IEEE Information Theory Society Newsletter

Vol. 58, No. 2, June 2008

Editor: Daniela Tuninetti

ISSN 1059-2362

President's Column

David Forney

I dare say that there is no other IEEE society that is a more purely volunteer society than the Information Theory Society. Our society has no staff, and is basically run out of the back pockets of a large number of dedicated and highly responsible volunteers. Moreover, I believe that there is no other IEEE society in which the principal volunteers are so often the principal technical contributors to its field.

The IT Society has no Executive Committee, but the officers of the society form a tight-knit collaborative group who are in continual contact and serve somewhat as an executive com-

mittee. I wish to express here my deep gratitude to last year's officers–Steve McLaughlin, Dave Neuhoff, Marc Fossorier, Andrea Goldsmith, and above all Bixio Rimoldi–who helped me enormously in making a smooth transition to my new role. This year Frank Kschischang has started his climb up the officer pyramid. Other officers are Anant Sahai, Treasurer and João Barros, Secretary.

The volunteers who probably spend the most time on society affairs are the editors of the IT Transactions, led by Ezio Biglieri, Editor-in-Chief. The EiC must not only maintain the quality of the Transactions through his astute choice of effective Associate Editors, but is also responsible for the operational and financial aspects of our Transactions. In this the EiC is strongly assisted by Publications Editors Elza Erkip and Adriaan van Wijngaarden. The quality, timeliness, and financial condition of our Transactions remain superb, but Ezio is pushing hard for improvements in our submission-topublication time, where we continue to lag.

The EiC also chairs the Publications Committee, which formulates policy for the Transactions and other publications. This committee has recently agreed that there is no good reason to continue to make a sharp distinction between Correspondence and regular papers, and has therefore recommended that the Correspondence section of the Transactions be phased out. It has also recommended discontinuing print publication of the annual Transactions index, which has been



superseded to a great extent by electronic tools; the index will still be available on-line.

Daniela Tuninetti, the Newsletter Editor, puts out this publication more or less single-handedly. She is responsible for obtaining a steady stream of interesting contributions, including the regular columns of our Historian, Tony Ephremides, and our Puzzle Master, Sol Golomb.

Beyond publications, the next largest activity of our society is our program of conferences and workshops. The Conference Committee

is chaired by Alex Grant, and includes João Barros, Dan Costello, Tony Ephremides, Bruce Hajek, and Anant Sahai. The committee is responsible for stimulating, evaluating and guiding conference proposals. Our next four ISITs seem to be well in hand: Toronto (2008), Seoul (2009), Austin (2010), and St. Petersburg (2011). However, after the Information Theory Workshop in Porto in May 2008, no further ITWs have been approved at this time. Proposals for ITWs of either the focussed topic type or the geographical outreach type are most welcome.

It is not possible to mention here the names of all those who take responsibility for all aspects of our conferences, from their overall organization to their technical and social programs. In my experience this is something that everyone should do at least once (but perhaps only once). The results are almost always very gratifying.

Another activity that the IT Society takes very seriously is its modest awards program. The Awards Committee is chaired by Andrea Goldsmith, and includes Ning Cai, Rob Calderbank, Anne Canteaut, Suhas Diggavi, Tuvi Etzion, Michael Honig, Ioannis Kontoyiannis, Frank Kschischang, Upamanyu Madhow, and Andreas Winter. It oversees the IT Society Paper Award, the IT/ComSoc Joint Paper Award, and the ISIT Student Paper Award. Separate committees chaired by the President are responsible for the Shannon Award (Dick

continued on page 4



From the Editor

Dear IT society members,

Spring has timidly arrived in Chicago after a cold and long winter. The semester is almost over and I am now making plans for summer and for ISIT in Toronto, where I hope to see you all. In the meantime, I hope you will enjoy this issue of the newsletter, featuring the regular columns by our President Dave Forney, our Historian Anthony Ephremides, our creative Puzzle Master Sol Golomb, NSF Program Manager Sirin Tekinay, the latest calls for papers, and the conference calendar.

In addition, you will find an interesting article by Yiannis Kontoiannins about how to use entropy to count prime numbers. You will be surprised to see how easy, and yet powerful, the idea is. I hope you will also enjoy the reports on the 3rd Information Theory and Application Workshop held at UCSD in San Diego in January, and the 14th Workshop on Information Theory in December last year in Guangzhou, China.

Before concluding this column, I sadly remark the passing away of Adam Rybowicz on February 11, 2008. Adam was the husband of Ms. Nela Rybowicz, Senior

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.

© 2008 IEEE. Information contained in this newsletter may be copied without permission provided that the copies are not made or distributed for direct commercial advantage, and the title of the publication and its date appear.

IEEE Information Theory Society Newsletter

Editor of the IEEE Transactions on Information Theory. Nela has been editing our Transactions since January 1995, and has been with IEEE publications for 35 years. Nela's passionate and meticulous work has contributed to the outstanding quality of our Transactions. We offer our sincere condolences to Nela and

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

Issue September 2008 December 2008 March 2009 June 2009

her son Joey.

July 10, 2008 October 10, 2008 January 10, 2009 April 10, 2009

Deadline

Electronic submission in Ascii, LaTeX and Word formats is encouraged. Potential authors should not worry about layout and fonts of their contributions. Our IEEE professionals take care of formatting the source files according to the IEEE Newsletter style. Electronic photos and graphs should be in high resolution and sent in as separate file.

Daniela Tuninetti

I may be reached at the following address:

Daniela Tuninetti Department of Electrical and Computer Engineering University of Illinois at Chicago, E-mail: daniela@ece.uic.edu

> See you in Toronto, Daniela Tuninetti

Table of Contents

President's Column	1
From the Editor	2
The Historian's Column	3
Golomb's Puzzle Column: Graceful Graphs	5
Counting Primes Using Entropy	6
Latest Activities of the IT Students	9
Workshop Report: 3rd Information Theory and Application	10
The 2007 Chinese Workshop on Information Theory	11
Golomb's Puzzle Column: Divisibilities in Numerical Triangle Solutions	12
Guest Column: News from National Science Foundation	13
Call for Papers	14
Conference Calendar	16



The Historian's Column

Anthony Ephremides

The alert readers will recall that I have paid tribute to the Society's Newsletter of yore, when the wit of Information Theorists was in abundant, almost exhibitionist, display.

I would like to revisit some of these early pages and extract some gems for the benefit of our younger readers. The editor at the time (we are talking early seventies, when many of our members were still in the ... crib) was Lalit Bahl, who had an irrepressible desire to mix some fun into life's cocktail. So he used to run a competition that shifted emphasis among different tasks at each issue.

The "kick-off" competition, also known as Competition No. 1, asked readers to invent fanciful definitions for technical terms. All entries received "honorable mention" and two of them were declared the winners. What is impressive was the intensity of participation by two of our most esteemed and venerable members, Marty Hellman and Tom Cover. Perhaps being at Stanford at the time provided additional inspiration. So here are the winning entries from Marty:

- "union bound": engaged couple,
- "transversal equalizer": gay affirmative action,
- "white noise": Ku Klux Klan.

And here is the winning entry from Tom:

- "Lim Sup": a stew of appendages.

Not to flatter Tom, but I would have given him the grand prize for this one. But do you think this was all? Here are additional entries from Marty:

- "cross talk": religious mass,
- "ensemble average": mediocre singing group,
- "tree code": department of agriculture regulation,
- "parity check": physical exam for a green talking bird,
- "wideband modulation": obese musician's modern dance,
- "envelope detector": FBI.

Clearly he was on a roll! But Tom was not far behind; here are some more of his entries:

- "expectation": A real number that upperbounds performance,
- "error bound": a tendency to commit mistakes,
- "stationary process": dead letter department.

Just in case you might conclude that Marty and Tom were the

only entrants, here are additional samples from three different people, F. Ward, S.J. Hong, and J. Gedaugas respectively (don't ask me who they were):

- "discrete ensemble": a group of musicians who play only when asked to,



- "sin-de-Rome": alas, the corrections came too late (this one takes some thinking to appreciate),

- "preamble": baby carriage pushed by Western Union messenger (question: how many know what Western Union was?)

Being certain that you have had enough of this, let me turn now to a contribution by Neil Sloane, who was the Editor-in-Chief of the Transactions during the late seventies. He sampled from a column by William Safire (who, although retired, still writes columns on language use). This one was from the New York Times Magazine issue of November 4, 1929 (you can check and verify through a perpetual calendar that this was a Sunday). It concerned examples of bad writing, some of which are, regrettably, present even in this column. It might be called "The relentless attraction of the tendency to err".

- No sentence fragments
- Avoid commas, that are not necessary
- A writer must not shift your point of view
- And don't start a sentence with a conjunction
- Don't overuse exclamation marks!!
- Avoid un-necessary hyphens
- Write all adverbial forms correct
- Writing carefully, dangling participles must be avoided
- Remember to never split an infinitive
- Don't use no double negatives
- Reserve the apostrophe for it's proper use
- · Verbs has to agree with their subjects
- Take the bull by the hand and avoid mixed metaphors
- Never, ever use repetitive redundancies
- Avoid overuse of " "quotation" "marks" "

• Last but not least avoid clichés like the plague and seek viable alternatives

Now that you've had enough of that too, consider the witty responses to the solicitation of unlikely titles of papers and books under competition No. 4:

- "Techniques for Factoring Large Primes with Applications to Cryptography" (due to non-other than Sol Golomb),

- "Matrix Inversion using Roman Numerals",
- "An Algorithm for Compression using Lead Weights",
- "Error-producing Codes",
- "Research on Pole Placement at the University of Warsaw",
- "Installing Mufflers on Noisy Channels".

(all by D. Pitt and M. Robinson - anyone knows them?)

- "New Results A Tutorial",
- "Estimation of Known Signals",
- "Crime-Detection Algorithms",
- (sadly, by "yours truly"!)

Ahh! Those were the days.

Correction to the March 2008 Historian's column

In my previous column I made reference to Sergio Verdu's usage of "Fleischer's Lemma" in his Shannon Lecture, which was not due to Fleischer and not even a lemma. In actuality, Sergio referred to it as "Stein's lemma". I am not sure what substitution code caused me to replace Stein with Fleischer. Nonetheless, if the non-lemma was not due to Stein, it could very well be due to Fleischer. And if, as the main point Sergio was making, it did not matter whom this result was attributed to, then it might as well be attributed to Fleischer!

President's Column continued from page 1

Blahut, Andrea Goldsmith, Frank Kschischang, Jim Massey, Sergio Verdu and Frans Willems) and Wyner Award (Tom Fuja, Andrea Goldsmith, Frank Kschischang and Bixio Rimoldi).

The IT Fellows Committee evaluates IEEE Fellow nominations and forwards their rankings to the IEEE Fellow Committee. Dan Costello chairs this important committee, which includes Bruce Hajek, Mike Honig, Vijay Kumar, Shlomo Shamai, and Frans Willems.

Frank Kschischang leads the Chapters Committee, which supports our modest chapter activities, and makes an annual Chapter of the Year award. This year we are pleased to report the re-activation of a joint chapter covering all regions of Russia.

Aylin Yener chairs a very active Student Committee, which is organizing a first annual School of Information Theory in North America in June 2008, as well as various other student activities (see their lively Web page). Other members of this committee are Ivana Maric and Brooke Shrader, Student Co-Chairs, and Lalitha Sankar, Volunteer Coordinator.

Nick Laneman, On-Line Editor, spends a lot of time not only on keeping the IT Web site current, but also on improving its look and

feel and utility. A major upgrade using the Plone content management system is underway. Nick is assisted in overseeing this project by a 17-person steering committee.

Finally, the members of many of these committees are selected and persuaded to serve by the Nominations and Appointments Committee, which is chaired by Dave Neuhoff, and includes Bruce Hajek, Prakash Narayan, Alon Orlitsky and Bixio Rimoldi. Dave and Bixio also comprise the Constitution and By-Laws Committee, which has recently completed revisions of these two governing documents.

I trust that the reader is duly impressed by the number and quality of volunteers serving in these various capacities. And I haven't even mentioned the 20 regular members of the IT Board of Governors, or the 32 Associate Editors of the IT Transactions (whose names you can find on the inside front cover of the Transactions), or the 19 ISIT 2008 organizers and 63 members of the ISIT 2008 Technical Program Committee (whose names are listed on the ISIT 2008 Web site), or various others who serve in so many different roles to keep this society humming. It is indeed very impressive. On behalf of everyone who benefits from their efforts, I wish to thank each and every one of our volunteers, from the bottom of my heart.

4

GOLOMB'S PUZZLE COLUMN™

GRACEFUL GRAPHS

Solomon W. Golomb

We consider a simple connected graph, Γ , with *n* nodes (a.k.a. *points*, or *vertices*) and *e edges* (a.k.a *lines*). We seek to assign a subset of the positive integers from 0 to e to the n nodes in such a way that the e edges get the edge labels from 1 to e, where the label on an edge is the absolute value of the difference between the node numbers at its two endpoints. (Such a numbering of the nodes of Γ is called a *graceful numbering*, and if Γ has such a numbering, Γ is called a *graceful graph*.)

ന

Here are some graceful numberings of some fairly small graphs.





(The edge labels are enclosed in circles.)

Problem 1. Find graceful numberings for each of the following graphs.



Problem 2. An Euler circuit on a connected graph Γ is a path that traverses each edge of the graph exactly once and returns to the starting point. (Nodes of the graph may be visited more than once. Of the six graphs in Problem 1, c. and e. – and no others – have Euler circuits.) Prove the following Theorem: If Γ is a graph with e edges that has an Euber circuit, then Γ cannot be graceful if $e \equiv 1 \pmod{10}$ 4) or if $e \equiv 2 \pmod{4}$.

Problem 3 As an application of the theorem in Problem 2, find the three (simple, connected) graphs on 5 nodes that have no graceful numberings.

Problem 4 The complete graph K_n is the graph with n nodes that has $e = \binom{n}{2}$ edges which connect each pair of nodes. Prove the following Theorem: For n > 4, K_n is not a graceful graph.



5

Counting Primes Using Entropy

Ioannis Kontoyiannis

Lecture given on Thursday, May 8 2008, at the 2008 IEEE Information Theory Workshop, Porto, Portugal

I. The Prime Number Theorem

Sometime before 300 BC someone showed that there are infinitely many prime numbers—we know this because a proof appears in Euclid's famous *Elements*. In modern notation, if we write $\pi(n)$ for the number of primes no greater than n, we can say that,

$$\pi(n) \to \infty, \quad \text{as } n \to \infty.$$
 (1)

Here's a proof, based on the idea of an argument of Chaitin from 1979 [6]. Let *N* be a random integer distributed uniformly in $\{1, 2, ..., n\}$, and write it in its unique prime factorization,

$$N = p_1^{X_1} \cdot p_2^{X_2} \cdots \cdot p_{\pi(n)}^{X_{\pi(n)}}, \qquad (2)$$

where $p_1, p_2, \ldots, p_{\pi(n)}$ are the primes up to n, and where each X_i is the largest power $k \ge 0$ such that p_i^k divides N. This defines a new collection of random variables $X_1, X_2, \ldots, X_{\pi(n)}$, and, since $p_i^{X_i}$ divides N, we must have,

$$2^{X_i} \le p_i^{X_i} \le N \le n,$$

or, writing log for log₂,

$$X_i \le \log n$$
, for each *i*. (3)

Now here's a cool thing:

$$log n = H(N) = H(X_1, X_2, ..., X_{\pi(n)}) \leq H(X_1) + H(X_2) + \dots + H(X_{\pi(n)}) \leq \pi(n) \log(\log n + 1).$$
(4)

The second equality comes from the uniqueness of prime factorization, that is, knowing N is the same as knowing the values of all the X_i ; the last inequality comes from (3). Therefore,

$$\pi(n) \ge \frac{\log n}{\log(\log n + 1)}, \quad \text{for all } n \ge 2,$$

which not only proves that $\pi(n) \to \infty$, but also gives a lower bound on how *fast* it grows with *n*.

This is a tiny glimpse into a very, very long story: A large portion of number theory—and a very significant portion of modern mathematics at large—is devoted to quantifying (1). For a long time we've wanted to know:

How fast, exactly, does
$$\pi(n) \to \infty$$
, as n grows?

Enter Gauss. According to Apostol [1], in 1792, while inspecting tables of prime numbers, Gauss conjectured what has come to be known as the celebrated *prime number theorem*, namely that,

$$\pi(n) \sim \frac{n}{\log_e n}, \quad \text{as } n \to \infty,$$
 (5)

where $a_n \sim b_n$ means that $a_n/b_n \rightarrow 1$ as $n \rightarrow \infty$. Apparently he was not able to prove it, and not because he was only 15 years old at the time—he kept trying, without success, for quite a while, and only disclosed his conjecture in a mathematical letter to Encke, over 50 years later.

In fact Gauss (still at 15) suggested that, for finite n, $\pi(n)$ is better approximated by the function,

$$\operatorname{Li}(n) = \int_2^n \frac{dt}{\log_e t}$$

sometimes called the *Eulerian logarithmic integral*. Since Li(n) asymptotically varies like $n/\log_e n$, the prime number theorem, henceforth PNT, can also be written,

$$\pi(n) \sim \operatorname{Li}(n), \text{ as } n \to \infty.$$

If you're not yet convinced that we should care all that much about how $\pi(n)$ behaves for large n, this should do it: Arguably the most important problem in mathematics today, the Riemann hypothesis, is equivalent to the following refined version of the PNT: For every $\epsilon > 0$,

$$\pi(n) = \operatorname{Li}(n) + O\left(n^{\frac{1}{2} + \epsilon}\right).$$

See [2] for more of the history and details.

II. Chebyshev's Attempt

The PNT was proved a little more than 100 years after Gauss conjectured it, but before talking about proofs (and attempted proofs), let's note that according to the PNT (5) our earlier estimate (3) was pretty loose. Can we do better?

Interestingly, a small modification of our basic argument in (4) gives a slightly better bound. Suppose that, instead of the usual prime factorization, we express N as,

$$N = M^2 \cdot p_1^{Y_1} \cdot p_2^{Y_2} \cdots \cdot p_{\pi(n)}^{Y_{\pi(n)}},$$
(6)

where $M \ge 1$ is the largest integer such that M^2 divides N, and the Y_i are now binary. Since M^2 divides N, we must have

 $M^2 \le N \le n$, or $M \le \sqrt{n}$, and noting that the representation (6) is also unique, arguing as before we get,

$$log n = H(N) = H(M, Y_1, Y_2, ..., Y_{\pi(n)}) \leq H(M) + H(Y_1) + H(Y_2) + \dots + H(Y_{\pi(n)}) \leq \frac{1}{2} \log n + \pi(n),$$

which implies that $\pi(n) \ge \frac{1}{2} \log n$, for all $n \ge 2$. This is better than (3) but still pretty far from the optimal rate in (5).

I don't know how (or if it is possible) to twist this argument around further to get more accurate estimates, so let's get back to the classical proofs of the PNT. Another early player in this drama is Chebyshev (the one of the inequality), who also gave the PNT a go and, although he didn't succeed in producing a complete proof, he discovered a number of beautiful results along the way. One of them is the following unexpected asymptotic formula:

Theorem 1. Chebyshev (1852) [7], [8]

As $n \to \infty$,

$$C(n) \triangleq \sum_{p \le n} \frac{\log p}{p} \sim \log n$$

where the sum is over all primes p not exceeding n.

Actually Chebyshev came pretty close to proving the PNT. For example, using Theorem 1 in a slightly refined form, he was able to find explicit constants constants A < 1 < B and n_0 such that:

$$A\frac{n}{\log_e n} \le \pi(n) \le B\frac{n}{\log_e n}$$
, for all $n \ge n_0$.

The PNT was finally proved in 1896 by Hadamard and, independently and almost simultaneously, by de la Vallée-Pousin. Both proofs were mathematically "heavy," relying on the use of Hadamard's theory of integral functions applied to the Riemann zeta function $\zeta(s)$; see [2] for details. In fact, for quite some time it was believed that no elementary proof would ever be found, and G.H. Hardy in a famous lecture to the Mathematical Society of Copenhagen in 1921 [5] went as far as to suggest that "*if anyone produces an elementary proof of the PNT* … *he will show that* … *it is time for the books to be cast aside and for the theory to be rewritten.*"

The announcement by Selberg and Erdös in 1948 that they had actually found such an elementary proof came as a big surprise to the mathematical world and caused quite a sensation; see [10] for a survey. What's particularly interesting for us, is that Chebyshev's result in Theorem 1 was used explicitly in their proof.

Thus motivated, we now discuss an elegant way to prove Theorem 1 using only elementary ideas from information theory and basic probability.

III. Entropy

Apparently the first person to connect prime-counting questions with information-theoretic ideas and methods is Patrick Billingsley. In 1973 he was invited to deliver the prestigious "Wald Memorial Lectures" at the IMS Annual Meeting in New York. Billingsley, a probabilist, has long been involved with entropy and information—and wrote a book [3] about it—and in the years before these lectures it appears he had developed a strong interest in "probabilistic number theory," that is, in the application of probabilistic techniques to derive results in number theory. In the transcript [4] of his 1973 lectures he describes a beautiful heuristic argument for proving Theorem 1 using simple computations in terms of the entropy. It goes like this.

Start as before with a random integer *N* uniformly distributed between 1 and some fixed $n \ge 2$, and write it in its unique prime factorization (2). What is the distribution of the induced random variables X_i ? Let's first look at one of them. Since the number of multiples of p_i^k between 1 and *n* is exactly $\lfloor n/p_i^k \rfloor$, we have,

$$\Pr\{X_i \ge k\} = \Pr\left\{N \text{ is a multiple of } p_i^k\right\} = \frac{1}{n} \left\lfloor \frac{n}{p_i^k} \right\rfloor.$$
(7)

Therefore, for large *n*,

$$\Pr\{X_i \ge k\} \approx \left(\frac{1}{p_i}\right)^k$$

i.e., the distribution of each X_i is approximately geometric with parameter $1/p_i$. Similarly, since the number of multiples of $p_i^k p_j^\ell$ between 1 and n is $\lfloor n/p_i^k p_j^\ell \rfloor$, for the joint distribution of X_i , X_j we find,

$$\Pr\{X_i \ge k, \ X_j \ge \ell\} = \frac{1}{n} \left\lfloor \frac{n}{p_i^k p_j^\ell} \right\rfloor \approx \left(\frac{1}{p_i}\right)^k \left(\frac{1}{p_j}\right)^\ell,$$

so X_i and X_j are approximately independent. The same argument works for any finite sub-collection of the $\{X_i\}$. This intuition, that we can think of the $\{X_i\}$ as approximately independent geometrics, was well known for at least a few decades before Billingsley's lectures; see, e.g., Kac's classic gem [11].

Billingsley's insight was to bring the entropy into play. Combining the initial steps of our basic argument (4) with the observation that the X_i are approximately independent geometrics,

$$\log n = H(N)$$

$$= H(X_1, X_2, \dots, X_{\pi(n)})$$

$$\approx \sum_{i=1}^{\pi(n)} H(X_i)$$
(8)

$$\approx \sum_{p \le n} \left[\frac{\log p}{p-1} - \log \left(1 - \frac{1}{p} \right) \right], \tag{9}$$

where in the last step we simply substituted the well-known [9] formula for the entropy of a geometric with parameter 1/p. And

8

since for large p the summands in (9) behave like

$$\frac{\log p}{p} + O\left(\frac{1}{p}\right),$$

from (9) we get the heuristic estimate,

$$C(n) = \sum_{p \le n} \frac{\log p}{p} \approx \log n$$
, for large n .

It would certainly be nice to have an actual information-theoretic proof of Theorem 1 along those lines—Billingsley suggests so too—but the obvious strategy doesn't work, or at least I wasn't able to make it work. The problem is that the approximation of the distribution of the $\{X_i\}$ by independent geometrics is not accurate enough to turn the two " \approx " steps in (8) and (9) into rigorous bounds. That's the bad news. But there's also good news.

IV. An Information Theoretic Proof

As it turns out, it *is* possible to give an elementary informationtheoretic proof of Theorem 1, albeit using somewhat different arguments from Billingsley's. Here's the more-beautiful-half of the proof; for the other half see [12].

Proof that C(n) *is asymptotically* $\geq \log n$. The starting point is again our basic argument in (4):

log
$$n = H(N) = H(X_1, X_2, \dots, X_{\pi(n)}) \le \sum_{i=1}^{\pi(n)} H(X_i).$$

Since the distribution of an integer-valued random variable *X* with mean $\mu > 0$ is maximized by the entropy

$$h(\mu) \triangleq (\mu + 1) \log(\mu + 1) - \mu \log \mu$$

of a geometric with the same mean, if we write $\mu_i = E(X_i)$ for the mean of X_i , then,

$$\log n \le \sum_{i=1}^{\pi(n)} h(\mu_i)$$

But from the distribution of X_i as expressed in (7) it is easy to get some useful information about μ_i :

$$\mu_i = \sum_{k \ge 1} \Pr\{X_i \ge k\} \le \sum_{k \ge 1} \left(\frac{1}{p_i}\right)^k = \frac{1/p_i}{1 - 1/p_i}.$$

Therefore, since $h(\mu)$ is an increasing function, we obtain,

$$\log n \leq \sum_{i=1}^{n} h\left(\frac{1/p_i}{1-1/p_i}\right)$$
$$= \sum_{p \leq n} \left[\frac{\log p}{p-1} - \log\left(1-\frac{1}{p}\right)\right], \quad (10)$$

and that's basically it.

Since the summands above behave like $\frac{\log p}{p}$ for large *p*, an easy exercise in elementary calculus gives,

$$\liminf_{n \to \infty} \frac{C(n)}{\log n} \ge 1,\tag{11}$$

as claimed.

V. Epilogue

It is very satisfying that elementary information-theoretic tools can produce optimal asymptotic estimates in number theory, like the lower bound (11) corresponding to Chebyshev's Theorem 1. In fact, from the actual result we derived in (10) it's also easy to deduce finite-n refinements of this lower bound, like, e.g.,

$$C(n) \ge \frac{86}{125} \log n - 2.35$$
, for all $n \ge 16$.

Unfortunately, it is not clear how to reverse the inequalities in the above proof to get a corresponding upper bound on C(n). Nevertheless, a different information-theoretic argument does work, and shows that,

$$\sum_{p \le n} \frac{\log p}{p} \le \log n + 2\log 2$$

for all $n \ge 2$; see [12].

Two final remarks before closing. First, although Biilingsley in [4] does not produce any information-theoretic proofs *per se*, he does go in the "opposite" direction: He uses probabilistic techniques and results about the primes to compute the entropy of several relevant collections of random variables.

And lastly, we mention that in Li and Vitányi's text [13], an elegant argument is given for a more accurate lower bound on $\pi(n)$ than those we saw above. Using ideas and results from algorithmic information theory, they show that $\pi(n)$ asymptotically grows at least as fast as $\frac{n}{(\log n)^2}$. The proof, which they attribute to unpublished work by P. Berman (1987) and J. Tromp (1990), is somewhat involved, and uses tools very different to those developed here.

References

- T.M. Apostol, Introduction to Analytic Number Theory. Springer-Verlag, New York, 1976.
- [2] P.T. Bateman and H.G. Diamond, A hundred years of prime numbers. Amer. Math. Monthly, vol. 103, no. 9, pp. 729–741, 1996.
- [3] P. Billingsley, Ergodic theory and information. John Wiley & Sons Inc., New York, 1965.
- [4] P. Billingsley, "The probability theory of additive arithmetic functions," Ann. Probab., vol. 2, pp. 749–791, 1974.
- [5] H. Bohr, "Address of Professor Harold Bohr," In Proceedings of the International Congress of Mathematicians (Cambridge, 1950), vol. 1, pages 127–134, Amer. Math. Soc., Providence, RI, 1952.
- [6] G.J. Chaitin, "Toward a mathematical definition of "life"," In Maximum entropy formalism (Conf., Mass. Inst. Tech., Cambridge, Mass., 1978), pages 477–498. MIT Press, Cambridge, Mass., 1979.
- [7] P.L. Chebychev, "Mémoire sur les nombres premiers, J. de Math. Pures Appl., vol. 17, pp. 366–390, 1852.

- [8] P.L. Chebychev, "Sur la totalité des nombres premiers inférieurs à une limite donnée," J. de Math. Pures Appl., vol. 17, pp. 341–365, 1852.
- [9] T.M. Cover and J.A. Thomas, *Elements of Information Theory*. J. Wiley, New York, 1991.
- [10] H.G. Diamond, "Elementary methods in the study of the distribution of prime numbers," Bull. Amer. Math. Soc. (N.S.), vol. 7, no. 3, pp. 553–589, 1982.
- [11] M. Kac, Statistical Independence in Probability, Analysis and Number Theory. Published by the Mathematical Association of America. Distributed by John Wiley and Sons, Inc., New York, 1959.
- [12] I. Kontoyiannis, Some information-theoretic computations related to the distribution of prime numbers. *Preprint, available online at*: http://aps.arxiv.org/abs/0710.4076, November 2007.
- [13] M. Li and P. Vitányi, An Introduction to Kolmogorov Complexity and its Applications. Springer-Verlag, New York, second edition, 1997.

Latest Activities of the IT Student Committee

A. Yener, L. Sankar, I. Maric, B. Shrader

The Student Committee has been hard at work since we last reported our activities in the December issue. In addition to having and planning our usual conference activities, a couple of new and exciting initiatives are underway.

First, a few words about our most recent event at the Conference on Information Sciences and Systems (CISS) in Princeton, NJ are in order. On Thursday, March 20, we organized a research discussion round table event for all participating students. About 90 students attended the event held at the Friend Center convocation room of Princeton University. There were six research topics discussed and led by the student volunteers. The following is a list of research topics and team leaders.

- 1. "MIMO Channels," leader: Jimmy Chui, Princeton University.
- 2. "Network Coding," leader: Anna Pantelidou, University of Maryland, College Park (UMD-CP).
- 3. "Sparse Representations and Compressed Sensing," leader: Eugene Brevdo, Princeton University.
- 4. "Ad-hoc Networks," leader: Sharon Betz, Princeton University
- 5. "Network and Information Security," leaders: Lifeng Lai and Ruoheng Liu, Princeton University, and Prasanth Ananthapadmanabhan, UMD-CP.



Jimmy Chui and Sharon Betz hold cards identifying the topics discussed at their tables at the CISS 2008 event.

6. "Network Optimization," leaders: Chee Wei Tan, Princeton University, and Joydeep Acharya, WINLAB, Rutgers.

We thank Lalitha Sankar for coordinating the event, and the student volunteers in the above list for leading these lively discussions and helping serve the lunch boxes. Aside from the non-vegetarian sandwiches going a bit faster than we anticipated (but no one went hungry!), the event appeared to be successful. The meeting concluded with the advertisement of the First Annual School of Information Theory by Gerhard Kramer who was our guest at the event. More details on the event and papers discussed can be found on the student website: http://students.itsoc.org/.

We are already well into April now, which means we are busy planning the events at the upcoming ISIT. As done every year, we are organizing two events: on Monday, July 7, we will have the research discussion round table and on Thursday, July 10, a panel discussion and committee meeting will be held. As every year, there will be IT Student Society T-shirts free for participants. Both events will be held at lunch time, so don't forget to bring your appetite along with your ideas! As always, please contact Lalitha Sankar if you would like to volunteer as a discussion leader at the round table discussion event. You can propose a round table research topic, or go with one already proposed. You can even throw in your ideas and comments about the student committee events in general. Graduate students and postdocs are both welcome. Don't be shy to volunteer; if you've been to any of the student committee meetings, you know that they are as informal and fun as they are informative!

An exciting new initiative worth mentioning here is the redesign of the student committee web page and the online content. Specifically, our aim is to move to a content management system from the static page that we have, in-line with the overall societywide effort going on. We thank Anand Sarwate for volunteering to help with this major task, as well as J. Nicholas Laneman and the rest of the IT Web committee. We are at the beginning now and will have more to report on this issue in the near future.

Last but not the least, a major student oriented initiative is the organization of an Annual School of Information Theory. The aim of the School of Information Theory is to bring together graduate students, postdoctoral researchers and senior researchers working on information theory related problems in an interactive campus environment once a year. In doing so, we follow the tradition of the European Winter School on Coding and Information Theory and bring it to North America. All the student committee leaders have been and are currently heavily involved in this organization. Aylin Yener and Gerhard Kramer proposed the school last year and they have been working towards raising funds to cover the cost of the school (The school has no registration fee and we hope to be able to award travel grants from remaining funds after the school concludes), as well as the organization, with a lot of help from Ivana Maric and Sennur Ulukus in selection of applications and session organization, Lalitha Sankar and Brooke Shrader in publicizing the school and Nick Laneman for developing the web-site of the school, http://school.itsoc.org/.

The First Annual School of Information Theory will be held Sunday, June 1, to Thursday, June 5, 2008, at the University Park Campus of Penn State University, PA. There will be three courses held on June 2, 3, and June 4, by Professors Muriel Medard, David Tse and Toby Berger, respectively. There will also be a panel of senior researchers and a keynote lecture on June 4 and 5. Each student attending the school will give a short presentation and/or a poster.

The response to the call for participation of the school has been well above our expectations, despite the relatively short window of applications. We look forward to the school and will report back here our observations of this exciting event.

That's all from the Student Committee for now. As always, please feel free to contact us with any questions or comments you might have. We hope to involve more student volunteers, once again please e-mail lalitha@princeton.edu if you'd like to participate.

Workshop Report: 3rd Information Theory and Applications Workshop

Ever since its inauguration in 2006, the Information Theory and Applications (ITA) centre at UC San Diego has made it an annual affair to hold a workshop. This enables eminent researchers to discuss the latest advances in information theory as well as its application to a myriad of different areas.

The third ITA workshop was held at UCSD from January 28 to February 1, 2008. It brought together around 500 participants from a variety of educational institutions and companies, for a week long scientific and illuminative interaction on variegated areas of scientific interests.

The workshop kicked off on Sunday January 27 with a small reception, while the next five days were filled with excellent invited talks and special sessions. Monday program was dedicated to a variety of technical talks on information and communication theory as well as an exciting open problem session. In addition, a memorial session to commemorate David Slepian's work and life was held on Monday. The agenda for Tuesday was similar, with sessions on a variety of topics in information theory. On Tuesday, Rudiger Urbanke's creative game/show/session, titled "Who wants to be a researchaire?" provided an enjoyable sense of relief and entertainment.

Wednesday saw a change in the routine, when a select number of

outstanding graduating students and postdocs were given the opportunity to expound their research in 30 minute talks. An edifying keynote plenary talk: "Sparse sampling: variations of theme by Shannon" by Martin Vetterli, EPFL, followed these "graduation day" talks.

On Thursday and Friday, the routine was resumed with sessions on applications of information theory in multifarious areas including Networking, Optimization and Control, Machine Learning, Neuroscience and Bioinformatics. In parallel, four tutorials on Compressed Sensing, Signal Processing for Integrative Bioinformatics, Visual Recognition and Multimedia data continued the interdisciplinary tradition of ITA workshops. The workshop ended with a short course on Compressive Sensing.

In addition to the technical and special sessions, the workshop included a tour of the Salk Institute and labs, a visit to the Torrey Pines Park, and a banquet where some of our very own talented scientists and information theorists pleasantly surprised the audience with their musical talents.

In short, the event was a success and the arrangements for the next workshop are under way. Detailed information about the past and previous workshops can be found on http://ita.ucsd.edu.

The 2007 Chinese Workshop on Information Theory, December 14-16 2008, Guangzhou, China

Li Ping

11

The 2007 Chinese Workshop on Information Theory was held at the South China University of Technology in Guangzhou, China, on December 14-16 2007, hosted by Gang Wei. This is the fourteenth workshop in the series sponsored by the Information Theory Chapter of Chinese Institute of Electronics. The program consisted of two days of technical sessions and forums on information theory related research and education activities in China. In his talk, past president of the IT Society Vijay Bhargava traced the progress of Information Theory in China from the early years. In particular, he mentioned the contributions of Xinmei Wang from Xidian University (who introduced, through a series of technical books, major discoveries in information theory to Chinese colleagues) and the research work presented by Chinese scholars at the 2007 IEEE Information Theory Workshop in Chengdu hosted by Pingzhi Fan of South-West Jiao Tong University. Following the conference banquet on 15 December, a meeting of the Chapter was held where it was decided to hold the 15th workshop in Beijing in 2009.

Guangzhou is a historical city that has seen rapid modernization. As the southern gateway to China, Guangdong has also taken up an important position in China's modern history. Following the workshop, some of us traveled to Zhongshan, a city next to Guangzhou, and visited the birth place of Dr Sun Yat Sen, who is regarded as the farther of modern China.

The organizers of the workshop received many compliments and the workshop was found to be very successful.



Participants to the workshop.

GOLOMB'S PUZZLE COLUMN™

Divisibilities in Numerical Triangles Solutions

Solomon W. Golomb



For simplicity, we denote the elements of the *n*-element set A_n by $\{1, 2, 3, ..., n\}$. We define the cyclic permutation mapping $m: A_n \rightarrow A_n$ by $m(j) \equiv j + 1 \pmod{n}$. That is, under *m*, $1 \rightarrow 2 \rightarrow 3 \rightarrow \cdots \rightarrow n - 1 \rightarrow n \rightarrow 1$.

For Problem 1. a. Consider all *k*-element subsets of A_n under the mapping *m*. For 0 < k < n, each *k*-subset is mapped to a different *k*-subset by *m*. When *n* is prime, repeating the mapping *m* gives new *k*-subsets for the first n - 1 iterations, and gets back to the original *k*-subset (only) after *n* iterations. Thus, under *m*, the *k*-subsets of A_n are partitioned into distinct groupings *n* at a time when *n* is prime; so in this case *n* divides C(n, k) for all *k* with 0 < k < n.

b. Consider all partitions of A_n into k parts (we will call these k-partitions) under the mapping m. For 1 < k < n, each k-partition of A_n is mapped to a different k-partition by m; and if n is prime, repeating m gives new k-partitions for the first n - 1 iterations, and gets back to the original k-partition (only) after n iterations. Thus, when n is prime, the k-partitions of A_n occur in groupings n-at-a-time under m; so for prime n, n must divide s(n, k) for all k with 1 < k < n.

c. Consider all permutations of A_n into k disjoint cycles (we will call these k-permutations) under the mapping m. For 1 < k < n, each such k-permutation is mapped to a different k-permutation by m; and when n is prime, repeating m gives new k-permutations for the first n - 1 iterations, and gets back to the original k-permutation (only) after n iterations. Thus, under m, the k-permutations of A_n form groupings n-at-a-time when n is prime, for 1 < k < n; so in these cases, n divides S(n, k).

For Problem 2. In all three cases, C(n, k), s(n, k), and S(n, k), when n = 2p where p is prime, the iterations of the mapping m will go through either p or 2p = n iterations in order to return to the starting point, for 1 < k < p and for p < k < 2p = n. (At $k = p = \frac{1}{2}n$, periodicity 2 is also possible.)

Thus, for these k, all of C(2p, k), s(2p, k), and S(2p, k) are divisible by p. (Also, C(2p, 1) = 2p is clearly divisible by p.)

For Problem 3. Because T(n + 1, k + 1) is a linear combination of T(n, k) and T(n, k + 1) with integer coefficients, when both T(n, k) and T(n, k + 1) are divisible by prime p, so too is T(n + 1, k + 1). (Here T stands for any of C, s, or S.) From divisibilities by p in row p (as in Problem 1), a narrowing descending triangle of entries in the subsequent rows will be divisible by p in all these case for $1 \le j \le p - 2$ and for j + 1 < k < p. (Actually, because C(p, 1) is divisible by p, there is an extra column on the left of the "descending triangle" in C(n, k) containing multiples of p; and because both s(p + 1, p) and S(p + 1, p) are multiples of p, there is an extra entry one position further to the right which is divisible by p in the "descending triangles" of s(n, k) and S(n, k) in rows p + 1 to 2p - 2.)

For Problem 4. From Problem 3, each of C(14, 5), s(14, 5) and S(14, 5) is simultaneously divisible by 11 and 13. From Problem 2, since $14 = 2 \times 7$, each of these numbers is also divisible by 7. So all three are divisible by $7 \times 11 \times 13 = 1001$. Specifically, $C(14,5) = 2002 = 1001 \times 2$, $s(14, 5) = 40,075,035 = 1001 \times 40,035$ and $S(14, 5) = 9,957,703,756 = 1001 \times 9,947,756$, but as the problem stated, the basic result needs no calculation.

Notes. 1. Several other numerical triangles have similar divisibility properties. For example, if L(n, k) is the number of permutations on A_n which, when written as a product of disjoint cycles have exactly k 1-cycles, when n is prime n divides L(n, k) for all k with $1 \le k < n$.

2. I have not seen the combinatorial proof approach to these problems as presented here in the literature, but it may be out there somewhere. Please notify me if you have a reference.

Guest Column: News from the National Science Foundation

Sirin Tekinay, Program Director for the Communications Program, and Cyber-Enabled Discovery and Innovation Program

Dear reader,

This is the eleventh quarterly guest column in this series. I'm thrilled to see this space continue to serve its purpose of enabling our interaction on all that impact us as professionals in the communications community as I write about relevant NSF programs and news.

New and Upcoming Programs

I continue to serve as the lead for the Cyber-Enabled Discovery and Innovation (CDI) [1] program is "mid-review-process" at the time of writing: a total of some thirteen hundred preliminary proposals were reviewed by multi-disciplinary panels run by teams of two to three NSF program officers mid-February. (This year, Valentine's Day was changed as CDI-Type II Panel Day 1.) In the aftermath of these panels, the CDI Working Group and the extended team of panel moderators poured over all of the panel reports and converged relatively quickly on two hundred invitations for the full proposal stage. Full proposals are due on April 29. We will hold the full proposal review panels early in June. It is thrilling to think that mid-July we will have the first set of CDI Awards granted! Among the submitted, then invited proposals, our community is well represented. Also, many of you have volunteered, and served on the review panels. If you would like to volunteer to participate in the CDI review process, please let us know by registering on our reviewer database [2]. As we get ready for the second stage of the CDI review process, we are also busy planning for the 2009 cycle. The solicitation is back on the drawing boards, with its much anticipated budget increase and revised timelines. It should appear by June-please stay tuned!

In the meantime, the CISE-wide Network Science and Engineering (NetSE) Program will be making its first appearance soon, with funding allotted for 2009. I have co-authored the text for the solicitation with my two other colleagues, representing the two other divisions in the directorate.

Speaking of 2009 funding, the entire directorate has joined in synchronizing its solicitations so that all communities served by the Directorate for Computer Information Sciences and Engineering (CISE) can consolidate their research proposal plans accordingly. Here is a deliberately sketchy description of what might happen as a result of our current efforts. Please treat this as work in progress, subject to deviate from the depiction below. Under the CISE umbrella, we will have three "core" programs, corresponding to the three divisions in the directorate. One of these three, Computing and Communications Foundations (CCF), of course includes what is currently "Theoretical Foundations- Communications Research, Signal Processing Research, Theory of Computing, etc." Then, a fourth program will include cross-cutting, CISE-wide program elements. Science for Internet's Next Generation (SING) is now part of NetSE, which is one of these four program elements. The general structure is meant to streamline the submissions to better serve the research community by introducing synchronized, structured timelines for different project sizes and content by staggering the due dates for small, medium and large projects, and introducing limits

on annual submissions to core and cross-cutting programs. What is for certain is that the spirit of this activity is to broaden the scope of impact of collective research output by CISE without sacrificing the usual depth of sharply focused projects.

News on Communications Program

The Theoretical Foundations 2008 Program Solicitation [3] (TF08) closed on March 19, 2008. We ended up receiving about four hundred and fifty proposals, with one hundred and fifty in Communications Foundations. The panels are formed, and we are about to start holding the panel meetings. The last of these meetings will take place mid-June, after which award decisions will have to be made efficiently in order to meet the grants administration deadline so that the awards can be granted by the federal close out. Thank you all for keeping up the submission volume and for all your help in the review process. I am committed to announcing the award decisions by the end of June.

That should give us and the reviewers a breather until we receive the CAREER proposals mid-July.

In addition to being part of the CISE solicitation in the 2009 cycle, I am happy to announce that the communications program element has now grown into a cluster of "Communications and Information Foundations." This cluster will include Communication Theory, Information Theory, and Signal Processing, in addition to emphasis areas of Foundations of Secure Communications, and Quantum Information and Communication Theory. The subtopics that will be covered by the cluster will be grouped together in the new CISE-CCF solicitation.

As of February 8, 2008, Ms Laurin Battle, Assistant to the Communications Program, has moved onto the position of Program Specialist with Cross-Directorate Programs in CISE, after four years of excellent service to our community. If you ever called our office, traveled to NSF, participated in a panel, sent in an inquiry, filed a mail review, in short, interacted with your NSF program in any way, chances are, you already know Laurin. With her professionalism, keen sense of duty, responsiveness, and whirlwind efficiency, she has made it not only easy, but also, with her confident, positive attitude, a pleasure, to run the program with her. Our new program assistant is no stranger to our community: Ms Dawn Patterson, who had filled in for Laurin during her maternity leave last year, is our new program assistant. Dawn will in fact support not only Communications Foundations, but the entire Theoretical Foundations Program. She has already rolled up her sleeves to take on the workload, with her cheerful disposition. The administrative support for our program is in her capable, safe hands.

NSF People

In every column, I introduce some of the people I work with; who embody the culture and spirit of NSF. This time I would like to introduce the newest Program Director in CCF: Professor Chita



Das, who has been on the faculty at the Pennsylvania State University since 1986, currently a professor in the Department of Computer Science and Engineering, has joined the Computing Processes and Artifacts Cluster. He received the Ph.D. degree in computer science from the Center for Advanced Computer Studies, University of Louisiana, in 1986. Chita's primary research interests include computer architecture, parallel and distributed computing, cluster systems, processor management in multiprocessors, performance evaluation and fault-tolerant computing. He has published extensively in these areas. Of late, he is working on multi-core/SoC systems, Network-on-Chip (NoC) microarchitectures, Internet QoS, multimedia servers, and mobile computing. He has served on the editorial board of *IEEE Transactions on Computers* and *IEEE Transactions on Parallel and Distributed Systems*. Dr. Das is a Fellow of the IEEE and a member of the ACM.

As a result of biased sampling of housing options around NSF, Chita and his lovely wife are my newest neighbors across the hall from me in my condo building next to NSF. He adds tremendously not only to the work environment but also to the neighborhood with his outgoing, helpful, always smiling personality.

The "Social Scene"

The colleagues from Theoretical Foundations seem to be at hand to run to one of the local favorite places for a quick bite. However, the weekly CISE dinners seem to be more strictly scheduled for Wednesdays. Finally, many combinations of CDI folks can be expected to have lunch and coffee breaks together. That most of the socialization happens among program officers is attributed to the transient culture of the environment: the process of making friends is somewhat accelerated here. Most folks have left their home institutions, homes, and families to serve as a program officer for a couple of years, so they have coined terms for themselves such as MBA: Married-but-Available, or "ineligible bachelors" to depict their social status.

On a Personal Note

The end of Summer 2008 marks the end of my third year here at the NSF. While whether I will stay on to continue my work with cross-disciplinary programs I helped formulate is still up in the air, I will most probably hand off my original responsibility of Program Director for Communications Research to a newcomer. My position was posted on the NSF web [4] recently. Please let me know how I can help facilitate your interest, your application, and who knows, maybe your orientation here...

True to tradition, I have been writing the draft of this installment on the train from New Jersey. The train is pulling into the beautiful Washington Union Station, signaling I should wrap up.

... Till next time, dream big, and keep in touch!

Sirin Tekinay Program Director, Communications Foundations National Science Foundation 4201 Wilson Blvd Arlington VA 22230 USA stekinay@nsf.gov http://www.nsf.gov/staff/staff_bio.jsp?lan=stekinay&org=CCF& from=staff

REFERENCES:

- [1] http://www.nsf.gov/crssprgm/cdi/
- [2] http://www.nsf.gov/crssprgm/cdi/form.cfm
- [3] http://www.nsf.gov/pubs/2008/nsf08518/nsf08518.htm
- [4] http://jobsearch.usajobs.opm.gov/getjob.asp?JobId= 69185928&AVSDM=2008%2D03%2D03+00%3A03%3A01

CALL FOR PAPERS

IEEE Journal on Selected Areas in Communications CAPACITY APPROACHING CODES

The field of channel coding began with Claude Shannon's 1948 landmark paper in which he introduced the notion of channel capacity and proved the existence of codes that can achieve reliable communication at rates approaching capacity. For the past 60 years, researchers have been trying to construct codes that have practical encoding and decoding procedures and can approach the performance promised by Shannon. For the first 45 years, these efforts fell short of the mark. Then, with the invention of turbo codes in 1993 and the re-discovery of low-density parity check (LDPC) codes a few years later, the goal of practical capacity approaching codes came within reach. Since that time, the area of channel coding has undergone a remarkable revival, and in areas such as space and satellite communication, digital video broadcasting, wireless telephony, and digital magnetic recording, older methods are being replaced by newer, less complex, and better performing codes.

The special issue solicits papers that present original and unpublished work on topics including, but not limited to:

- Turbo codes, including parallel, serial, and hybrid concatenation
- Repeat-accumulate type codes

- LDPC codes and codes on graphs
- Algebraic and protograph-based constructions of LDPC codes
- Iterative decoding methods
- Density evolution and EXIT chart techniques
- Performance bounds for iterative decoding
- Capacity approaching codes in networks, coded modulation, and MIMO systems
- Fountain (rateless) codes for packet erasure channels
- VLSI implementation of capacity approaching codes

Papers stressing applications are particularly encouraged. Prospective authors should follow the IEEE JSAC manuscript format described in the information for authors. The paper should be formatted to print on either A4 or letter paper with no more than 20 double-spaced pages, excluding illustrations and figures. Prospective authors should send a PDF version of their manuscript with a separate cover letter (in word or text format), which contains the paper title, authors with contact information, and a 150-word abstract, to Prof. Daniel Costello.

Submission Deadline: October 1, 2008 Acceptance Notification: February 1, 2009 Final Manuscript Due: April 1, 2009 Publication Date: Third Quarter 2009

The Guest Editors for this issue are: **Prof. Daniel Costello** University of Notre Dame Email: costello.2@nd.edu

Prof. Shu Lin University of California, Davis Email: shulin@ece.ucdavis.edu

Prof. William Ryan University of Arizona Email: ryan@ece.arizona.edu

Dr. Thomas Richardson Qualcomm, Inc. Email: tomr@qualcomm.com

Prof. Ruediger Urbanke EPFL Email: ruediger.urbanke@epfl.ch

Prof. Richard Wesel University of California, Los Angeles Email: wesel@ee.ucla.edu

Institute for Information Transmission Problems RAS IEEE Information Theory Society Saint-Petersburg State University of Aerospace Instrumentation

The Workshop "Coding Theory Days in St. Petersburg" 6 - 10 October 2008, St. Petersburg, Russia.

First Call for Papers

The Workshop "Coding Theory Days in St. Petersburg" will be held from Monday October 6th to Friday 10th in St. Petersburg, Russia.

Previously unpublished contributions from a broad range of topics in information theory will be solicited, including (but not limited to) the following areas:

- Error-correcting codes
- Combinatorics of coding theory
- Code-based cryptography
- Spherical codes and designs

Submitted papers, not to exceed six pages, should be of sufficient detail for review by experts in the field. Survey, tutorial, and expository papers are also welcome. The paper submission deadline is **June 1, 2008**, with notification of acceptance by **July 15, 2008**.

Conference registration fee is € 250 and includes: conference materials, CD-ROM proceedings, welcome reception, coffee breaks, banquet.

For more information and general inquiries please visit <u>http://k36.org/codingdays/</u> or send your requests to <u>codingdays@vu.spb.ru</u>

The Organizing Committee:

Eugene Krouk, General Chair Sergei Fedorenko, General Vice Chair

The Program Committee:

Ilya Dumer, Program Co-Chair Grigory Kabatiansky, Program Co-Chair

Important dates:

June 1, 2008: deadline for extended abstract submission (<u>http://k36.org/codingdays/</u>) June 1, 2008: deadline Registration Form submission (e-mail: <u>codingdays@vu.spb.ru</u>) July 15, 2008: notification of acceptance September 1, 2008: final paper upload deadline

Conference Calendar

DATE	CONFERENCE	LOCATION	CONTACT/INFORMATION	DUE DATE
June 16, 2008	First IEEE International Workshop on Wireless Network Coding (WiNC 2008	San Francisco, California,)) USA	http://wine.dnsalias.org/winc2008/	March 30, 2008
June 24 – 26, 2008	24th Biennial Symposium on Communications	Ontario, Canada	http://www.ece.queensu.ca/ symposium/	February 15, 2008
July 6 – 11, 2008	2008 IEEE International Symposium on Information Theory (ISIT 2008)	Toronto, Canada	http://www.isit2008.org	January 7, 2008
July 6–9, 2008	IEEE International Workshop on Signal Processing Advances for Wireless Communications (SPAWC 200	Recife, Brazil 8)	http://spawc2008.org/	February 11, 2008
July 14 - 15, 2008	2008 Information Theory and Statistical Learning (ITSL 2008)	Las Vegas, Nevada	http://www.bio-complexity.com /ITSL/ITSL_index.html	Feb. 25, 2008
August 18 - 19, 2008	Workshop on Information Theoretic Methods in Science and Engineering	Tampere, Finland	http://???.fi	-
September 1 – 5, 2008	2008 International Symposium on Turbo Codes and Related Topics	Lausanne, Switzerland	http://www.turbo-coding-2008.org/	March 27, 2008
Sept. 15–19, 2008	2008 International Castle Meeting on Coding Theory and Applications (ICMCTA 2008)	Valladolid, Spain	http://wmatem.eis.uva.es/2icmcta/	May 15, 2008
Sept. 24–26, 2008	The Annual Allerton Conference on Communication, Control and Computing (Allerton 2008)	Monticello, IL, USA	http://www.comm.csl.uiuc.edu /allerton/	July 1, 2008
Oct. 6-10, 2008	Workshop: Coding Theory Days in St. Petersburg	St. Peterburg, Russia	http://k36.org/codingdays/	June 1, 2008
Dec. 7 - 10, 2008	2008 International Symposium on Information Theory and its Applications (ISITA 2008)	Auckland, New Zealand	www.sita.gr.jp/ISITA2008/	May 7, 2008