian); pp. 236-240 (in English), 1982.

GOLOMB'S PUZZLE COLUMN™



–Solomon W. Golomb

Some Combinatorial Questions

1. There are 15 balls on a billiard table, bearing the numbers from 1 to 15. Any one of these can be selected to be the first ball to go off the table; but thereafter, each subsequent ball must have a number consecutive (up or down by 1) with that of a ball already off the table. [Thus, if the first ball to go had the number 4,the next must be either number 3 or number 5. If the first ball to go had the number 15, the next to go would have to be number 14.] How many possible sequences are there for the order in which all 15 balls go off the table?

2. If n points are placed independently and at random on the unit circle, what is the probability that they will all lie on a semicircle (i.e. within an arc of length π, starting anywhere on the unit circle)? Generalize to the case of all lying on an arc of length $\alpha, 0 \le \alpha \le \pi$. What happens if $\pi < \alpha < 2\pi$?

3. Every permutation on n symbols $\{a_1, a_2, \ldots, a_n\}$ can be written as a product of disjoint cycles whose cycle lengths sum to n. Let L_n be the expected length of the longest cycle in a random permutation on n symbols, and let $\lim_{n \to \infty} \frac{Ln}{n} = \lambda$. Let $P_n^{(1)}$ be the probability that the first symbol, a_1, is on the longest cycle of a random permutation on n symbols.

a. Prove that the limit λ exists.

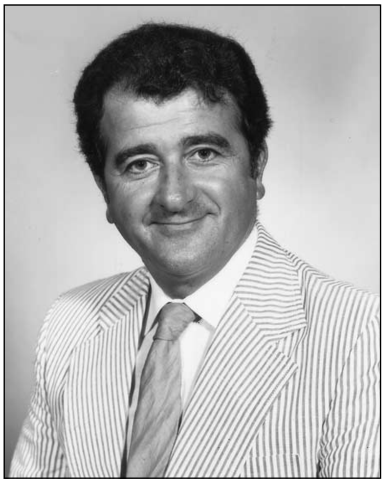
b. Express $\lim_{n \to \infty} P_n^{(1)}$ in terms of λ.

(To obtain probabilities and expected values for a "random "permutation on n symbols, simply take the average over all $n!$ permutations.)

4. If n black beads and $n + 1$ white beads are placed on a string, and the ends of the string are joined to form a necklace, how many cyclically distinct necklaces can result?

Historian's Column

A. Ephremides



A. Ephremides

Inspired by Alexander Dumas's "sampling" period of twenty years, I thought I would take you back twenty years today, for a "sample" of what our Society was like then. So, in 1982, a deliciously different mindset seemed to have been prevailing along with the innocent ignorance of magnificent things yet to come. Join me in surveying some of the highlights. Just to help you imbed your thinking in the proper "zeitgeist", let me remind you that 1982 was the year in which Ronald Reagan was in the second year of his first term Presidency, the Berlin Wall stood tall, Bin Laden was shaking off the problems of puberty, Pavarotti was just becoming a household name (along with CuisinArt), China had just gotten rid of the "Gang-of-Four", and Starbuck's was still largely confined to Seattle. Manual switching of TV channels was still the norm, cell telephones were rare and found only in ornate consoles by the driver seat, Al Leon-Garcia was the *IT Newsletter* Editor, Bob Gray the *Transactions* Editor, and Bob Gallager, Shu Lin, Jim Massey, Jim Modestino, Neil Sloane, and Kung Yao were the newly elected (or re-elected) members of the Board of Governors.

In 1982 the International Symposium on Information Theory was held in late June in Les Arcs, a mountain resort in the French Alps. It was the first time in the Symposium's history that the entire Program Committee included no one affiliated with an institution in North America. It marked the "existence" proof of the Society's globalization. Remarkably, the Technical Program Committee, under the chairmanship of J-M Goethals, consisted of only eleven members (Ahlswede, Bremawd, Camion, Devijver, Flajolet, Longo, Macchi, Massey, Metivier, van der Meulen, and Schalkwijk). There were only 396 attendees and 310 papers organized in 41 sessions (a record maximum at the time in the ISIT's history). Irv Reed was the Shannon Lecturer and Tom Kailath, Pino Longo, Neil Sloane, and Bernard Marti were the Plenary Lecturers talking about VLSI-Signal Processing, Combinatorial Source Coding, Quantization, and Computer Networks respectively. There were some imaginative invited sessions on Questionnaire Theory and on Links between Coding Theory and Languages. Copious amounts of second-rate red wine were accompanying all meals ("sauf" breakfast), the weather was gorgeous, and two of the papers in the Recent Results session were delivered in … French ("construction d'entropies" and "Realisations Stochastiques de Signaux Nonstutionnaires et Identification sur un seul echantrillon").

A glance at the November issue of the *Transactions* revealed a very different location for the center of gravity of the Society's technical focus than what it is today. There were articles on "Adaptive Digital Matched Filters", "Efficient Run-Length Encodings", "Rate Distortion for Correlated Sources with Partially Separate Encoders", and a correspondence item by Sergio Verdu, that, in paraphrasing one of Gioachino Rossini's compositions, one could name "Les Pechers de ma .. Jeunesse", was titled "Comments on 'Anomalous Behavior of Receiver Output SNR as a Prediction of Signal Detection Performance Exemplified for Quadratic Receivers and Incoherent Fading Channels' ". The author of the article with this convoluted title on which Sergio was commenting was W.A. Gardner and he had published it in 1979. In those comments, Sergio pointed out that there were some incorrect results in the paper but their "essence" could be salvaged with the right approach. Even then, he knew!

The Society numbered about 4,500 members at the time, with about 180 members in Canada, 450 in Region 10 (Asia, Oceania), 110 in Region 9 (South America), 750 in Region 8 (Europe, Africa, Middle-East, Russia), and the rest in the United States. Vijay Bhargava would be happy to know that in 1982 the newsletter published the entire directory of our members organized not only by Region but by Section as well! By contrast, today, the Society has about 6,000 members with more than 50% being from outside the United States! What is noteworthy is that approximately 5% of the total membership had achieved in 1982 the grade of IEEE **Fellow**. This has been and continues to be the highest percentage of Fellows in any Society of IEEE.

An amusing item in the Newsletter at the time was the so-called "Competitions", in which preposterous word-plays and wisecracks were solicited from the readers with humorous to, sometimes, hilarious results. For example, competition no. 9 had solicited advertisements (real or imaginary) for products that would blend terms of our trade with consumer items in a "witty" way. Examples were: "Melittron: the first X-25-compatible coffeemaker", "Alias, Ltd: flexible vocoder capable of encoding speech at any bit rate by using newly developed sampling technologies", or "The Transcendental Modem: device that achieves bit rates above Shannon Capacity using BIG DIPPER, a newly patented signal constellation". In connection with this competition, Nelson Blachman had sent a letter to the Editor pointing out that in the United States, all TV sets were not able to tune to Channel 1! It was pointed out that strange though this may be, the public acceptance of it is even stranger (Perhaps a bit like the public acceptance of daylight saving time starting and ending at times that are highly asymmetrical around the time of the equinox or the solstice). Hence, the following advertisement was proposed:

"CHANNEL ONE: Receive the channel the Federal Secrecy Commission has refused to let TV set manufacturers permit you to see. With our translator attached to your set's VHF antenna terminals you can enjoy all of the top-secret programming appearing on channel 1. Send 20 cents for kit and complete details".

And related to another competition (no. 11) here are some other quips: "Tarzan escapes from the Tree-Coders by swinging through the trees using the shortest path algorithm" or "The Bound of Baskervilles is the research topic studied by Dr. Watson and his Research Assistant Mr. S. Holmes", both offered by Pas ("we miss you") Pasupathy!

That was also the year in which our Society was informed that the Japanese Information Theorists had been holding their own annual meeting called "JOHORIRON-TO-SONO-OYO", that translates to our (by now) familiar "Symposium on Information Theory and its Applications", which due to the outreach efforts of people like Shu Lin has added the word "International" to its name and has evolved into the well-known ISITA of today. That meeting was inaugurated in 1978 and by 1981, when it was held in Kasikojima, it featured over 150 papers.

Another interesting footnote concerning 1982 is the founding of the Society on Social Implications on Technology (SSIT) as a regular society of the IEEE. This society, still in quiet existence today set out some lofty goals for representing the "ethical" conscience of the collective IEEE membership and for keeping a watchful eye on the consequences in our daily lives of the technology and the products we develop. Unfortunately, it never really took off the ground. It has only about 2000 members worldwide and has been the frequent target of elimination by various strong-minded members of the Institute's governing bodies. Especially colorful was an attempt by a member of the Board of Directors of the IEEE to have the SSIT "reviewed" in 1989, (at the time, "review" served as a moniker for elimination), because it published an article on the use of technology in creating various instruments of sexual gratification!

Overall 1982 was a year of transition. It marked the beginnings of many practices that flourished subsequently within our Society both in the realm of our technical activities as well as in our administrative life. And it marked also the gradual withering of some of the traits that characterized its youth. In other words, it was a mark of the Society's maturation.

In the future we will sample the life of our Society a little more frequently than the Dumas rate; perhaps we can attain the Nyquist rate. These visits will form a sub-series in the history of this column that might be called "Those were the days…". And, until then, time keeps marching on!

Newsletter to be Added to the IT Digital Library

Lance C. Pérez
Newsletter Editor

The Information Theory Society Board of Governors has approved funds to add the newsletter to the Information Theory Society digital library (http://galaxy.ucsd.edu/). The newsletter digital library will be of the same form currently used by the Information Theory Transactions, that is, pdf files with a limited database. The main articles will have separate entries in the database, while conference reports and other items will be grouped by type and date. Parity Computing, which handles the IT Transactions, is handling the digitization and database creation which should be completed this spring.

The impetus for this project comes from the donation of a nearly complete collection of newsletters from the first issue in 1954 to 1989 from Lawrence L. Rauch to Robert McEliece. Bob and others then added the issues from 1990 to the present. A complete inventory of the collection is shown below with missing issues and anomalies shown in blue.

Year	**Issues**	**Year**	**Issues**
1954	Mar.	1978	#74 Mar., #75 Jun., Sep.
1955	#1 Mar., #2 Jun., #3 Nov.	1979	Mar., Jun., Sep.
1956	#4 Feb., #5 Jun., #6 Oct.	1980	Mar., Jun., Sep., Dec.
1957	#7 Feb., #8 Jun.	1981	Mar., Jun., Sep., Dec.
1958		1982	Mar., Jun., Sep., Dec.
1959		1983	Mar., Jun., Sep., Dec.
1960		1984	Mar., Jun., Sep., Dec.
1961	#14 Jul., #22 Nov.	1985	Mar., Sep., Dec.
1962	#23 Jan.., #24 Mar., #25 Jun, #26 Dec.	1986	Spring, Summer
1963	#27 Apr.	1987	Mar., Jun., Sep., Dec.
1964	#29 Jan., #30 Apr., #31 Aug.	1988	Mar., Jun., Sep., Dec.
1965	#32 Jan., #33 Apr., #34 Aug.	1989	Mar., Jun., Sep., Dec.
1966	#35 Jan., #36 Apr., Aug?	1990	Mar., Jun., Sep., Dec.
1967	#38 May, #39 Sep.	1991	vol. 41, #1 Mar., #2 Jun., #3 Sep., #4 Dec.
1968	Feb., #41 Aug., #42 Oct.	1992	vol. 42, #1 Mar., #2 Jun., #3 Sep., #4 Dec.
1969	#43 May, #44 Jul., #45 Jan.	1993	vol. 43, #1 Mar., #2 Jun., #3 Sep., #4 Dec.
1970	#46 Feb., #47 May, #48 Aug., #49 Oct.	1994	vol. 44, #1 Mar., #2 Jun., #3 Sep., #4 Dec.
1971	#50 Feb., #51 May, #52 Sep., #53 Dec.	1995	vol. 45, #1 Mar., #2 Jun., #3 Sep., #4 Dec.
1972	#54 Apr., #55 Jun., #56 Dec.	1996	vol. 46, #1 Mar., #2 Jun., #3 Sep., #4 Dec.
1973	#57 Mar., #58 Jun., #59 Oct.	1997	vol. 47, #1 Mar., #2 Jun., #3 Sep., #4 Dec.
1974	#60 Feb., #61 Jun., #62 Aug.	1998	vol. 48, #1 Mar., #2 Jun., Summer, #3 Sep., #4 Dec.
1975	#63 Apr., #64 May, #65 Sep.	1999	vol. 49, #1 Mar., #2 Jun., #3 Sep., #4 Dec.
1976	#66 Mar., #67 Jun., #68 Sep., Dec.	2000	vol. 50, #1 Mar., #2 Jun., #3 Sep., #4 Dec.
1977	#70 Mar., #71 Jun., #72 Sep., #73 Dec.	2001	vol. 51, #1 Mar., #2 Jun., #3 Sep., #4 Dec.

1. We are missing issues #9 through #13 published in 1958, 1959, 1960 and possibly 1961.
2. In 1961, the issues numbers jump from #14 to #22. Are there missing issues or is there another explanation for this numbering?
3. The August 1996 (this issue is not actually dated), February 1968, and December 1976 issues are not numbered. However, it does not appear that any issues are missing. Is this correct?
4. Issue #45 is dated January 1969, however it contains AdCom minutes from June and August of 1969. Is this really the January 1970 issue?
5. Pages 3 through 6 are missing from our copy of the #46 February, 1970 issue.
6. Quarterly publication of the newsletter apparently began in 1976, but 1978, 1979, 1985 and 1986 do not have four issues. Are any issues missing?

I would appreciate the Society's help in completing the collection and clarifying these anomalies.

My contact information can be found on the inside front cover of the newsletter. In order to avoid multiple copies, please send me an email before mailing any missing issues.

Professor Robert Scholtz Receives 2001 MILCOM Award for Lifetime Achievement in Wireless Research

Dr. Robert Scholtz, a former Board of Governors member of IEEE's Information Theory Society and long-time Professor of Electrical Engineering-Systems at the University of Southern California, has received the 2001 Military Communications (MILCOM) Conference Award for Technical Excellence for sustained contributions over his lifetime to military wireless research into spread spectrum communications, including ultrawideband (UWB) radio.

He was honored for his achievements in the field by the Military Communications Conference Board at the annual MILCOM Conference in October in McLean, Va.

Dr. Scholtz was only the fourth investigator to receive the award in the 20-year history of the conference, which is sponsored by IEEE and the Armed Forces Communications and Electronics Association (AFCEA). The award committee was composed of the three previous award winners.

He is an IEEE Fellow and has held other leadership positions in the organization over the years, including Finance Chairman for the 1977 National Telecommunications Conference, Program Chairman for the 1981 International Symposium on Information Theory, and member of the Board of Governors of the Communications Society from 1981 to 1983. He was a member of the Board of Governors of the Information Theory Society from 1981 to 1986.

"I am truly honored that the Board has seen fit to recognize my research in this way," Dr. Scholtz said.

USC Professor Robert Scholtz, who has received the 2001 Military Communications (MILCOM) Conference Award for Technical Excellence for contributions to military wireless research, shows an ultrawideband radio antenna set up in USC's Paul G. Allen Wireless Test Facility.

He pointed out that spread spectrum communications research is used in such areas as wireless voice communications, high-speed data communications and advanced radar systems. In spread spectrum communications, he said, more radio frequency bandwidth is used than is necessary to communicate the data, providing a means for a radio to reject external interference, including jamming. He stressed that the military is especially interested in spread spectrum communications for its anti-jamming capabilities. He said that ultrawideband radio technology is the specialty within spread spectrum communications that uses pulses of radio energy rather than radio waves to transmit information wirelessly in a digital form.

The Chairman of the award committee, Professor Laurence Milstein at the University of California, San Diego, said of Dr. Scholtz: "He has been one of the foremost contributors in moving the military communications field ahead, and he has been one of the most visible investigators nationally in the new field of ultrawideband radio."

Dr. Scholtz, who has been a professor at USC for 38 years, began investigating spread spectrum communications some

30 years ago and in the early 1990s started research into the UWB specialty. With three others, he wrote the key three-volume book, “Spread Spectrum Communications.”

He was Chairman of the USC School of Engineering’s Electrical Engineering-Systems Department for six years and Director of the School’s Communication Sciences Institute for five years.

He spearheaded research in ultrawideband radio at the School’s Integrated Media Systems Center (IMSC), the National Science Foundation’s Engineering Research Center for multimedia and Internet research. He organized an IMSC workshop in 1998 that focused private industry concerns on restrictive regulation of UWB radio research and commercialization by the Federal Communications Commission (FCC), and in 1999 the FCC changed its rules to ease restrictions on experimenting with the new UWB technology. In addition, he recently led a three-university team in winning a three-year, $3.6 million U.S. Army grant for additional UWB research.

IT Society Members Selected as 2002 IEEE Fellows

Dr. Richard G. Baraniuk COMM, IT, SP SP
Rice University
Dept. Of Electrical & Computer Engineering
MS 380, 6100 Main Street
Houston, TX 77251
Richb@rice.edu

For contributions to the development of techniques for time-frequency and multiscale analysis.

Dr. Sankar Basu C, CAS, CS, IT, SP CAS
17 North Summit Street
Tenafly, NJ 07670
basuhome@hotmail.com

For contributions to theory and application of multidimensional circuits, systems, and signal processing.

Dr. William Dale Blair AES, Ed, IT AES
Georgia Tech Research Institute
SEAL, 7220 Richardson Road
Smyrna, GA 30080
dale.blair@gtri.gatech.edu

For technical leadership in and contribution to developing multitarget-multisensor tracking technology and applications.

Dr. Bor-Sen Chen COMM, CS, IT NN
National Tsing Hua University
Dept. Of Electrical Engineering
Hsinchu, 30013 Taiwan
bschen@moti.ee.nthu.edu.tw

For contribution to fuzzy control theory and its applications.

Dr. Oliver Collins COMM, IT IT
The University of Notre Dame
Fitzpatrick Hall
Notre Dame, IN 46617
Oliver.M.Collins.62@nd.edu

For contributions to the theory on practice of error-correcting codes.

Dr. Evangelos S. Eleftheriou COMM, IT COMM
IBM Zurich Research Laboratory
IBM Research Division
Zurich Research Laboratory
Ruschlikon, CH-8803 Switzerland
ele@zurich.ibm.com

For contributions to equalization and coding, and for noise-predictive maximum likelihood detection in magnetic recording.

Dr. Patrick Guy Farrell CAS, COMM, IT, SP, VT IT
University of Lancaster, UK
Dept. Of Communication Systems
Lancaster, LA1 4YR
P.G.Farrell@lancaster.ac.uk

For contributions to error-correcting codes.

Dr. Patrick P. Flandrin IT, SP SP
CNRS
Laboratoire de Physique, Ecole Normale Superieure (ENS) de Lyon
46 allee d’Italic
Lyon Cedex 07, 69364 France
flandrin@ens-lyon.fr

For contributions to time-frequency and time-scale analysis of signals and systems.

Dr. Shuji Hirakawa BT, COMM, IT BT
27-7, 3-Chome Azamino Aoba-Ku
Yokohama, 225-0011 Japan
shuji.hirakawa@toshiba.co.jp

For contributions to the innovation of coded-modulation and set-partitioning, and applications of error-correcting codes to a real digital broadcasting system.

Mr. James David Johnston IT, SP Sp
AT&T Labs - Research Building 103, Room E165
180 Park Avenue
Florham Park, NJ 07932
jj@research.att.com

For contributions in perceptual audio coding and its standardization.

Dr. Douglas L. Jones COMM, IT, SP SP
University of Illinois
Department of Electrical and Computer Engineering
U. Of I, 1406 W. Gren Street

Urbana, IL 61801
jones@ifp.uiuc.edu

For contributions to adaptive and statistical time-frequency analysis.

Dr. Jelena Kovacevic IT, SP SP
Bell Labs/Lucent Technologies
Room 2C-176, 600 Mountain Avenue
Murray Hill, NJ 07974
jelena@bell-labs.com

For contributions to the theory of signal representation.

Dr. P. Vijay Kumar COMM, IT IT
University of Southern California
EEB 500, EE-Systems
3740 McClintock Avenue
Los Angeles, CA 90089-2565
vijayk@usc.edu

For contributions to the theory of error-correcting codes and low correlation sequence design.

Dr. Rajiv Laroia IT IT
445 Somerville Road
Basking Ridge, NJ 07920
laroia@flarion com

For contributions to reliable data transmission through dispersive channels.

Dr. Murray Howard Loew C, EMB, IT, SP EMB
George Washington University
Dept. Of Electrical & Computer Engineering
801 22nd Street N.W.
Washington, DC 20052
loew@seas.gwu.edu

For contributions to medical image analysis, pattern recognition, and digital image.

Dr. Michael W. Marcellin CAS, COMM, IT, SP IT
University of Arizona
Dept. Of Electrical & Computer Engineering
Tucson, AZ 85721-0104
marcellin@ece.arizona.edu

For contributions to data compression and constrained coding systems.

Dr. Sean P. Meyn CS, IT CS
University of Illinois at Urbana-Champaign
1308 West Main Street
Urbana, IL 61801-2307
s-meyn@uiuc.edu

For contributions to stochastic control, dynamic optimization, and control of large networks.

Dr. Shojiro Sakata IT IT
University of Electro-Communications
1-5-1 Chofugaoka
Tokyo, 182-8585 Japan
sakata@ice.uec.ac.jp

For contributions to the theory of multidimensional arrays and codes.

Dr. Igor Vajda IT, SP IT
Inst. Of Inform. Theory and Automation, Czech Acad. Science
Pod Vodarenskou verzi 4
POB 18
Prague 8, 18203 Czech Republic
vajda@utia.cas.cz

For contributions to the use of statistics in information theory.

Dr. Wing Shing Wong COMM, CS, IT CS VT
Chinese University of Hong Kong
Department of Information Engineering
Shatin
Hong Kong, China
wswong@ie.cuhk.edu.hk

For contributions to estimation theory of nonlinear systems and application of system theory to communication and information processing problems.

Dr. Bin Yu IT, SP IT
University of California at Berkeley
367 Evans Hall #3860
Berkeley, CA 94720
binyu@stat.berkeley.edu

For contributions to statistical methods in information theory.

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 very successful in winning. Your help is needed to identify candidates and, equally importantly, help us to find people who know the candidates and their work, so that nomination forms can be completed in a substantial way.

All of the awards have a NOMINATION DEADLINE of JULY 1, 2002. We strongly encourage suggestions and or nominations, which can be directed to Han Vinck at vinck@exp-math.uni-essen.de. More information can be found on the Web at http://www.ieee.org/awards/.

IT Society Members Elected to Senior Member of the IEEE in 2001

Alexander Barg
Kristine L. Bell
Martin J Bishop
Robert J. Bonneau
Brian K. Butler
Bruno Cernuschi-Frias
Ramesh C. Chauhan
Yue Chen
Mohamed F. Chouikha
Gustavo De Veci
Xinzhou Dong
George Hacken
Slim Hammadi
Masachika Harada
Abm Siddique Hossain
Masaaki Ikehara
James Irvine
Hamid Jafarkhani
Rodney A. Kennedy
Cheol-Sung Kim
Jongwon Kim
P. Vijay Kumar
Rajiv Laroia
Francois Le Chevalier
Man Hyung Lee
Vladimir Levenshtein
Alan R. Lindsey
Petri Mahonen
Takehiro Moriya
Sukumar Nandi
S. S. Narayanan
Hiroshi Nogami
Tomoaki Otsuki
Vladimir Parizhsky
Ankil Patel
Lance C. Pérez
Athina P. Petropulu
Gregory J. Pottie
Ramesh M. Pyndiah
R.M.A.P. Rajatheva
Lars K. Rasmussen
Syed A. Rizvi
Antonio Artes Rodriguez
Kenneth Rose
Junibakti Sanubari
Bennie L. Shearer, Jr.
R. Srikant
Erik G. Strom
Gary J. Sullivan
Oguz Sunay
Joseph G. Teti, Jr
Lang Tong
Cesar Vargas-Rosales
William E. Ryan
Abu-Bakarr Sesay
Eric R. Wandel
Richard B. Wells
Richard D. Wesel
Brian D. Woerner
Gregory W. Wornell
Jian Qiu Zhang
Yiming Zhou

CALL FOR NOMINATIONS

IEEE Information Theory Society Paper Award

The Information Theory Society Paper Award shall be given annually for an outstanding publication in the fields of interest to the Society appearing anywhere during the preceding two calendar years (2000-2001).

The purpose of this Award is to recognize exceptional publications in the field and to stimulate interest in and encourage contributions to fields of interest of the Society. The Award consists of an appropriately worded certificate(s) and an honorarium of $ 10,000 equally split among the authors of the paper.

Nomination Procedure (from the bylaws):

The Awards Subcommittee shall take into account

(a) all nominations submitted in response to the open call for nominations in the last two years;

(b) the nominations supplied by the Publications Committee in the last two years;

(c) any nomination that its members may want to submit for consideration.

The Awards Subcommittee shall submit to the Board a list of up to three selected nominations for the Information Theory Society Paper Award at least 3 weeks in advance of the first Board meeting following June 1st of the award year, and shall enclose a rationale for each nominated paper explaining its contribution to the field.

The Board shall then vote for the nominees by ballot, conducted by the Society President or designee at the first Board Meeting following June 1st of the award year. The paper receiving the highest total number of votes in the balloting shall be declared the winner of the Information Theory Society Paper Award.

Please send a brief rationale (limited to 300 words) for each nominated paper explaining its contribution to the field by April 15, 2002 to the Society's First Vice President: Professor A.J. Han Vinck via e-mail (Vinck@exp-math.uni-essen.de) or by post addressed as: A.J. Han Vinck, Institute for Experimental Mathematics, University of Essen, Ellernstr. 29, 45326, Essen, Germany.

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." A list of the 2001 class of IEEE Fellows can be found through the IEEE Website at (http://www.ieee.org/about/awards/fellows/new-fellows.htm).

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/about/awards/fellows/request.htm/

A hardcopy may be requested by sending email to fellow-kit @ieee.org.

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!

From Marconi to Wireless Internet: An Information Theoretic Perspective

Vijay Bhargava

December 12, 1901. A signal is transmitted from a high power spark transmitter located in Poldhu, Cornwall, England. Some 3500 kilometers away at Signal Hill, in St. John's, Newfoundland, Canada, a nine foot long kite carries an antenna to the clouds. Guglielmo Marconi and his assistant George Kemp wait. The first transatlantic wireless communication is received, and the world gets a little smaller. Since that time wireless technologies and the application of Information Theory has altered many aspects of telecommunications and human conditions.

We now fast forward to the 1940's, the concept of cellular communications is born and as we all know, Shannon writes his landmark paper resulting in the new discipline of Information Theory. In the next several decades members of the Information Theory Society will invent: BCH and Reed Solomon codes; the Viterbi algorithm; public key cryptography; compression algorithms; coded modulation; CDMA and multiuser detection; turbo codes, and space-time codes. Almost all of these are being used or are planned to be used in second and third-generation cellular

(From left to right) IEEE Newfoundland Section Chair Yves Fontaine, IEEE 1996 President Wally Read, 2000 IT Society President Vijay Bhargava and Professor S.O. Young at Signal Hill on 12 December 2001. In the back is Cabot Tower, constructed on Signal Hill in 1897 to commemorate the 400th anniversary of John Cabot's landfall in North America.

wireless communications systems, and several other wireless communications systems.

December 12, 2001. Politicians, musicians and other celebrities gather in St. John's for the Centenary Celebration of Marconi's wireless transmission. The Canadian Broadcasting Corporation (CBC) in cooperation with its sister organizations in England and Italy is doing a live-show in front of some 1000 people. At 12:30 p.m. Marconi's grandson, Guglielmo Marconi Giovenelli, tapped three times on a telegraph Key in Poldhu. There was silence and then a technician yelled "We are receiving it". We all erupted in cheers!

Looking ahead, by the year 2003, the world will have more wireless phones than wired phones. Indeed it may well be the preferred and most affordable mode for accessing the Internet. And Information Theory will continue to play its role in removing limitations on wireless communications.

Shannon Symposium and Statue Dedication at CMRR

Paul H. Siegel

At 2 PM on October 16, 2001, a statue of Claude Elwood Shannon, the Father of Information Theory, was dedicated in the lobby of the Center for Magnetic Recording Research (CMRR) at the University of California, San Diego. The sculpture is one of six casts of the bust originally commissioned by the IEEE Information Theory Society, in a project coordinated by Professor Dave Neuhoff of the University of Michigan. (The other five statues have been unveiled in Shannon Park in Gaylord, Michigan; Lucent-Bell Labs in Murray Hill, New Jersey; AT&T Shannon Labs in Florham Park, New Jersey; MIT in Cambridge, Massachusetts; and, most recently, the University of Michigan in Ann Arbor, Michigan.)

In conjunction with the dedication, a symposium honoring Shannon's life and work was held on October 15th and the morning of October 16th. The symposium and dedication ceremony were attended by an audience of approximately 100 people, including many UCSD students.

Generous support for both events, including a live webcast of the symposium, was provided by the California Institute of Telecommunications and Information Technology (Cal(IT)^2) at UCSD. The Jacobs School of Engineering and UCSD-TV supplied the resources to videotape the symposium proceedings, as well as interviews with many of the speakers, for use in a forthcoming UCSD-TV documentary highlighting the enormous impact of Shannon's genius.

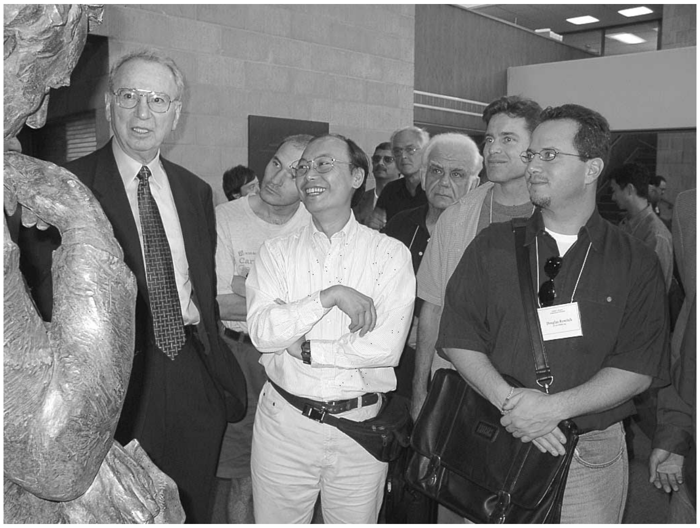
The acquisition of the sculpture and the organization of the Shannon Symposium were spearheaded by Jack Keil Wolf, who is a Professor in the Electrical and Computer Engineering department in the Jacobs School of Engineering, and holder of one of the four CMRR endowed chairs.

The Shannon Symposium program included invited technical presentations and personal reflections by fourteen information theorists from industry and academia, including CMRR Director Paul Siegel and UCSD Professor Alon Orlitsky. Many of the speakers themselves have made enormous contributions to the astounding advances in telecommunications that have transformed our world in the past half-century. Among them were six recipients of the prestigious Claude E. Shannon Award, the highest technical honor bestowed upon an individual by the IEEE Information Theory Society. The Shannon Award, which Jack Wolf himself received in 2001, is given annually in recognition of consistent and profound contributions to the field of information theory.

The Symposium speakers and their presentation titles were as follows:

Toby Berger, "Living Systems are Shannon Optimum Without Coding"

Paul Siegel, "The Continuing Miracle of Information Storage Technology"



Irwing Jacobs and others admire the new Shannon statue at CMRR.

(Left to right) Bob Conn, Gene Daub, Jack Wolf, and Marsha Chandler with the newly dedicated Shannon Statue.

Jacob Ziv and Alon Orlitsky, "Universal Data Compression"

David Neuhoff, "Time Stamp Coding-A Problem Shannon Did Not Answer"

Thomas Cover, "The Value of State Information in Communications and Data Compression"

G. David Forney Jr., "Approaching Channel Capacity"

Edward van der Meulen, "The Duality Between Successive Refinement of Information by Source Coding with Fidelity Constraints and Efficient Multilevel Channel Coding Under Cost Constraints"

Robert Lucky, "Impact of Shannon on Modern Telecommunications"

Ian Blake, "Randomness and Determination in Coding Theory"

Andrew Viterbi, "Quantized Iterative Decoding with Closed-Form Density Evolution Recursions for LDPC Codes on the AWGN Channel"

Jack and Toby Wolf with granddaughter Rachel get ready to unveil the new Shannon statue at CMRR at UCSD.

Solomon Golomb, “The Claude Shannon I Knew”

Elwyn Berlekamp, “Shannon’s Work on Block Code Performance and It’s Impact”

Shu Lin, “ Construction of Low Density Parity Check Codes: Combinatorial Approaches”

Robert McEliece “The Generalized Distributive Law (with Loops) and Free Energy Minimization”

The dedication ceremony that followed the Symposium was hosted by Jack Wolf, and included remarks from UCSD Senior Vice Chancellor Marsha Chandler; UCSD Professor and Director of the San Diego Division of the California Institute for Telecommunications and Information Technology Ramesh Rao; and Jacobs School of Engineering Dean Bob Conn. The next speaker, Qualcomm Chairman and CEO — and former UCSD faculty member — Dr. Irwin Jacobs, commented on the enormous impact of Shannon’s work upon communications and shared a fascinating historical tidbit, namely that in 1967 Claude Shannon was named a Fellow of Muir College at UCSD. Sculptor Eugene Daub concluded with remarks about the creative process from which emerged his beautiful and moving work of art. Finally, to the delight of all in attendance, the bust was unveiled by Rachel Wolf, Jack Wolf’s granddaughter.

The bronze plaque on the pedestal of the statue reads:

CLAUDE ELWOOD SHANNON
1916-2001

Father of Information Theory

His formulation of the mathematical
theory of communication provided
the foundation for the development of
data storage and transmission systems
that launched the information age.

Dedicated October 16, 2001

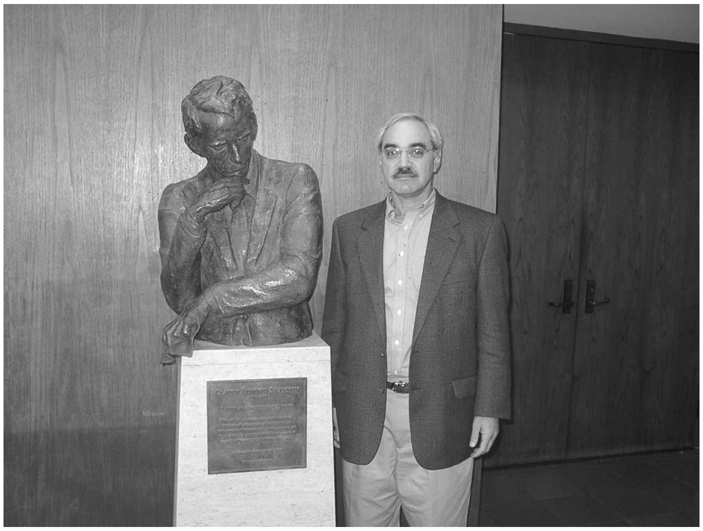
Eugene Daub, Sculptor

As depicted in the sculpture, Shannon holds in his left hand a sheet of paper. On this sheet is inscribed a formula taken from Shannon’s celebrated 1948 paper, “A Mathematical Theory of Communication,” whose publication is universally acknowledged to mark the genesis of information theory. The formula, selected for its relevance to digital data recording and communications, gives the capacity of a discrete noisy channel:

$$C = \mathrm{Max}\ (H(X) - Hy(X)).$$

Be sure to enjoy the sculpture that now graces the CMRR lobby on your next visit to the UCSD campus, and look for the symposium proceedings and further details about the UCSD-TV documentary on the CMRR and Cal(IT)^2 websites (www.ucsd.edu/cmrr and www.calit2.net, respectively).

Jack Wolf reads the plaque accompanying the bust of Shannon.



Dave Neuhof, of the University of Michigan, and the Shannon statue.

GOLOMB'S PUZZLE COLUMN™

WHAT COLOR IS MY HAT? SOLUTIONS

1. In this version, the members of the team are lined up single file, and each member sees the colors of all the hats ahead, but not his/her own or those behind. They are promised that not all the hats will be the same color; and they will be interrogated ("What color is your hat?") from the back of the line forward, one at a time. Each member can say either "white" or "black" or "pass". A single wrong color causes the whole team to lose, which also happens if they all say "pass".

A winning strategy is the following: When it is a member's turn, if all behind him/her have said "pass", that member will also say "pass" unless everyone in front has a white hat, in which case he/she should say "black". Thereafter, everyone ahead can say "pass" (or "white", which will also be correct). If everyone behind the first-in-line has said "pass", that person can correctly say "black".

Note that this strategy guarantees that the team will win.

2. In this version, the n members of the team are assembled in a room where the members can see the color of every hat but their own, and they are interrogated in random order, again with the assurance that not all hats have the same color.

In reality, the team members have more information (as a result of seeing more hats) than in the previous case. If they wish, they can adopt (and adapt) the winning strategy from that case. The first member to be asked "What color is your hat" plays the role of the last-in-line from Case 1; the second to be asked plays the role of the next-to-last- in- line from Case 1; and so on. The winning result is the same.

3. This version is substantially different. Here the n team members are in separate rooms, numbered from 1 to n, with no communication between them. Each is told the colors of the hats of all the others, but not of their own hats; and they do not hear how any other member has answered "What color is your hat?" Also, the n colors have been assigned independently and at random, with each hat being equally likely white or black. In particular, all hats might be the same color, though this would be unlikely for large n.

With three team members, they could agree in advance on the following strategy: If the other two hats have opposite colors, say "pass". If the other two hats have the same color, guess the other color. This strategy will win unless all three hats have the same color, which will happen only one-fourth of the time; so the team will win three-fourths of the time. (Note that when all three hats are the same color, all three team members guess wrong, while in the other cases, there is one correct guess and two "passes". Thus, over the ensemble of all situations, there are equally many correct and incorrect guesses, so the laws of probability are not violated.)

A simple generalization to the case of $n=2^r-1$ team members is as follows. The team members agree in advance on a single-error-correcting $(n,n-r)$Hamming code. Each member's room number becomes one of the n *positions* in the codewords. Each member rewrites the r parity-check equations of the code so that r–1 of the resulting equations do not involve his/her own *position*. Upon learning the colors of the others' hats, these r–1 equations are tested. If at least one *fails*, our team member says "pass". Only if all these other r–1 equations *check*, our team member picks the hat color that makes the r^{th} equation fail. By this strategy, the team will *win*, *unless* the random assignment of hat colors matches a Hamming codeword. When the pattern is not a codeword, the team member who "guesses" is at the error location, while all the others say "pass". When the pattern *is* a codeword, all n team members guess incorrectly. Since single errors are more common than codewords, this strategy succeeds with probability $1–2^{-r}$. (The special case of $n = 3$, considered earlier, is the case of $r = 2$.)

Between successive values of $n=2^r–1$, where the best strategy, just described, wins with probability $1–2^{-r}$, there may be covering codes which achieve intermediate results. These coding strategies for guessing hat colors are described in considerable detail in [1], which was my source for Case 3. This "hat problem" has actually inspired research leading to the discovery of new "covering codes".

Reference

1. "Why Mathematicians Now Care About Their Hat Color", by Sara Robinson, *The New York Times*, SCIENCE, April 10, 2001, page D5.

CALL FOR PAPERS

2002 IEEE International Symposium on Information Theory

Palais de Beaulieu, Lausanne, Switzerland
June 30 – July 5, 2002

General Co-Chairs:
James L. Massey
Bixio Rimoldi

Program Committee:
Amos Lapidoth (co-chair)
Emre Telatar (co-chair)
Venkat Anantharam
Erdal Arıkan
Alexander Barg
Ezio Biglieri
Giuseppe Caire
Pierre Chevillat
Daniel J. Costello, Jr.
Imre Csiszár
Evangelos Eleftheriou
Michelle Effros
Dave Forney
Joachim Hagenauer
Bruce Hajek
Johannes Huber
K. A. Schouhamer Immink
Rolf Johannesson
Frank Kschischang
Sanjeev Kulkarni
P. Vijay Kumar
Hans-Andrea Loeliger
Thomas Marzetta
Ueli Maurer
Neri Merhav
Prakash Narayan
Balaji Prabhakar
Vincent Poor
Joachim Rosenthal
Ron Roth
Serap Savari
Shlomo Shamai
Amin Shokrollahi
Emina Soljanin
Yossi Steinberg
Michael Tanner
Henk van Tilborg
David Tse
Ugo Vaccaro
Han Vinck
Greg Wornell
Raymond Yeung
Ram Zamir

Sponsor Liaisons:
David Tse
Martin Vetterli

Finance:
Serge Vaudenay

Local Arrangements:
Rüdiger Urbanke

Publications:
Hans-Andrea Loeliger

Publicity:
Ueli Maurer
Michael Gastpar

The 2002 IEEE International Symposium on Information Theory will be held at the Palais de Beaulieu in Lausanne, Switzerland, from Sunday, June 30, through Friday, July 5, 2002.

Previously unpublished 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
Information theory and statistics
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 (not exceeding six pages) of sufficient detail to permit reasonable evaluation. The deadlines for submission is September 30, 2001 for paper copies and October 7, 2001 for electronic copies, with notification of decisions by February 8, 2002. In view of the large number of submissions expected, multiple submissions by the same author will receive especially stringent scrutiny. All accepted papers will be allowed twenty minutes for presentation, and one-page abstracts will be printed in the conference proceedings. Authors are strongly encouraged to submit electronic versions of their summaries by following the guidelines on the symposium web page. For those unable to submit electronically, *four copies* of the summary should be mailed to

Ms. Monique Borcard
ISIT 2002 Paper Submission
EPFL — DSC — LTHI
CH-1015 Lausanne
Switzerland

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 included in subsequent mailings, and will be posted at the symposium web site

`http://isit02.epfl.ch`

Inquiries on general matters related to the symposium should be addressed to

Prof. Bixio Rimoldi
Communication Systems Department
Swiss Federal Institute of Technology
CH-1015 Lausanne, Switzerland
E-mail: `isit02chair@epfl.ch`
Phone: +41 21 693 76 62
Fax: +41 21 693 43 12

Announcement and Call for Papers

2002 IEEE Information Theory Workshop

Bangalore, India, October 20-25, 2002.

General Co-Chairs

Thomas E. Fuja
Dept. of Electrical Engineering
University of Notre Dame
Notre Dame, IN 46556
tfuja@nd.edu
Phone: (219) 631-7244
FAX: (219) 631-4393

Anurag Kumar
Dept. of Electrical Engineering
Indian Institute of Science
Bangalore, India
anurag@ece.iisc.ernet.in
Phone: (91)-80-360 0855
FAX: (91)-80-360 0991

Technical Co-Chairs

Prakash Narayan.
University of Maryland
prakash@eng.umd.edu

B. Sundar Rajan
Indian Institute of Science
bsrajan@ece.iisc.ernet.in

Local Arrangements

Vijay Bhargava
University of Victoria
bhargava@engr.uvic.ca

Vinod Sharma
Indian Institute of Science
vinod@ece.iisc.ernet.in

Treasurer

Marc Fossorier
University of Hawaii
marc@aravis.eng.hawaii.edu

Workshop Announcement

The 2002 IEEE Information Theory Workshop will be held at the Windsor Manor Sheraton Hotel, Bangalore, India. The workshop will begin on Sunday, October 20, 2002 and end on Friday, October 25, 2002.

Program Information

Invited Papers and Plenaries

There will be seven half-day sessions featuring invited speakers; these sessions will be organized around the seven topics listed below.

- Communication networks
- Channel coding and modulation
- Shannon theory
- Information theory and statistics
- Space-time coding and processing
- Source coding
- Cryptography

There will also be plenary talks by G. David Forney and Thomas Kailath.

Contributed Papers

There will be slots for approximately fifteen contributed papers in addition to the invited papers described above; therefore, papers presenting new results in the above areas are solicited. The submission deadline is May 1, 2002. Any submissions that cannot be accommodated as a contributed paper will be considered as a "recent result" (see below) unless the authors indicate otherwise.

Recent Results Sessions

Papers presenting recent results on any topic of interest to the information theory community are solicited. One-page summaries of these papers will be published in the workshop proceedings, provided they are submitted by July 1, 2002; however, on-site recent result contributions will also be accepted.

Further Inquiries

Further information including submission guidelines and contact information will be available at the ITW 2002 website:

http://www.iisc.ernet.in/ieee-itw2002

CALL FOR PAPERS

ISITA2002
2002 International Symposium on Information Theory and Its Applications

October 7-11, 2002

Xi'an International Conference Center, Xi'an, the People's Republic of China

2002 International Symposium on Information Theory and Its Applications (ISITA 2002) will be held at Xi'an International Conference Center, Xi'an, the People's Republic of China on October 7-11, 2002. This symposium is organized by the Institute of Information Theory and Its Applications and Institute of Artificial Intelligence and Robotics, Xi'an Jiaotong University. Xi'an, the capital of the Silk-road, is situated in the heart of China. It is a city full of historic sights represented by the Artistic Reproduction of the Battle Formation in Qin Dynasty.

ISITA2002 will be held with the technical co-sponsorship of the IEEE Information Theory Society and the Institution of Electronics, Information and Communication Engineers (IEICE)

The Symposium will include regular technical sessions, plenary sessions and special sessions.

The objective of ISITA is to provide a forum for researchers and technologists to present new ideas and contributions related to information theory and its applications.

The topics of interest include but not are limited to the following:

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

ISITA 2002 will be held in conjunction with International Symposium on Nonlinear Theory and its Applications (NOLTA2002). Crossfertilization of both fields is strongly encouraged.

For submission, an extended summary (500-1000 words) including title, topic, authors' names, affiliations and e-mail address are requested. Summary must be submitted electronically in PDF or postscript format. **ONLY ELECTRONIC SUBMISSIONS WILL BE ACCEPTED**. No hard copies will be accepted.

All summaries will be peer reviewed by the ISITA2002 Technical Program Committee. Authors are expected to present their paper at the Symposium. **AT LEAST ONE AUTHOR OF EACH PAPER MUST REGISTER FOR THE SYMPOSIUM FOR PAPERS TO BE INCLUDED IN THE PROGRAM**.

For further information please visit the symposium official web site,

http://ISITA2002.katayama.nuee.nagoya-u.ac.jp/

or e-mail to,

isita2002@katayama.nuee.nagoya-u.ac.jp

Important Dates:

Submission of 1-page summaries:	May 1 - **June 2**, 2002
(*ELECTRONIC SUBMISSIONS ONLY*)	
Deadline for special session proposal:	June 2, 2002
Notification of acceptance:	July 1, 2002
Deadline for 4-page camera-ready papers:	July 31, 2002
Deadline for author registration:	July 31, 2002

International Advisory Committee Chair

Hideki Imai (Tokyo Univ.)

Symposium General Chairs

Nanning Zheng (Xi'an Jiaotong Univ.), Shinsaku Mori (Nippon Inst. of Tech.), Akira Ogawa (Meijo Univ.)

7th International OFDM-Workshop

September 10th and 11th, 2002
Hamburg, Germany

Notification 2002

Dear friends,

the discussions focused on the next generation of mobile communication systems will increase the interest in flexible and adaptive transmission techniques. The OFDM modulation scheme offers these properties at a comparably low degree of computational complexity and has therefore gained a lot of attention during the last years.

As a platform for discussions and exchange among researcher active in this field we plan to continue the international workshop on communication systems related to multi-carrier communications techniques.

Today we would like to invite you to next year's event, the 7th International OFDM-Workshop in Hamburg, Germany on September 10th and 11th, 2002 at the Hotel Hafen Hamburg.

Information concerning InOWo'02 will be published in time on the workshop web site

http://ofdm.tu-harburg.de

Deadlines

Deadline for Extended Abstracts:	June 2nd, 2002
Notification of Acceptance:	July 5th, 2002
Camera-Ready Papers Due:	August 11th, 2002
Early Registration:	August 11th, 2002

I am looking forward to seeing you in Hamburg next year.

Sincerely yours,

Hermann Rohling

Conference Chair

Prof. Hermann Rohling
Department of Telecommunications
Technical University Hamburg-Harburg
Eißendorfer Straße 40
21073 Hamburg, Germany
Phone: +49 (040) 42878–3028

OFDM-Workshop Secretariat

Dirk Galda, Tobias Giebel
Department of Telecommunications
Technical University Hamburg-Harburg
Phone: +49 (040) 42878–2745
Fax: +49 (040) 42878–2281
E-Mail: OFDM@tu-harburg.de
http://ofdm.tu-harburg.de

General Co-Chairs:
Hideki Imai
Robert McEliece
Ryuji Kohno

Program Committee:
Brian Marcus (Co -chair)
Shojiro Sakata (Co-chair)
Te Sun Han (Co-chair)
Venkat Anantharam
Erdal Arikan
Martin Bossert
Roy Cideciyan
Gerard Cohen
Thomas Ericson
Meir Feder
Tadashi Fujino
Toru Fujiwara
Joachim Hagenauer
Bruce Hajek
Tom Hoeholdt
Brian L. Hughes
Kees A. Schouhamer Immink
Fumio Kanaya
John Kieffer
Kingo Kobayashi
Tamas Linder
Toshiyasu Matsushima
Dharmendra Modha
David L. Neuhoff
Ikuo Oka
Alon Orlitsky
Tom Richardson
Ron Roth
Kohichi Sakaniwa
Amin Shokrollahi
Hatsukazu Tanaka
R. Michael Tanner
David Tse
Henk C.A. van Tilborg
Mahesh K. Varanasi
A. J. Han Vinck
Stefan Wolf
Kazuhiko Yamaguchi
Raymond Yeung
Bin Yu
Hirosuke Yamamoto
Sandro Zampieri
Zhen Zhang

International Advisory Committee Chair:
Vijay Bharagava

Executive Committee Secretary:
Motohiko Isaka
Hideki Ochiai

Finance:
Takeshi Hashimoto
Hirohito Suda
Toyoo Takata

Registration:
Koichiro Wakasugi
Toshiyasu Matsushima
Keiichi Iwamura

Local Arrangements:
Iwao Sasase
Tomohiko Uyematsu
Robert Morelos-Zaragoza
Tomoaki Ohtsuki
Yukitoshi Sanada

Publications:
Ikuo Oka
Atsuko Miyaji
Masayoshi Ohashi

Publicity:
Toru Fujiwara
Masayuki Hattori
Atsuhiro Yamagishi
Nobukazu Doi
Shinichi Kawamura

First Call for Papers

2003 IEEE International Symposium on Information Theory

Pacifico Yokohama, Yokohama, Japan
June 29 - July 4, 2003

The 2003 IEEE International Symposium on Information Theory will be held at Pacifico Yokohama, Yokohama, Japan, (http://www.pacifico.co.jp/) from Sunday, June 29, through Friday, July 4, 2003.

Previously unpublished contributions to the following areas are solicited

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

Papers will be reviewed on the basis of an extended abstract (not exceeding six pages) of sufficient detail to permit reasonable evaluation. The deadline for submission is November 1, 2002, with notification of decisions by March 1, 2003. In view of the large number of submissions expected, multiple submissions by the same author will receive especially stringent scrutiny. All accepted papers will be allowed twenty minutes for presentation, and one-page abstracts will be printed in the conference proceedings. Authors are strongly encouraged to submit electronic versions of their summaries in the form of PDF files by following the guidelines, which will be posted in June on the TPC web pages linked with the symposium web site. Anybody having trouble in submitting PDF files should make contact with

Dr. **Kazuhiko Yamaguchi**
ISIT 2003 Paper Submission
The University of Electro-Communications
Department of Information and Communication Engineering
Chofugaoka 1 -5-1, Chofu -shi, Tokyo, 182-8585 JAPAN
Email: yama@ice.uec.ac.jp

Detailed information on the technical program, special events, accommodations, travel arrangements, excursions and applications for travel grants will be included in subsequent mailings, and will be posted at Symposium web site:

http://www.kohnolab.dnj.ynu.ac.jp/~isit2003/

Inquiries on general matters related to the symposium should be addressed to

Ryuji Kohno, Professor, Division Head,
Yokohama National University, Graduate School of Engineering
Division of Physics, Electrical and Computer Engineering
79-5 Tokiwadai, Hodogaya-ku, Yokohama, 240-8501 JAPAN
Email: isit2003@kohnolab.dnj.ynu.ac.jp
Tel:+81 -45-339-4116, Fax(G4):+81-45-338 -1157

Conference Calendar

DATE	CONFERENCE	LOCATION	CONTACT/INFORMATION	DUE DATE
March 17-21, 2002	**2002 IEEE Wireless Communications and Networking Conference (WCNC 2002)**	Orlando, Florida, USA	Dick Lynch Verizon Wireless, USA www.wcnc.org/2002	August 15, 2001
April 28-May 2, 2002	**2002 IEEE International Conference on Communications (ICC 2002)**	New York, New York, USA	Mark Karol Avaya Inc., USA mk@avaya.com www.icc2002.com	August 15, 2001
May 5-11, 2003	**2003 International Conference on Communications (ICC 2003)**	Anchorage Convention Center Anchorage, AK	Ocie Mitchell GCI 800 E. Dimond Blvd Suite 3-213 Anchorage, AK 99515 (+1 907 868 6160 +1 907 868 9731 (Fax) omitchell@gci.com	
May 19-22, 2002	**2002 IEEE Communications Theory Workshop**	Sundial Beach Resort Sanibel Island, FL	Prof. Gordon Stuber GCATT, Room 571 250 14th Street, NW Atlanta, GA 30318 +1 404 894 2923 +1 404 894 7883 (Fax) stuber@ece.gatech.edu http://www.ct02.gatech.edu	March 15, 2002
June 23-27, 2002	**INFOCOM 2002**	New York Hilton New York, NY	Dr. Parviz Kermani IBM-Watson Research Center 30 Saw Mill River Road Hawthorne, NY 10532 (+1 914 784 7769 +1 914 784 6205 (Fax) parviz@us.ibm.com http://www.ieee-infocom.org/2002/	July 31, 2001
June 30-July 5, 2002	**2002 IEEE International Symposium on Information Theory**	Lausanne, Switerland	Palais de Beaulieu, Prof. Bixio Rimoldi Communication Systems Department Swiss Federal Institute of Technology CH-1015 Lausanne, Switzerland E-mail: isit02chair@epfl.ch Phone: +41 21 693 76 62 Fax: +41 21 693 43 12	September 30, 2001

Continued on next page

Conference Calendar

DATE	CONFERENCE	LOCATION	CONTACT/INFORMATION	DUE DATE
October 7-11, 2002	**2002 International Symposium on Information Theory and Its Applications (ISITA 2002)**	Xi'an International Conference Center, Xi'an, PRC	Kouichi Yamazaki isita2002@katayama.nuee.nagoya-u.ac.jp ISITA2002.katayama.nuee.nagoya-u.ac.jp/	June, 2, 2002
November 18-22, 2002	**GLOBECOM 2002 - 2002 IEEE Global Telecommunications Conference**	Taipei International Conventional Center, Taipei, Taiwan	Mr. Douglas S. J. Hsiao 12, Lane 551 Min-Tsu Road Sec. 5, Yang-Mei, Taoyuan 326 TAIWAN +886 3 424 5210 +886 3 424 4168 (Fax) sjhsiao@chttl.com.tw	TBA
December 1-5, 2003	**GLOBECOM 2003**	San Francisco Marriott San Francisco, CA	Ms. Patricia Dyett IEEE Communications Society 305 E. 47th St., 9th Floor New York, NY 10017 +1 212 705 8999 (Fax) +1 212 705 8943 GLO2003C@comsoc.org	

IEEE
IEEE Information Theory
Society Newsletter

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