IEEE Information Theory Society Newsletter

Vol. 54, No. 4, December 2004 Editor: Lance C. Pérez ISSN 1059-2362

President's Column

It's been almost a year since I became President of this Society. As I wrote in my first column at the beginning of this year our main task at hand is the broadening of the technical coverage and the globalization of the Society. We need to put a stop to the recent drop in IT Society membership and instead expand it. I am aware that this is a long-term challenge and not much can be accomplished in the short term. However, I feel that we are beginning to take one small, but sure, step.

ISITA 2004 General Co-Chairs Katsuhiro Nakamura and Ezio Biglieri with IT Society President Hideki Imai.

First, I will report the situation with regards to the globalization of the Society. As I indicated in my March column, we are promoting collaboration between the Society of Information Theory and its Applications (SITA) and our Society. The 2004 International Symposium on Information Theory and its Applications (ISITA 2004) was held in Parma, Italy, in October, sponsored by SITA and technically cosponsored by our Society. Many key members of the IT Society were there because a Board of Governors meeting was held. This emerging cooperation is symbolized in the accompanying photograph of the General Co-Chairs of the Symposium, Prof. Katsuhiro Nakamura and Prof. Ezio Biglieri, and myself at the ISITA 2004 reception. At the Symposium, the members of both Societies had fruitful discussions on various topics. It was also resolved at the IT Society BoG meeting that the cooperation of the two societies should be further encouraged.

Next, I will talk about the broadening of the technical coverage of the Society. As one movement to achieve this goal, we are creating a cooperative partnership with the International Association of Cryptologic Research (IACR). The IACR is the largest and most active international academic society in the area of cryptography. An ad hoc joint working group is now being established to investigate the feasibility of cooperative projects. As the first step of our partnership, the 2005 Information Theory Workshop (ITW05) on the Theory and Practice in Information-Theoretic Security is going to take place in Japan in October of next year. It is fitting that the area of this workshop is a fusion of cryptography and information theory. Moreover, these are times when cryptographic schemes based on computational assumptions are at risk of being broken and a new computing paradigm, such as quantum computing, is expected to emerge at any time. For this reason, it is evident that more emphasis will be placed on the cryptography of information-theoretic security (unconditionally secure cryptography) that is independent from any computational assumptions, and therefore, will not be threatened by the emergence of computers having infinite computational power. I encourage anybody interested in this new field to participate in ITW05.

Another thing I would like to mention is the IEEE Transactions on Information Theory. The number of cryptography related contributions to the Transactions is steadily increasing. Therefore we have reinforced the field of Complexity and Cryptography by increasing the number of Associate Editors in this area from one to two. This will make it more convenient than before for authors to contribute papers on cryptography to the Transactions. This should also be appealing to the cryptography community.

The biggest challenge in information theory is to construct coding schemes that achieve the limits of communications presented by Claude E. Shannon. The invention of turbo codes and LDPC codes has solved the problem for basic communication channels. However, information theory is not a dead subject. We still have to work out and generalize Shannon theory to make it of use in our life. In actual life,

continued on page 3

From the Editor

Lance C. Pérez

This issue of the IEEE Information Theory Society Newsletter once again honors the passing of an esteemed member of the Information Theory community. Alain Glavieux, one of the co-discoverers of turbo codes and iterative decoding, passed away in September. The Newsletter features a short memoriam to Alain written by his colleague and co-discoverer, Claude Berrou.

Please help make the Newsletter as interesting and informative as possible by offering suggestions and contributing news. The deadlines for the 2005 issues of the Newsletter are as follows:

Issue	**Deadline**
March 2005	January 15, 2005
June 2005	April 15, 2005
September 2005	July 15, 2005
December 2005	October 15, 2005

Electronic submission, especially in ascii, LaTeX and Word formats, is encouraged. Please keep in mind that any electronic photographs should be high resolution.

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

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

President's Column 1
From the Editor 2
In Memoriam of Alain Glavieux 3
Shannon Lecture 3
Kees ImminkWins SMPTE Progress Medal 5
The Historian's Column 6
Call for Nominations: 2005 Information Theory Society Aaron D. Wyner Award 7
Call for Nominations: 2005 IEEE Information Theory Society Paper Award 7
Call for Nominations: 2005 Joint Information Theory/Communications Society Paper Award . 7
Golomb's Puzzle Column 8
New Books 8
4th Asia-Europe Workshop on Concepts in Information Theory 9
Golomb's Puzzle Solutions 10
2004 International Symposium on Information Theory (ISIT) 11
Call for Papers: IEEE/ACM 13
Call for Papers: ITW 2005 14
Call for Papers: ISIT 2005 15
Call for Papers: ISIT 2006 16
Call for Participation: LANL Workshop 17
Call for Papers: OC 2005 17
Call for Papers: 2005 Canadian Worksop on Information Theory 18
Call for Papers: InOWo 2005 19
Conference Calendar 20

President's Column

Hideki Imai

there exist various communication channels besides the basic ones. It is our duty to challenge such unexplored channels.

Some of them are not easily discernible. Here is an example of what I mean by a problem not being easily discernible. Take the basic two-party protocols, namely, bit commitment and oblivious transfer, that are the basis for all cryptographic protocols. Just as Shannon looked into the quantifiable information content that can be transferred through a channel, we can ask the question of under what circumstances can we efficiently perform such cryptographic tasks. In fact, taking the information theoretic approach to this question, the limits and the conditions that constitute the protocol have been successfully demonstrated. This is another example of the combination of information theory and cryptography, and the expansion of the world of information theory.

In conclusion, our Society is on the sure way to expansion. However, as I discussed in my second column, the problems brought about by the electronic publication of the Transactions, such as open access, remain significant. Recently, an information theory (IT) category has been set up on the public preprint server ArXiv (arXiv.org). Our society has decided to actively promote contributing preprints to ArXiv. In the process, we shall find a new model for our Society in the IT age. We shall see the path our Society should take from there.

Our world is undergoing drastic changes. So is our Society. Let us see this moment as yet another opportunity for our Society to expand. In the hope of the further development of the IEEE Information Theory Society, I remain.

In Memoriam of Alain Glavieux

by Claude Berrou

Alain Glavieux, Professor and Deputy Director of ENST Bretagne, died on September 25, 2004, after spending many years fighting a long illness. He was 55 years old. He leaves behind his wife Marie-Louise, his adoptive daughter Christelle, and many friends.

Alain Glavieux
1949-2004

Prof. Glavieux graduated as an engineer from ENST (Paris). On his arrival at the newly founded ENST Bretagne in 1978, he designed a teaching program in digital communications and established and supervised a high-level research program in underwater communications. At the beginning of the 1990's, he contributed, with his colleague and friend Claude Berrou, to the invention of turbo codes which are considered today to be one of the major innovations of the post-Shannon era. The concepts used in turbo codes have, in particular, opened up the way for iterative probabilistic processing in communication receivers. For his work, Prof. Glavieux, along with Claude Berrou, received many French and international awards, including a Golden Jubilee Award for Technological Innovation (IEEE IT, 1998), the Richard W. Hamming Medal (IEEE, 2003) and the French Academy of Science's "Grand Prix France Télécom" award (2003).

His many students and all his colleagues, in France and abroad, appreciated Prof. Glavieux as a kind-hearted, understanding individual and an outstanding pedagogue. The Information Theory Society shares in the sorrow of his family, his relatives and his friends.

2004 Shannon Lecture

By Robert J. McEliece

2003 Shannon Award Winner Robert J. McEliece delivering his Shannon Lecture in top hat and tails at ISIT 2004 in Chicago.

In my Shannon Lecture at ISIT 2004 I tried to present my tribute to Shannon in an entertaining and multimedia way. But for this Newsletter Article, I will stick to the black-and white facts. If you want a more visual treatment, visit http://www.systems.caltech.edu/EE/Faculty/rjm/and click on "The 2004 Shannon Lecture."

The Hamming Code.

A long time ago I noticed that the (7,4) Hamming code can be visualized with a simple Venn diagram. Recently, with the help of Ed and Tomomi Soedarmadji, I developed a computer animation for illustrating this approach, which I demonstrated to the audience at ISIT. If you'd like to play around with it, just go to http://www.systems.caltech.edu/EE/Faculty/rjm/ and click on "Hamming Code Animation." The demonstration is more-or-less self-explanatory.

Surprisingly, the (7,4) Hamming code can be used to illustrate the power as well as the shortcomings of iterative decoding

based on graphical models. If you go to the "erasure correction" mode, you will soon convince your self that a simple (but suboptimum) erasure fill-in strategy will correct any pattern of two or fewer erasures. The situation with three erasures is much more interesting. Of the 35 patterns of three erasures, 25 are correctable using erasure fill-in, and 10 are not. These uncorrectable erasure patterns are in fact "'stopping sets," in the parlance of modern coding theory. Seven of the stopping sets correspond to weight-three codewords and are therefore not correctable with any algorithm, but three of the stopping sets are pseudocodewords, and in fact are correctable (though not with erasure fill-in).

I wondered what happens with the general Hamming code of length $2^m - 1$. And I came up with the following, which is the only Theorem in the talk.

Theorem. In the $n = 2^m–1, k = 2^m—1–m$ Hamming code, the minimum weight codeword or stopping set has weight 3. There are exactly $(4^m–32^m + 2)/6$ weight 3 codewords and $(5^m–3^{m+1} + 2^{m+1})/6$ weight three stopping sets.

Pictures from Mars, 1965 to Present

Everybody knows Shannon's definition of the fundamental problem of communication, as given in the introduction of *The Mathematical Theory of Communication*

"The fundamental problem of communication is that or reproducing at one point either exactly or approximately as message selected at another point."

But hardly anyone remembers what Shannon said next:

"Frequently the messages have meaning … [which is] irrelevant to the engineering problem."

Shannon's tongue-in-cheek remarks notwithstanding, I'd like to discuss messages that have real meaning: the bits that bring us information about the solar system. For this article, I'll just discuss the progress made in telecommunications efficiency from Mars to Earth in the time span 1965-2004.

Why Mars in particular? Only this: Since 1965 NASA's Jet Propulsion Laboratory has launched 11 successful (and 5 unsuccessful) earth-to-mars missions, which is enough so that I can illustrate the incremental improvements made in the coding and compression subsystems, and thereby assess the impact of Shannon on the technology of remote planetary imaging, which is my primary goal.

So now I will briefly describe 5 or 6 JPL spacecraft which have successfully visited Mars and sent back pictures, each spacecraft in the sequence having an increasingly sophisticated combination of coding and/or compression algorithms, and try to assess Shannon's impact on space communications.

Summary: Data Rate 8.33 bps. No Coding, No Compression.

Viking: There were two Viking Orbiter/Lander spacecraft, launched in the Summer of 1975 and reaching Mars about a year later. Scientifically, this was the first Mars Landing. Information Theoretically, this was the first Mars mission to use error-correction.

Summary: Data Rate: 3kbps, (32,6) Biorthogonal Code, No Compression.

Mars Global Surveyor became the first successful mission to the red planet in two decades when it launched November 7, 1996 (251 Gm), and entered orbit on September 12, 1997 (254 Gm). The mission has studied the entire Martian surface, atmosphere, and interior, and has returned more data about the red planet than all other Mars missions combined.

Summary: Data Rate 130 Kbps, Coding: K = 7 R = 1/2 convolutional code plus a (255,223) Reed-Solomon outer code. Compression: 2:1 Rice compression.

Pathfinder:

Launch Date: December 1996 Arrival Date: July 1997. The Mars Pathfinder mission consisted of a stationary lander and a surface rover (Sojourner).

Summary: Data Rate: 8 Kbps, Coding K=15, R = 1/6 convolutional code plus (255,223) outer RS code. Compression 6;1 lossy JPEG..

Mars Exploration Rover:

MER was launched toward Mars on June 10 and July 7, 2003 to take advantage of the unusually close opposition August 2003. Both spacecraft landed in January 2004.

Summary: Data rate 168 Kbps, Coding K=15, R = 1/6 convolutional code plus (255,223) outer RS code. Compression 12;1 lossy ICER.

Shannon versus Newton.

The following table summarizes the salient acts about the various missions I described in the last section (in addition it includes data for the upcoming Mars Reconnaisance Orbiiter, set to launch in August 2005 and arrive at Mars in March 2006.

Spacecraft Year Data Rate @215 Gm Coding Data Compression Mariner 4 1965 8.33 bps None None Voyager 1 & 2 1976 3000 bps Biorthogonal None Mars Global Surveyor 1997 128000 bps (7,1/2) + RS 2:1 Rice Pathfinder 1997 8000 bps (15,1/6) + RS 6:1 JPEG MER 2004 168000 (15,1/6) + RS 12:1 ICER MRO 2007 12 Mbps` CCSDS Turbo 2:1 Felics

We thus see that in the 39 years from Mariner 4 to Mars Exploration Rover, the rate at which we can communicate images has increased from 8.33 bits per second to 168,000 bits per second, an increase of 4.2 orders of magnitude, or 42 dB. Where has this astonishing increase come from?

In general terms, the telecommunications improvements are of two types:

those attributable to Physics (aperture, power, system temperature, etc.) and those attributable to Mathematics (source and channel coding). After a short calculation, using data supplied to me by Shervin Shambayati and others, I reached the following conclusion: Using Newton to represent Physics and Shannon to represent Mathematics, the 42 dB is accounted for as follows.

Spacecraft	Year	Data Rate @215 Gm	Coding	Data Compression
Mariner 4	1965	8.33 bps	None	None
Voyager 1 & 2	1976	3000 bps	Biorthogonal	None
Mars Global Surveyor	1997	128000 bps	(7,1/2) + RS	2:1 Rice
Pathfinder	1997	8000 bps	(15,1/6) + RS	6:1 JPEG
MER	2004	168000	(15,1/6) + RS	12:1 ICER
MRO	2007	12 Mbps`	CCSDS Turbo	2:1 Felics

Newton: 63%
Shannon 37%

Not bad for a boy who grew up in Gaylord Michigan!

The Future of Mars-Earth Communications

It is natural to wonder about the future: will we see another 42 dB improvement in the next 40 years? I cannot answer that, but researchers in many areas of interplanetary telecommunications are busy.

Channel Coding: Turbo codes will almost certainly give way to some kind of LDPC codes, because of their favorable performance to complexity tradeoff, but little in the way of increased data rate can be hoped for because of the Shannon Limit.

Source Coding: Expert opinion seems to be that 15:1 compression is the limit, but this is not sure since there is no reliable Shannon Limit to guide us.

"Physics": Systems designers are doing advanced research into increasing the transmission frequency from X-band to K band and even optical frequencies. Also, the building of gigantic microwave antenna arrays (the "Square Kilometer Array," for example) is being contemplated.

Why should we care?

Why do we bother to explore the solar systems at all? Is it the search for extraterrestrial life that motivates us? I think not.

I only met Shannon once, at ISIT 1986 in Brighton. As co-chair (with Paddy Farrell) I sat at the Head Table next to Claude and his wife Betty. Shannon seemed reluctant to discuss technical matters, but on politics, music, and literature he was a font of knowledge. We soon discovered a common admiration for the poet T.S. Eliot. (In fact Shannon quotes Eliot in his 1959 paper "Coding theorems for a discrete source with a fidelity criterion.") Thus Shannon must have been familiar with the following lines from "Little Gidding", and which gives the best explanation of the "why" of research that I know of.

We shall not cease from exploration
And the end of all our exploring
Will be to arrive where we started
And know the place for the first time.

Kees Immink wins SMPTE Progress Medal

The Society of Motion Picture and Television Engineers (SMPTE) has awarded its premier accolade, the Progress Medal, to Kees A. Schouhamer Immink, president of Turing Machines Inc. Prof. Immink received the award for the central role he played in research and development of audio and video recording products.

It is virtually impossible to listen to digital audio, or watch digital video, played from any brand or type of recorder -optical, magnetic, or magneto optical-, -disc or tape- that does not use one of his inventions. He developed the coding technology of a wide variety of digital video and audio recorders such as the Compact Disc, Compact Disc Video, CD-R, MiniDisc, DAT, DCC, DVD, and recently the BluRay disc system. His research resulted in four books, more than 100 articles, and more than 1000 international patents; most of them are basic patents underlying all modern digital recorder products introduced since the early 1980s. His inventions cover such diverse topics as acoustics, optics, signal processing, servos, and notably coding technology.

Knighted by Beatrix, Queen of the Netherlands, Dr Immink has received, among others, an "Emmy", the AES Gold Medal, SMPTE Poniatoff Gold Medal, IEEE Masaru Ibuka consumer electronics award, and IEEE Edison Medal. He was inducted into the Consumer Electronics Hall of Fame, and elected into the Royal Netherlands Academy of Sciences. He has been honored with fellow status in many professional organizations, including the SMPTE, IEEE, AES, and IEE.

Dr Immink, a native of Rotterdam, The Netherlands, obtained his Master's and PhD degrees from the Eindhoven University of Technology. He is currently president and founder of Turing Machines Inc. He is a guest professor at the Institute for Experimental Mathematics, Essen-Duisburg University, Germany, and the National University of Singapore. He serves as immediate-past president of the Audio Engineering Society (AES).

The Historian's Column

A. Ephremides

Information Theory has had connections with several other fields. Computer Science, Physics, Probability Theory, Economics, Signal Processing, and, of course, Communications and Networking come to mind. Yet, there is one field with which Information Theory has not had any overt connection although it shares with it a great deal of common culture and, sometimes, techniques. This field is Control Theory. In fact, in recognition of the commonality of methodology and culture between the two fields, the Information Theory Society and the Control Systems Society have been in the same IEEE Division for many years and, with the exception of a brief interlude, continue to be so today. In tribute to this odd relationship, I thought I would take a look at the history of that field. In fact, in 1996 the main conference of the Control Systems Society, the Conference on Decision and Control (known as CDC and often attended regularly by some of our members) devoted a session to the celebration of the 300th anniversary of the birth of Optimal Control.

Considering that our field is only fifty some years old, it appears surprising that some kindred fields can be …. almost ancient. But of course, this is a superficial observation. Even though the precisely defined field of Information Theory was born in 1948, the motivation for it (through communication theory) precedes it by almost a century and, in fact, as documented in this column a few years ago, it goes all the way back to … (where else?) Ancient Greece. The first illustrations of coding ideas and remote communication can be traced to Homeric times. So, in retrospect, we know that everything has started in Ancient Greece. This is a purely unbiased view shared fully by all people of Hellenic descent and in part by almost everyone else. So, after paying the usual tribute to Ancient Greece as the root of all good and evil (just a note here for those who may not have detected it: I am clearly saying this in jest), let us move on to identify the origins of more specific elements of the field of Control Theory in its modern form.

Optimal Control Theory is a branch of Control Theory that is concerned with driving dynamical systems to a specific state in a fashion that optimizes a performance criterion. This particular branch of the field was apparently born in 1696. It is attributed to a problem that Johann Bernoulli considered during the early years of his tenure at the University of Groningen. Johann Bernoulli, the kid brother of Jacob Bernoulli (more familiar to us through his work on probability), considered the following intriguing problem. Consider two points in space, X and Y. Suppose X lies higher than Y relative to the earth's surface. Imagine an object at X. We want to find a curve connecting X and Y such that if we let an object at X fall toward Y following this curve, it reaches Y in minimum time. This is clearly a modern control theory problem and the first of its kind to be so clearly formulated.

Optimization problems per se had been studied for many centuries prior to that. In fact, the Ancient Greeks (there we go again) had considered, for example, what should be the shape of a region enclosed by a curve of given length that maximizes the area of the enclosed region (answer: the circle). Aristotle conjectured the correct answer on philosophical grounds (the circle is the perfect figure, so it would have to be it). But it was actually proven rigorously only in the 19th century.

What distinguishes this problem is the coupling of optimization with a dynamical system. In fact, this problem was termed the brachystochrone problem which in Greek means fastest or shortest time (we can't get away, it seems, from the Greeks, can we?). Apparently, this problem captured the imagination of a great many illustrious mathematicians of the time. In addition to Bernoulli (and his brother) other notables who offered independent solutions to it or who were involved in some way with this problem include Leibnitz, L'Hopital, Newton, and Galileo. By now you must be curious about the solution to this problem. Well, it turns out that the brachystochrone curve is what Bernoulli called a cycloid (which in Greek – not AGAIN! – means related to or akin to a circle). Such a curve is charted by rolling a circle of diameter equal to the vertical distance between X and Y along a horizontal line that passes through X. Then the graph traced by the point on the circle that touches the horizontal at X in its initial position (and reaches Y at its final position) is the curve along which an object under frictionless free fall will reach Y from X in minimum time. Jan Willems and Hector Sussmann had interesting articles relating to this problem in the proceedings of the 1996 CDC [1,2].

This fascinating historical observation should raise our respect for the field of optimal control. After all, we are involved with optimization all the time. Isn't Viterbi decoding a form of dynamic programming? Aren't we frequently posing problems of choosing encoders, decoders, modulators, demodulators, protocols, etc., that minimize error probability, delay, complexity criteria, etc., etc.? In a way the solution schema (wouldn't you know it, another Greek word) for all these problems is imbedded in the core of optimal control theory. So, to paraphrase J.F.K.'s famous pronouncement under the shadow of the Berlin wall, we are all … optimal control theorists!

[1] J.C. Willems, "1696: The Birth of Optimal Control", Proc. of IEEE CDC, December 1996, Kobe, Japan.

[2] H.J. Sussmann, "From the Brachystochrone to the Maximum Principle", Proc. of IEEE CDC, December 1996, Kobe, Japan.

Call for Nominations: 2005 Information Theory Society Aaron D. Wyner Award

The IT Society Aaron D. Wyner Award honors individuals who have shown outstanding leadership in, and provided long standing exceptional service to, the Information Theory community. This award was formerly known as the IT Society Distinguished Service Award.

Nominations for the Aaron D. Wyner Award can be submitted by anyone and are made by sending a letter of nomination to the President of the IT Society by April 15, 2005. The individual or individuals making the nomination have the primary responsibility for justifying why the nominee should receive this award.

How to nominate: Letters of nomination should

- Identify the nominee's areas of leadership and exceptional service, detailing the activities for which the nominee is believed to deserve this award;
- Include the nominee's current vita;
- Include two letters of endorsement.

Current officers and members of the IT Society Board of Governors are ineligible.

Please send all nominations by April 15, 2005 to
Steven W. McLaughlin
IEEE IT Society President
Georgia Tech Lorraine
2-3, rue Marconi
Metz Technopole
57070 Metz FRANCE
email: swm@ece.gatech.edu

Call for Nominations: 2005 IEEE Information Theory Society Paper Award

Nominations are invited for the 2005 IEEE Information Theory Society Paper Award.

Outstanding publications in the field of interest to the IT Society appearing anywhere during 2003 and 2004 are eligible. The purpose of this award is to recognize exceptional publications in the field and to stimulate interest in and encourage contributions to the fields of interest of the IT Society.

The Award consists of an appropriately worded certificate and an honorarium of US$1000 for a single author, or US$2000 equally split among multiple authors.

NOMINATION PROCEDURE: Please email a brief rationale (limited to 300 words) for each nominated paper explaining its contributions to the field by March 1, 2005 to the Transactions Editor-in-Chief at poor@princeton.edu, with a cc to Lynn Stetson at lstetson@princeton.edu.

Call for Nominations: 2005 Joint Information Theory/Communications Society Paper Award

The Joint Information Theory/Communications Society Paper Award recognizes one or two outstanding papers that address both communications and information theory. Any paper appearing in a ComSoc or IT Society publication during the year 2004 is eligible for the 2005 award.

Please send nominations to David Neuhoff (neuhoff@eecs.umich.edu) by February 1, 2004.

A Joint Award committee will make the selection by April 10, 2005.

GOLOMB'S PUZZLE COLUMN™

A QUADRATIC SEQUENCE

Solomon W. Golomb

Let $s_n = 2n^2 + 2n + 1$ for all integers $n \geq 0$. Thus, $S = \{s_n\} = \{1, 5, 13, 25, 41, 61, 85, 113, 145, 181, 221, 265, ...\}$. Some knowledge of elementary number theory will be helpful in addressing the following questions.

1. Prove that if p is a prime number that divides any term of the sequence S, then $p = 4m + 1$ for some positive integer m.

2. Show that *every* prime p of the form $4m + 1$ divides terms of the sequence S.

3. Show further that for each prime p of the form $4m + 1$, there are two residue classes, a and b, modulo p, such that p divides s_n for all $n \equiv a (\text{mod } p)$ and for all $n \equiv b (\text{mod } p)$, where $a + b \equiv -1 (\text{mod } p)$ and $a \neq b$. (For example, with $p = 5$, we can take $a = 1$ and $b = 3$.)

4. Note that $s_0 = 1^2$, $s_3 = 5^2$, and $s_{20} = 29^2$. Find all the values of n for which s_n is a square integer.

5. In the previous problem, consider the sequence $c = \{c_n\} = \{1, 5, 29, \dots\}$ of the numbers whose squares occur (in increasing order) in the sequence S. Find a recursion relation satisfied by the terms of C, and determine $\lim_{n\to\infty} (\frac{c_{n+1}}{c_n})$.

*6. Are any of the terms of S perfect cubes or higher powers?

*7. What can you say about the frequency of prime numbers in the sequence S?

(Complete solutions to the starred problems may exceed the current state of knowledge.)

New Books

By Raymond Yeung

Error Control Coding, 2nd Edition,
by Shu Lin and Daniel J. Costello. Prentice Hall, 2004, 1272 pp., $124, ISBN 0130426725.
Contents:
Coding for Reliable Digital Transmission and Storage; Introduction to Algebra; Linear Block Codes; Important Linear Block Codes; Cyclic Codes; Binary BCH Codes; Nonbinary BCH Codes, Reed-Solomon Codes, and Decoding Algorithms; Majority-Logic Decodable Codes; Trellises for Linear Block Codes; Reliability-Based Soft-Decision Decoding Algorithms for Linear Block Codes; Convolutional Codes; Trellis-Based Decoding Algorithms for Convolutional Codes; Sequential and Threshold Decoding of Convolutional Codes; Trellis-Based Soft-Decision Algorithms for Linear Block Codes; Concatenated Coding, Code Decomposition ad Multistage Decoding; Turbo Coding; Low Density Parity Check Codes; Trellis Coded Modulation; Block Coded Modulation; Burst-Error-Correcting Codes; Automatic-Repeat-Request Strategies.

Space-Time Codes and MIMO Systems,
by Mohinder Jankiraman. Artech House Publishers, 2004, 350 pp., £73, ISBN 1-58053-865-7.
Contents:
Introduction; The MIMO Wireless Channel; Channel Propagation,Fading & Link Budget Analysis; Space-Time Block Codes; Space-Time Trellis Codes; Layered Space-Time Codes; Orthogonal Frequency Division Multiplexing (OFDM); IEEE 802.11a Packet Transmission System; Space-Time Coding for Broadband Channel; The Way Ahead.

Wireless Sensor Networks Architectures and Protocols,
by Edgar H.\ Callaway. Auerbach Publications, 2004, 360 pp., $99.95, ISBN 0-8493-1823-8.
Contents:
Introduction to Wireless Sensor Networks; The Development of Wireless Sensor Networks; The Physical Layer; The Data Link Layer; The Network Layer; Practical Implementation Issues; Power Management; Antennas and the Definition of RF Performance; Electromagnetic Compatibility; Electrostatic Discharge; Wireless Sensor Network Standards; Summary and Opportunities for Future Development.

Information Theory, Coding and Cryptography,
by Ranjan Bose. McGraw-Hill, 2002, 288 pp., ISBN 0-07-048297-7, ISBN 0-07-123133-1 (international edition).
Contents:
Source Coding; Channel Capacity and Coding; Linear Block Codes for Error Correction; Cyclic Codes; Bose-Chaudhuri-Hocquenghem (BCH) Codes; Convolutional Codes; Trellis Coded Modulation (TCM); Cryptography.

A Course in Error-Correcting Codes,
by Jorn Justesen and Tom Hoholdt. European Mathematical Society, 2004, 204 pp., 39.50 €, ISBN 3-03719-001-9.

Codes for Mass Data Storage Systems, 2nd Edition,
by Kees A. Schouhamer Immink. Shannon Foundation Publishers, 2004, 350 pp., 91 €, ISBN 90-74249-27-2, http://www.shannonfoundation.org/order.html (web purchasing only).

Finite Automata,
by Mark V.\ Lawson. Chapman & Hall CRC, 2003, 320 pp., $69.95, ISBN 1-58488-255-7.

Handbook of Graph Theory,
edited by Jonathan L.\ Gross and Jay Yellen. CRC Press, 2003, 1176 pp., $119.95, ISBN 1-58488-090-2.

Computability Theory,
by S. Barry Cooper. Chapman & Hall CRC, 2003, 424 pp., $69.95, ISBN 1-58488-237-9.

Spanning Trees and Optimization Problems,
by Bang Ye Wu and Kun-Mao Chao. Chapman & Hall CRC, 2004, 200 pp., $79.95, ISBN 1-58488-436-3.

Telecommunications Performance Engineering,
edited by Roger Ackerley. IEE, 2004, 304 pp., £55, ISBN 0-86341-341-2.

Mobile and Wireless Communications: Key Technologies and Future Applications,
edited by Peter Smyth. IEE, 2004, 400 pp., £55, ISBN 0-86341-368-4.

Security for Mobility,
edited by Chris Mitchell. IEE, 2004, 464 pp., £63, ISBN 0-86341-337-4.

What is Thought?
by Eric B. Baum. MIT Press, 2004, 478 pp., $40, ISBN 0-262-02548-5.

Protocol,
by Alexander R. Galloway. MIT Press, 2004, 286 pp., $32.95, ISBN 0-262-07247-5.

The Digital Sublime: Myth, Power, and Cyberspace,
by Vincent Mosco. MIT Press, 2004, 218 pp., $27.95, ISBN 0-262-13439-X.

Imitation of Life: How Biology is Inspiring Computing,
by Nancy Forbes. MIT Press, 2004, 171 pp., $25.95, ISBN 0-262-06241-0.

Communication Network, Second Edition,
by Alberto Leon-Garcia. McGraw-Hill, 2004, 848 pp., $106.25, ISBN 0-07-246352-X, ISBN 0-07-119848-2 (international edition).

Handbook of Sensor Networks: Compact Wireless and Wired Sensing Systems,
by Mohammad Ilyas and Imad Mahgoub. CRC Press, 2004, 672 pp., $149.95, ISBN 0849319684.

Bluetooth Security,
by Christian Gehrmann, Joakim Persson and Ben Smeets. Artech House Publishers, 2004, 222 pp., £52, ISBN 1-58053-504-6.

OFDM for Wireless Communications Systems,
by Ramjee Prasad. Artech House Publishers, 2004, 268 pp., £66, ISBN 1-58053-796-0.

Ant Colony Optimization,
by Macro Dorigo and Thomas Stützle. MIT Press, 2004, 305 pp., $40.00, ISBN 0-262-02563-9.

4th Asia-Europe Workshop on Concepts in Information Theory

Jossy Sayir, Stan Baggen, Han Vinck, Joao Barros and Tony Ephremides demonstrate their musical skills.

The 4th Asia-Europe Workshop (AEW) on Concepts in Information Theory took place in Viareggio, Italy, October 6-8, 2004. The 45 participants (25 from Japan) enjoyed the beautiful surroundings and setting of this famous resort in Italy. The contributions concentrated on concepts and the authors paid great attention to the clear presentation of basic results. One of the main contributors was Prof. Jack Wolf from UCLA, USA. To honor his style of work and presentation of results, the workshop was also a tribute to him. Andrew Viterbi was present to give an impression of Jack's work and personality. A total of twenty-nine papers were presented at the workshop. The highlight of the social program of the workshop was the banquet, where a small group of participants showed their musical skills. The workshop concluded with an excursion to two famous villas near Lucca and a wine farm with tasting of the local products. The proceedings (130 pages) can be obtained from Birgit Rieth at rieth@exp-math.uni-essen.de.

Participants in the 4th Asia-Europe Workshop in Lucca, Italy.

GOLOMB'S PUZZLE COLUMN™

Countable or Uncountable Solutions

Solomon W. Golomb

In all three problems, $S = \{A_i\}$ is a collection of infinite subsets (or, infinite subsequences) A_i of the positive integers.

1. If $A_i \cap A_j = \emptyset$ whenever $i \neq j$, then S is (at most) countably infinite.

   Proof. Let M be the collection of smallest elements of all the sets A_i. Since the sets A_i are pairwise disjoint, each one contributes a *different* positive integer to M; so M is (at most) countably infinite; but the elements of M are in one-to-one correspondence with the elements A_i of S. □

2. If $A_i \cap A_j$ is finite (or empty) whenever $i \neq j$, it is possible for S to be uncountably infinite. Here is one such construction. For each real number α on the interval $(\frac{1}{2}, 1)$, write the binary expansion of α in the form $\alpha = 0.1a_2a_3a_4\ldots$, and associate with α the subsequence A_α of the positive integers consisting of $\{1, 1a_2, 1a_2a_3, 1a_2a_3a_4, \ldots\}$ where these are the binary representations of integers. (For example, $\alpha = \frac{2}{3} = 0.1010101\ldots$ is associated with the sequences $\{1, 10, 101, 1010, 10101, \ldots\}$ of integers in binary representation, or $\{1, 2, 5, 10, 21, \ldots\}$ in decimal notation.) For those real numbers with two representations, one "terminating" and one "repeating", we can use either representation; for specificity, let us use the repeating representation. (For example, $\alpha = \frac{3}{4}$ can be written as either 0.1100000... or 0.101111111.... For the former representation the sequence becomes $\{1, 3, 6, 12, 24, 48, \ldots\}$; for the latter representation, it becomes $\{1, 2, 5, 11, 23, 47, \ldots\}$. For the present construction, we can use either of these; and in fact the argument is *strengthened* if we use *both*.) Suppose $\beta \neq \alpha$ where $\beta = 0.1b_2b_3b_4b_5\ldots$ is the binary expansion of β. The *sequence* A_β has only finitely many terms in common with the sequence A_α; because, since $\alpha \neq \beta$, there is a smallest t for which $a_t \neq b_t$. Then not only $1a_2a_3\cdots a_t \neq 1b_2b_3\cdots b_t$, but all *subsequent* integers in A_α and A_β are different. Thus, $A_\alpha \cap A_\beta$ is a finite set for every $\alpha \neq \beta$, and there is such a set A_α for every α in the uncountably infinite set of real numbers in the interval $(\frac{1}{2}, 1)$. □

3. If $A_i \cap A_j$ has at most m elements whenever $i \neq j$, then S is (at most) countably infinite.

   Proof. Replace each set A_i by the finite set F_i consisting of the $m+1$ smallest elements of A_i. Then if $A_i \neq A_j$ we must have $F_i \neq F_j$, because A_i and A_j can have at most m common elements, by hypothesis. Hence there is a one-to-one correspondence between the sets A_i and the sets F_i. But the collection of *all* finite subsets of the positive integers is a countably infinite collection, and a fortiori the collection of subsets of $m+1$ elements from the set of positive integers is a countably infinite collection; so $S = \{A_i\}$ is (at most) a countably infinite collection. □

Note the similarity of the solutions given here for Problem 1 and Problem 3.

2004 International Symposium on Information Theory (ISIT)

June 27-July 2, 2004
Chicago, Illinois USA

Daniel J. Costello Jr. and Bruce Hajek, General Co-chairs

Roughly 810 information theorists attended the 2004 IEEE International Symposium on Information Theory in Chicago, Illinois, under mostly sunny skies with mild temperatures, June 27 - July 2, 2004. Attendees came from 37 countries, with the approximate numbers by country as follows:

Armenia 2
Austrailia 22
Austria 4
Belgium 4
Brazil 1
Canada 57
China 7
Czech Republic 1
Denmark 9
Finland 7
France 30
Germany 24
Greece 1
Hong Kong 3
Hungary 3
India 6
Ireland 2
Israel 27
Italy 11
Japan 29
Malawi 1
Netherlands 8
New Zealand 3
Norway 7
Portugal 1
Puerto Rico 2
Republic of Korea 21
Russian Federation 4
Singapore 6
South Africa 1
Spain 2
Sweden 15
Switzerland 39
Taiwan 7
Thailand 1
United States 463
Yugoslavia 1

There were 949 papers submitted for presentation, and 570, or about 60%, were accepted. On Wednesday afternoon, about 80 participants attended the Chicago Cubs baseball game and about 45 participants took the Chicago City tour. About 810 people attended the Thursday night banquet at Chicago's Navy Pier with entertainment by Chicago's Second City Comedy club.

Stormy weather forced the Sunday evening welcoming reception to be moved indoors, but otherwise the weather throughout the week was pleasant.

Robert J. McEliece delivered a lively Shannon lecture entitled, "Are there Turbo-Codes on Mars?" The lecture included a rousing song of thank you to Claude Shannon, accompanied by Marvin Simon on piano. See the lyrics, and also a list of anagrams devised by Dr. McEliece, at the end of this article.

Engaging lectures were also given by the other four plenary lecturers:

- Persi Diaconis (*The Mathematics of Making a Mess*),
- Ueli Maurer (*Information Theory in Cryptography*)
- Tom Richardson (*The Methods of Iterative Methods*), and
- Martin Vetterli (*On Fourier and Wavelets: Representation, Approximation and Compression*.)

The four preconference tutorials drew a total of 307 attendees. The presenters and topics were:

- Ueli Maurer, Cryptography
- Brendan Frey, Iterative Algorithms with Applications in Sensory Processing, Multiple Sequence Analysis and Machine Learning
- Giuseppe Caire, Hesham El Gamal, and Mohamed Oussama Damen, Space-Time Coding
- Gilles Brassard, Quantum Information Processing

President Hideki Imai presided over the Society's annual awards luncheon on Tuesday, and delivered an excellent speech at the banquet.

The dedication of so many volunteers and several professionals helped the conference run smoothly without any major glitches. Beside the Organizing Committee, Program Committee, speakers, and attendees, we would like to acknowledge in particular: University of Toronto student Aaron Meyers for providing an excellent paper submission and handling system, Karen Galuchie of IEEE for processing many travel grants with diligence, the Downtown Chicago Marriott staff for reliable and friendly support, and Conference Management Services, Incorporated (on the web at www.cmsworldwide.com), run by Billene Mercer, for excellent professional support with registration and publications. We encourage future IT Society workshop and symposium organizers to contact Billene about supporting a meeting anywhere in the world.

Some Information -Theoretic Anagrams

by Robert J. McEliece

- A Sound Channel
- Brainy Coed
- Rome Noodles
- Cubed Roots
- UCLA Shenanigans
- Coordinate Spasm
- Momentary Mixup
- Acquiescent Yelp

Robert J. McEliece's Shannon Lecture Song

Music and Original lyrics by Leslie Bricusse
Additional Lyrics by Bob McEliece

On behalf of everyone who has assembled here
I would merely like to mention -- if I may

That our unanimous attitude is one of lasting gratitude
For what Dr. S. has done for us today
And therefore I would simply like to say:

Thank you very much
Thank you very much
For the nicest theorems that anyone's ever proved to me
When you came our way
It was our lucky day
You taught us all about the sum of p log p
Now we calculate the mutual info
To measure X and Y's dependency
So every individual bit
Will be quite accurate
Thank you very, very, very much

Thank you very much
Thank you very much
For the nicest theorems that anyone's ever proved to me
Before you came along
Our messages went wrong
We didn't know a thing about capacity.
Now we maximize the mutual info
To minimize the probability
That any individual bit
Will be inaccurate
Thank you very, very, very, much

Thank you very much
Thank you very much
For the nicest theorems that anyone's ever proved to me
Before you came along
Our files were far too long
We could not eliminate redundancy.
Now we minimize the mutual info
To maximize compressibility
And every individual bit
is still quite accurate
Thank you very, very, very much
Thank you very, very, very much!

Call for Papers

Joint special issue of the IEEE TRANSACTIONS ON INFORMATION THEORY and the IEEE/ACM TRANSACTIONS ON NETWORKING

Networking and Information Theory

A joint issue of the IEEE TRANSACTIONS ON INFORMATION THEORY and the IEEE/ACM TRANSACTIONS ON NETWORKING will be devoted to the connections between networking and information theory. Original research papers that make major contributions to research on information theoretic aspects of networking, operations of networks and other related problems with an information theoretic components are sought.

While connections between networking and information theory have always been promising, recent developments point to especially fruitful common ground between these two areas. On the networking side, the complexity of physical layer issues, particularly in wireless networks, has prompted an inter-layer approach that fits well in the context of information theory. On the information-theoretic side, classical approaches to multiuser information theory have been enhanced by an active interest in casting practical networking problems in an information-theoretic setting. In particular, theoretical developments in information theory have drastically changed the angle of attack on information theoretic problems of networking.

Examples of such intersection areas are scaling laws in networks, network coding, implementation and theory of multiuser systems, wireless network design involving multi-input multi-output channels, and queueing and delay issues in information-theoretic capacity settings. A special issue that focuses on these activities and gives an overview of related efforts would serve both the networking and information theory communities and, we hope, deepen interest in interdisciplinary work.

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

- Network coding
- Limit behavior of large networks
- Multi-terminal information theory for networks
- Information theory for queueing and network delay
- Coding for network robustness and reliability

Prospective authors should follow the regular guidelines of the IEEE TRANSACTIONS ON INFORMATION THEORY. Further information and submission details can be found at:

`http:www.special-issue-it-ton.info`

Guest Editors

N. Cai, University of Bielefeld
M. Chiang, Princeton University
M. Effros, Caltech
R. Koetter, University of Illinois Urbana-Champaign
M. Medard, Massachusetts Institute of Technology
B. Prabakhar, Stanford University
R. Srikant, University of Illinois Urbana-Champaign
D. Towsley, University of Massachusetts
R. W. Yeung, The Chinese University of Hong Kong

Schedule

Submission deadline: Feb. 15, 2005
Selection of papers: Dec. 15, 2005
Publication: June, 2006

Call for Papers
IEEE Information Theory Workshop
on
CODING AND COMPLEXITY
(ITW2005)

http://www.cs.auckland.ac.nz/itw2005

August 29 – 1 September 2005, The Royal Lakeside Novotel, Rotorua, New Zealand

Organising Committee

M. Titchener (chair), Auckland, NZ
U. Speidel, Auckland, NZ
M. Dinneen, Auckland, NZ
P. Barry, Auckland, NZ
K. Sweeby, Auckland, NZ
R. Ehmann, Auckland, NZ

Programme Committee

D. Taylor (co-chair), University of Canterbury, NZ
U. Speidel (co-chair), University of Auckland, NZ
T. Aulin, Chalmers University, Sweden
M. Bossert, University of Ulm, Germany
C. S. Calude, University of Auckland, NZ
B. Downey, Victoria University of Wellington, NZ
M. Effros, Caltech, USA
M. Fossorier, University of Hawaii, USA
A. Grant, University of South Australia
A. Gulliver, Victoria University, Canada
P. Harremoës, University of Copenhagen, Denmark
R. Johannesson, Lund University, Sweden
T. Kløve, University of Bergen, Norway
I. Kontoyiannis, Brown University, USA
B. Mills, Massey University, NZ
G. Shamir, University of Utah, USA
L. Staiger, University of Halle, Germany
N. Suehiro, University of Tsukuba, Japan
H. Takahashi, Tokyo Inst. of Technology, Japan
M. Titchener, University of Auckland, NZ
A. J. H. Vinck, University of Essen-Duisburg, Germany
T. Wadayama, Okayama Prefectural University, Japan

Important Dates

Submissions Due:	31 January 2005
Notification:	29 April 2005
Final Copies Due:	27 May 2005

The workshop is organised by the University of Auckland on behalf of the IEEE Information Theory Society (ITSOC). Original papers are solicited on aspects of coding and complexity and their relationship and related areas. Topics of interest include but are not necessarily limited to:

Algorithmic information theory; channel coding; coded modulation; complexity, information and entropy; complexity measures; convolutional coding; error-correcting codes; information theory and statistics; iterative decoding; LDPC codes; quantum information theory; quantum-theoretical aspects of coding; randomness and pseudo-randomness; relationships between codes and complexity; rate distortion theory; soft-decision decoding; source coding; source-channel coding; spreading sequences and CDMA; turbo codes.

Authors are invited to submit papers electronically via the workshop home page (`http://www.cs.auckland.ac.nz/itw2005`).

Invited Speaker: Péter Gács (Computer Science Department, Boston University)

Location: Located at the southern shores of the lake that shares its name, Rotorua is New Zealand's geothermal wonderland and famous for its indigeneous Maori culture. Its hot springs, geysers and other colourful volcanic features have made it a popular destination with tourists for over a century. At the time of the workshop, the steam from the geothermal areas all over town should be at its most spectacular. Rotorua also boasts a wide variety of attractions for the entire family, ranging from various natural hot pools via lake cruises, parks and cultural shows to historic buildings and tours of Rotorua's exciting environs. Keep an eye on the local activities page for the chair's favourites.

Rotorua is well connected by road and air, with Auckland being the nearest large international airport.

The conference venue, the Royal Lakeside Novotel, is located right at the lakefront and within easy walking distance of many of Rotorua's downtown attractions.

The workshop will be held in the week prior to ISIT2005 in Adelaide, Australia, and participation in both events is explicitly encouraged.

Additional Information: See the workshop home page `http://www.cs.auckland.ac.nz/itw2005` or email the conference co-chair Ulrich Speidel (`ulrich@cs.auckland.ac.nz`).

CALL FOR PAPERS

2005 IEEE International Symposium on Information Theory

Adelaide Convention Centre, Adelaide, Australia

September 4 – 9, 2005

The 2005 IEEE International Symposium on Information Theory will be held at the Adelaide Convention Centre in Adelaide, Australia from Sunday, September 4 through Friday September 9, 2005.

Previously unpublished contributions to the following areas will be solicited:

Coded modulation
Information theory and statistics

Coding theory and practice
Multiuser detection

Communication complexity
Multiuser information theory

Communication systems
Pattern recognition and learning

Cryptology and data security
Quantum information processing

Data compression
Shannon theory

Data networks
Signal processing

Detection and estimation
Source coding

Papers will be reviewed on the basis of a manuscript (not exceeding five pages) of sufficient detail to permit reasonable evaluation. The deadline for submission is **January 30, 2005**, with notification of decisions by May 15, 2005. The deadline will be strictly enforced. In view of the large number of submissions expected, multiple submissions by the same author will receive especially stringent scrutiny. All accepted papers will be allowed twenty minutes for presentation, and will be published in full (up to five pages). Authors are strongly encouraged to submit electronic versions of their extended abstracts in the form of Portable Document Format (PDF) files.

Detailed information on paper submission, technical program, accommodation, travel, and excursions will be posted on the Symposium web site

`http://www.isit2005.org`

Inquiries on general matters related to the Symposium should be directed to

Prof. Alex Grant
Prof. Rodney A. Kennedy

Institute for
Telecommunications Research
Research School of Information Sciences and Engineering

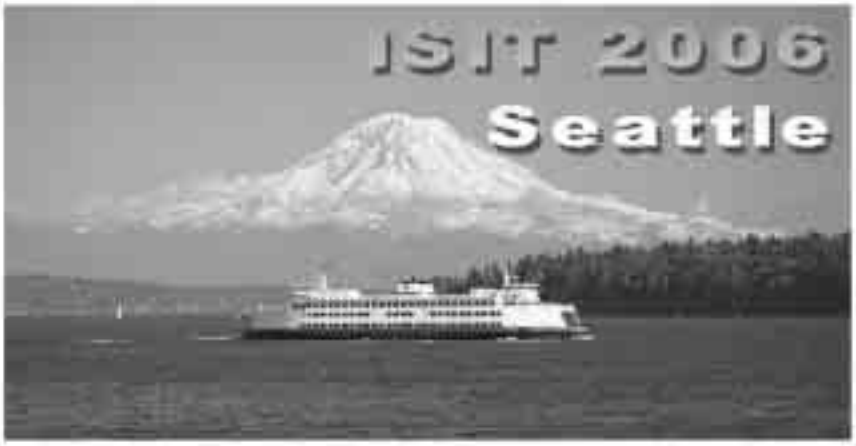
University of South Australia
Australian National University

SA 5095 Australia
ACT 0200 Australia

alex.grant@unisa.edu.au
rodney.kennedy@anu.edu.au

Editor's Note: Please notice that the ISIT 2005 proceedings will include 5 page papers rather than one page abstracts. Further information about this change will appear in a future issue of the Newsletter.

Conference Announcement



2006 IEEE International Symposium on Information Theory

Sheraton Hotel and Towers, Seattle, Washington
July 9 – July 14, 2006

The 2006 IEEE International Symposium on Information Theory will be held at the Sheraton Hotel and Towers in Seattle, Washington from Sunday July 9 through Friday July 14, 2006. Seattle is conveniently located on the west coast, making it easily accessible from everywhere in North America and from Asia. This thriving city offers a range of cultural activities. Mountains, Olympic Peninsula, Puget Sound, and Lake Washington offer inspiring recreational opportunities.

Previously unpublished contributions to the following areas will be solicited:

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

Papers will be reviewed on the basis of an extended abstract of sufficient detail to permit reasonable evaluation. In addition to new results in areas that form the core of information theory, efforts will be made to encourage participation by researchers in related fields and researchers working on novel applications of information theory.

Detailed information on paper submission, technical program, accommodation, tutorials, travel, and excursions will be posted on the Symposium web site:
`http://www.isit2006.org`

http://www.isit2006.org

General co-chairs:
Joseph A. O'Sullivan,
Washington University
John B. Anderson,
Lund University

Program co-chairs:
Alexander Barg,
University of Maryland
Raymond W. Yeung,
The Chinese University of Hong Kong

Local arrangements chair:
Radha Poovendran,
University of Washington

General vice chair:
Anthony Ephremides,
University of Maryland

Treasurer:
Amer Hassan, Microsoft

Direct inquiries to either:

Radha Poovendran
434 EE1
Box 352500
University of Washington
Seattle, WA 98195-2500
radha@ee.washington.edu

Joseph A. O'Sullivan
One Brookings Dr
Campus Box 1127
Washington University
St. Louis, MO 63130
jao@wustl.edu

Los Alamos National Laboratory Workshop
on Applications of Statistical Physics to Coding Theory

Santa Fe, New Mexico
January 10-12, 2005

Call for Participation

The LANL Workshop on Applications of Statistical Physics to Coding Theory will take place on January 10-12 in Santa Fe, New Mexico, and will be an excellent venue with outstanding speakers and high-quality technical content. It is sponsored by the Center for Nonlinear Studies (CNLS) at Los Alamos National Laboratory. The program consists of plenary sessions with invited presentations and provides plenty of time for discussion.
More information on the workshop agenda can be found at

http://cnls.lanl.gov/~chertkov/FEC.htm

Interested attendees are invited to register through automatic registration system provided at the website. The number of seats in the hotel conference room is going to be limited to 50-60 participants.

The Organizing Committee:
Misha Chertkov (LANL)
Ildar Gabitov (LANL & University of Arizona, Department of Mathematics)
Bane Vasic (University of Arizona, Department of ECE and Department of Mathematics)

CALL FOR PAPERS AND FIRST ANNOUNCEMENT

Fourth International Workshop on Optimal Codes and related topics – OC 2005

Programme Committee	Stefan Dodunekov (Sofia), Tor Helleseth (Bergen) Ivan Landjev (Sofia), Jurriaan Simonis (Delft) Leo Storme (Gent), Henk van Tilborg (Eindhoven)
Organizing Committee	Silvia Bouyuklieva (Sofia), Peter Boyvalenkov (Sofia) Emil Kolev (Sofia), Ivan Landjev (Sofia), Nikolay Manev (Sofia)
Local Organizer	Institute of Mathematics and Informatics, Bulgarian Academy of Sciences
Topics	• Optimal linear codes over finite fields and rings; • Bounds for codes; • Spherical codes and designs; • Covering problems for linear and nonlinear codes; • Optimization problems for nonlinear codes; • Sets of points in finite geometries; • Combinatorial configurations and codes; • Optimality problems in cryptography; • Graph theory and codes; • Related topics
Time	**June 17 – 23, 2005**
Location	The Workshop will take place at Hotel Snejanka (http://www.pmk-bg.com/index.php?p=snejanka, in Bulgarian), Pamporovo, Bulgaria. Pamporovo is the smallest winter resort in Bulgaria and is located at 220 km from Sofia and 85 km south from Plovdiv. There are good bus connections to Sofia and Plovdiv. Hotel Snejanka offers nice accommodation and conference facilities. More information from the organizers at oc2005@moi.math.bas.bg.
Registration Fee (includes accommodation in hotel "Snejanka", full board, social events, workshop proceedings and materials)	EURO 450 prior to May 16, 2005; EURO 500 after May 16, 2005; EURO 350 for students prior to May 16, 2005; EURO 300 for spouses.
Deadlines	**March 31, 2005:** to inform the organizers if you intend to come; **April 15, 2005:** Deadline for submission of papers; **May 1, 2005:** Notification of acceptance (to be mailed out).
Language	The official language of the Workshop will be English.
Proceedings	The organizers intend to prepare a book of proceedings of the workshop. Authors are invited to submit at most six pages camera-ready papers in English, LaTeX format 132×190 mm, by e-mail to oc2005@moi.math.bas.bg.
More information	Visit our web site http://www.moi.math.bas.bg/oc2005/oc2005.html.

CALL FOR PAPERS

THE 2005 CANADIAN WORKSHOP ON INFORMATION THEORY

MONTRÉAL, QUÉBEC

JUNE 5 – JUNE 8, 2005

The 9th Canadian Workshop on Information Theory will be held at McGill University in Montréal, Québec, from Sunday evening, June 5 through Wednesday, June 8, 2005. This workshop provides an opportunity for Canadian as well as international researchers in Information Theory to meet and discuss aspects of their work.

Papers presenting new results in (but not limited to) the following areas are solicited:

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

Papers will be reviewed on the basis of a two-page summary. All summaries should be submitted through the EDAS online submission system (http://edas.info/) and include the authors' names, complete mailing addresses, telephone/fax numbers and e-mail addresses (as applicable). Electronic submission of Microsoft Word, Postscript or PDF files is encouraged.

The deadline for submission of a two-page extended abstract is at noon (EST) of **February 14, 2005**. Acceptance will be announced in the **middle of March 2005**. Authors of papers accepted for the workshop will be requested to submit a four page camera-ready paper no later than **April 20, 2005**. The workshop starts on **June 5, 2005**.

Correspondence regarding the workshop should be addressed to one of the co-chairs:

Dr. Paul Fortier
Faculty of Science and Engineering
Université Laval
Sainte-Foy, Québec, G1K 7P4
Tel: (418) 656-7368
Fax: (418) 656-5903
Email: *paul.fortier@fsg.ulaval.ca*

Dr. Jan Bajcsy
Electrical & Computer Engineering Dept.
McGill University, 3480 University St.
Montréal, Québec, H3A 2A7
Tel: (514) 398-7462
Fax: (514) 398-4470
Email: *jbajcsy@ece.mcgill.ca*

For further information on this Workshop, please visit our web page at:

http://www.ece.mcgill.ca/~cwit2005

Sponsored by *The Canadian Society for Information Theory*.

Call for Papers

10th International OFDM-Workshop 2005 (InOWo'05)

31. August - 1. September 2005
Hotel Atlantic, Hamburg, Germany

The 10th International OFDM-Workshop (InOWo'05) is comming back to the beautifull city of Hamburg, Germany, and is held from Wednesday, 31. August through Thursday, 31. September 2005. The Workshop provides an opportunity for international researchers interested in all aspects of the OFDM transmission technique to meet and discuss current results of their research work. In addition to the two day conference a half-day tutorial on various aspects of the OFDM transmission technique is planned for the 30. August 2005.

Paper submissions for technical sessions may cover all aspects of multi-carrier transmission including any of the following areas (but not limited to):

Signal Processing in OFDM Systems:
- Modulation Techniques
- Equalisation and Synchronisation
- Channel Coding
- Non-Linearities
- Multiple Access Techniques

OFDM System Concepts:
- Crosslayer Optimisation
- 4th Generation Networks
- Hiperlan/2 and IEEE 802.11a
- DLC-Protocol Issues
- Ad-Hoc Networking
- XDSL

MIMO with OFDM:
- Antenna Techniques
- MIMO Coding
- Multi User Systems and MIMO

Experimental Systems and Field Trials:
- Implementation Issues
- VLSI Architectures
- Software Defined Radio for OFDM

Authors are invited to submit a one-page extended abstract, including the authors' full contact information, to the Workshop e-mail address ofdm@tu-harburg.de.

Important Dates

Deadline for Extended Abstracts:	April 17, 2005
Notification of Acceptance:	May 29, 2005
Early Registration:	July 17, 2005
Final Papers Due:	July 17, 2005

For further information about this Workshop, as well as detailed instruction for submitting the final paper, please visit our web page at:

http://ofdm.tu-harburg.de/

Conference Chair

Prof. Hermann Rohling
Department of Telecommunications
Technical University Hamburg-Harburg
Eissendorfer Strasse 40
21073 Hamburg, Germany
Phone: +49 (0)40 – 42878 – 3028
E-Mail: rohling@tu-harburg.de

OFDM-Workshop Organizers

Christian Stimming, Nico Tönder
Department of Telecommunications
Technical University Hamburg-Harburg
Phone: +49 (0)40 – 42878 – 2164/2168
Fax: +49 (0)40 – 42878 – 2281
E-Mail: ofdm@tu-harburg.de
http://ofdm.tu-harburg.de

Conference Calendar

DATE	CONFERENCE	LOCATION	CONTACT/INFORMATION	DUE DATE
January 10-12, 2005	**LANL Workshop on Applications of Statistical Physics to Coding Theory**	Santa Fe, New Mexico	http://cnls.lanl.gov/~chertkov/FEC.htm See CFP in this issue	TBA
April 3-7, 2005	**WiOpt 2005**	Trento, Italy	http://www.wiopt.org/	October 5, 2004
June 5-8, 2005	**Canadian Workshop on Information Theory (CWIT) 2005**	Monteal, Quebec	http://www.ece.mcgill.ca/~cwit2005 See CFP in this issue	February 14, 2005
June 17-23, 2005	**Four International Workshop on Optimal Codes and Related Topics 2005**	Pamporovo, Bulgaria	http://www.moi.math.bas.bg/oc2005/oc2005.html See CFP in this issue	March 31, 2005
August 29 - September 1, 2005	**2005 Information Theory Workshop (ITW)**	The Royal Lakeside Novotel Rotorua, New Zealand	http://www.cs.auckland.ac.nz/itw2005 See CFP in this issue	January 31, 2005
Aug. 31 - Sept. 1	**InOWo'05 - 10th International OFDM Workshop 2005**	Hamburg, Germany	http://ofdm.tu-harburg.de See CFP in this issue	April 17, 2005
September 4-9, 2005	**2005 IEEE International Symposium on Information Theory (ISIT)**	Adelaide Convention Center Adelaide, AUSTRALIA	See CFP in this issue. http://www.isit2005.org Dr. Alex Grant Institute for Telecommunications Research University of South Australia SA 5095 Australia Prof. Rodney A. Kennedy Research School of Information Sciences and Engineering Australian National University ACT 0200 Australia rodney.kennedy@anu.edu.au	January 30, 2005
April 3-7, 2006	**4th International Symposium on Turbo Codes and Related Topics**	Munich, Germany	http://www-turbo.enst-bretagne,fr/	Oct. 15, 2005
TBA	**2006 IEEE International Symposium on Information Theory (ISIT)**	Seattle, Washington, USA	TBA	TBA