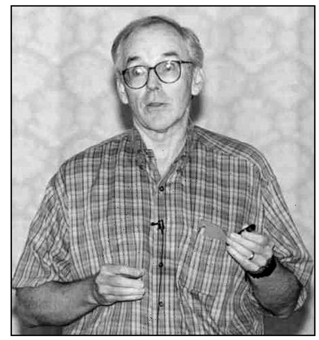
IEEE Information Theory Society Newsletter

Vol. 51, No. 4, December 2001 Editor: Lance C. Pérez ISSN 1059-2362

2001 ISIT Plenary Lecture

Are Turbo-like Codes Effective on Nonstandard Channels?*



Robert J. McEliece
California Institute of Technology
Pasadena, California USA
E-mail: rjm@systems.caltech.edu

Abstract

Turbo codes and their close relatives, e.g. Gallager and RA codes, have been shown to be extraordinarily effective on the "standard" channel models, e.g. the binary erasure, binary symmetric, and the AWGN channels. In this paper we discuss the possibility of using turbo-like codes on a variety of other channel models, including some that are nonsymmetric, nonbinary, and multiuser. Our basic conclusion is that binary turbo-like codes with graph-based iterative decoding have great potential on nearly all such channels.

1. How Hard is it to Approach Channel Capacity?

We begin at the beginning, with Shannon's celebrated channel coding theorem. It can be stated as follows:

Theorem 1. *(Shannon) For any discrete-input memoryless channel, there exists a number C, the channel capacity, such that for any desired data rate $R < C$ and any desired error probability $p > 0$, it is possible to design an encoder-decoder pair that permits the transmission of data over the channel at rate R and decoded error probability $< p$.*

Shannon's theorem and a bit more is illustrated in Figure 1. There we see the smallest attainable decoded bit error probability p as a function of the data rate R, where R is measured in multiples of capacity. Note the phase transition at $R = C$. For $R < C$, the minimum attainable p is 0+, whereas for $R > C$, $p_{\min} = H_2^{-1}(1 - C/R)$, where $H_2(x)$ is the binary entropy function.

Shannon's theorem is an existence theorem, and as engineers we naturally ask, "how hard is it to communicate at rate R and decoded error probability p?" We will restrict ourselves to the case $R < C$, for if $R > C$ we would need to consider source coding, which is beyond the scope of this paper. We are especially interested in communicating reliably at rates very near capacity, so let us assume in fact that

$$R = (1 - \epsilon)C,$$

where ϵ is a small positive number. Now let's define $\chi_E(\epsilon, p)$ to be the minimum possible *encoding* complexity, $\chi_D(\epsilon, p)$ to be the minimum possible *decoding* complexity, both measured in arithmetic operations per information bit, for an encoder-decoder pair that operates at rate $(1 - \epsilon)C$ and decoded bit error probability p.

It is important to know the behavior of $\chi_E(\epsilon, p)$ and $\chi_D(\epsilon, p)$, for fixed p, as $\epsilon \to 0$. Naturally we expect a singularity at $\epsilon = 0$, but how severe is it? The classical results (i.e., prior to 1970) in this direction are not encouraging:

Theorem 2. *On a discrete memoryless channel of capacity C, for any fixed $p > 0$, as $\epsilon \to 0$,*

$$\chi_E(\epsilon, p) = O\left(1/\epsilon^2\right)$$

continued on page 3

*This work was supported by NSF grant no. CCR-9804793, and grants from Sony, Qualcomm, and Caltech's Lee Center for Advanced Networking.

From the Editor

Lance C. Pérez

In this issue of the IEEE Information Theory Society Newsletter we are fortunate to have an article written by Robert J. McEliece entitled "Are Turbo-like Codes Effective on Nonstandard Channels?" based on his plenary lecture at the 2001 ISIT. This is a provocative article with bold conclusions about some of the most basic questions in information theory; I am sure that IT Society members will find it good reading. There is also a tribute to Claude E. Shannon written by Art Lewbel, a juggling friend of Shannon's, from a unique perspective and accompanied by several fascinating photographs.

I am pleased to announce that the Board of Governors has approved a proposal to add this newsletter to the IT digital library. The impetus for this proposal came from the donation of a collection of IT Newsletters, beginning with the March 1954 issue, by Larry Rauch to Bob McEliece who then offered them to the IT Society. Details about this project will appear in the March 2002 newsletter.

Lance C. Pérez

Finally, this issue marks the return of the IT Newsletter to the normal publication schedule! This would not have been possible without the efforts of many people from the Society and from IEEE who accepted short lead times and met unreasonable deadlines. Thank you.

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

Issue	Deadline
March 2002	January 15, 2002
June 2002	April 12, 2002
September 2002	July 16, 2002

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

I may be reached at the following address:

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

Sincerely,
Lance C. Perez

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

Are Turbo-like Codes Effective on Nonstandard Channels?*

Continued from page 1

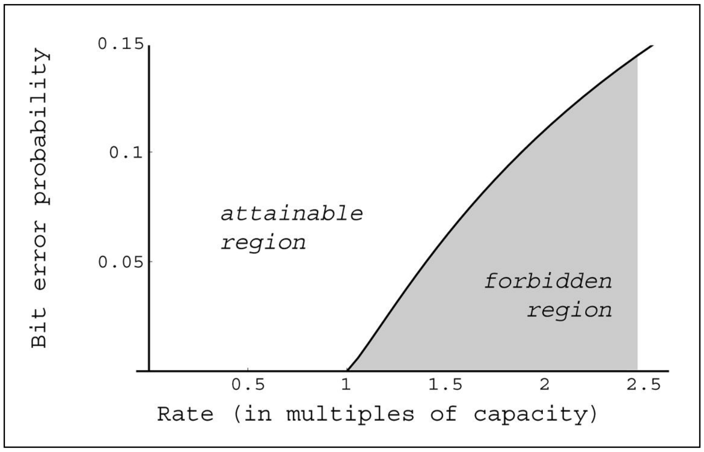


Figure 1. Shannon's Channel Coding Theorem.

$$\chi_D(\epsilon, p) = 2^{O(1/\epsilon^2)}$$

Proof: (Sketch) Use linear codes with (per-bit) encoding complexity $O(n)$,and ML decoding with decoding complexity $2^{O(n)}$. The blocklength n is related to ϵ by $n=O(1/\epsilon^2)$, because of the random coding error exponent, which says the average error probability for the ensemble of linear codes of rate R satisfies

$$\overline{p} \le e^{-nE_r(R)}$$

and

$$E_r(C(1-\epsilon)) \approx K\epsilon^2 \text{ as } \epsilon \to 0.$$

Theorem 2 tells us that the encoding problem is not especially difficult, but it suggests that decoding will be a real bottleneck.[1]

2. Turbo-like Codes on Symmetric Binary-Input Channels.

However, in the wake of the turbo-code revolution, the decoding problem looks much less formidable, and we offer the following conjecture.

Conjecture 1. *[9] Turbolike codes are effective on any symmetric binary input channel. More precisely, for any SBIC, there exists a sequence of "turbo-like" code ensembles plus matched iterative decoding algorithms, such that for any fixed p, as* $\epsilon \to 0$,

$$\chi_E(\epsilon, p) = O\left(\log \frac{1}{\epsilon}\right)$$

$$\chi_D(\epsilon, p) = O\left(\frac{1}{\epsilon} \log \frac{1}{\epsilon}\right).$$

By a "turbo-like" code I mean any binary linear code that has a low-complexity iterative message-passing decoding algorithm. Besides classical turbo codes, parallel and serial, turbo-like codes include:

- *Gallager* (Low-Density Parity-Check) Codes [11]
- *Irregular LDPC Codes* (Luby, Mitzenmacher, Richardson, Shokrollahi, Speilman, Stemann, and Urbanke) [15,16].
- *Repeat-Accumulate Codes* (Divsalar, Jin, McEliece) [6,14].
- *Irregular Turbo-Like Codes* (Frey and MacKay) [8]
- *Asymmetric Turbo Codes* (Massey and Costello) [19]
- *Mixture Turbo Codes* (Divsalar, Dolinar, and Pollara) [4]
- *Doped Turbo Codes* (ten Brink) [26,27].
- *Concatenated Tree Codes* (Ping and Wu) [23]

⋮

What do I mean by a "symmetric binary input channel"? A symmetric binary-input channel is a memoryless, discrete-time channel with input alphabet $X = \{+1, -1\}$, output alphabet Y (a subset of the real numbers), and transition probabilities characterized by a pdf $f(y)$:

$$p(y|x=+1) = f(y)$$
$$p(y|x=-1) = f(-y).$$

This class of channel models was introduced by Gallager [11, Chapter 3]. SBIC's include

- *The Binary Erasure Channel:*

$$f(y) = (1-p)\delta(y-1) + p\delta(y).$$

- *The Binary Symmetric Channel:*

$$f(y) = (1-p)\delta(y-1) + p\delta(y+1).$$

- *The Additive Gaussian Noise Channel:*

$$f(y)=K \exp((y-1)^2/2\sigma^2).$$

- *Fast Rayleigh Fading (noncoherent model):*

$$f(y) = \begin{cases} K\exp(-y/A) & \text{if } y \ge 0 \\ K\exp(y(1+A)/y) & \text{if } y < 0. \end{cases}$$

What evidence supports Conjecture 1? The strongest is surely the following.

Theorem 3. *(Luby, Mitzenmacher, Shokrollahi, Speilman, Stemann) For the binary erasure channel, for the ensemble of (degree-profile optimized) irregular LDPC codes with iterative belief propagation decoding, as* $\epsilon \to 0$,

[1]Actually, Forney [7], in his seminal work on concatenated codes, showed that $\chi_D(\epsilon,p)$ is bounded by a polynomial in $1/\epsilon$. I regret having overlooked this important fact in my lecture.

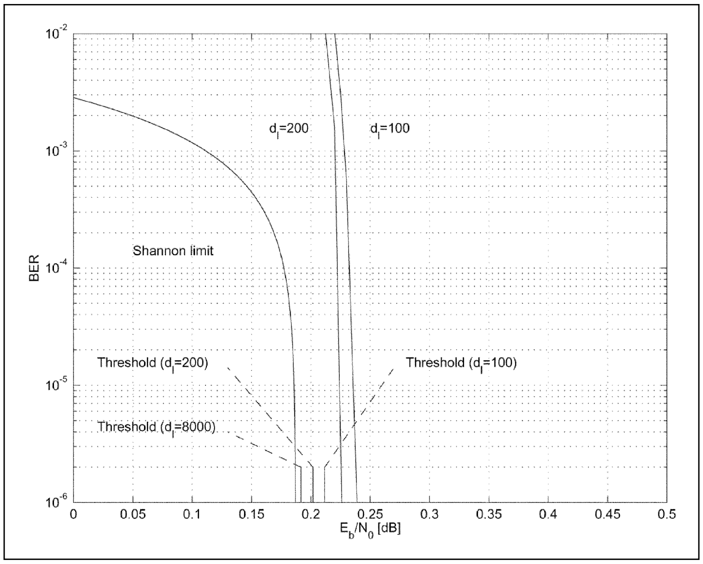


Figure 2. Irregular LDPC Codes on the AWGN Channel. (Chung, Forney, Richardson, Urbanke, 2001)

$$\chi_D(\epsilon, p) = O\left(\log \frac{1}{\epsilon}\right)$$

There are as yet no further rigorous theorems to support Conjecture 1, but there is overwhelming experimental evidence. The strongest such evidence is surely that of the AWGN channel, as illustrated in Figures 2 and 3. Figure 2, which is taken from [2], shows the iterative decoding threshold for a degree-profile optimized ensemble of rate 1/2 irregular LDPC codes for the AWGN channel. It is only 0.0045 dB from the Shannon limit for rate 1/2 codes! It takes little imagination to conjecture that further refining of the degree profile will push the iterative threshold all the way to the Shannon limit.

Equally remarkable is the performance shown in Figure 3, which is taken from [22]. In Figure 3 we see the actual performance of a code of rate about 1/60, with decoded bit error probability of around 10^{-5}, and E_b/N_0 less than –1 .3db, compared to the Shannon limit of –1.6 dB!

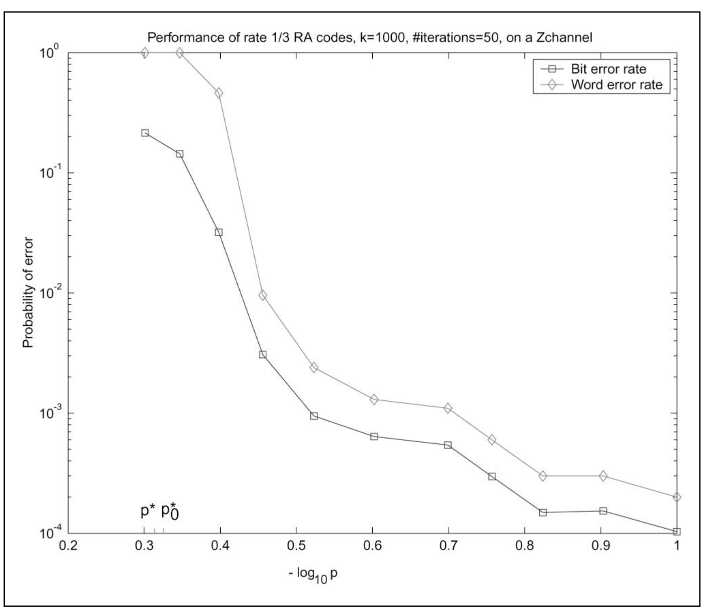


Figure 5. Performance of a *R* = 1/3 RA code ensemble with *k* = 1000 on a *Z*-channel.

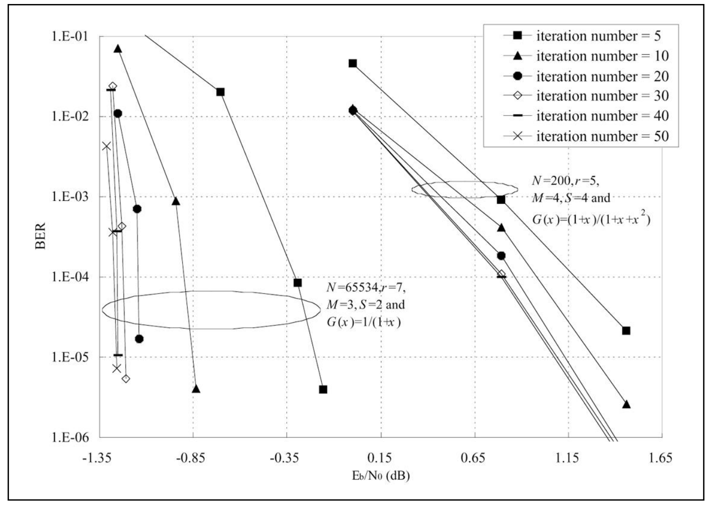


Figure 3. Turbo-Hadamard Codes on the AWGN Channel. (Ping, Leung, Wu [22])

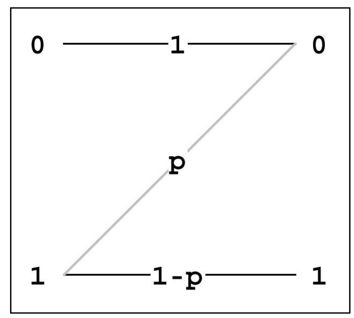


Figure 4. The *Z*-Channel.

3. Beyond SBIC's.

But what about non-SBIC's, i.e., channels that are

- Nonsymmetric?
- Nonbinary?
- Multiuser?
- Non-Memoryless?
- Etc.?

I believe that turbo-like codes can be used effectively on virtually any such channel. Let me illustrate with a few examples. First, let's consider the simplest nonsymmetric channel, the *Z*-channel.

4. Nonsymmetric Channels.

Rather than give a general discussion, we focus in this section on the simplest example of a nonsymmetric binary-input channel: the *Z*-channel. The *Z*-channel has input and output alphabets both equal to {0, 1}, and the channel transition probabilities are shown in Figure 4.

The challenge with this channel is that the input-achieving probability distribution is not uniform. For example, if the crossover probability is $p = 1/2$, the capacity of the *Z*-channel is 0.321928 bits per transmission, which is achieved by an input distribution of (0.6, 0.4). But we observe that by using a (1/2, 1/2) input, the resulting mutual information is 0.311278, which is only 3% less than capacity. This suggests

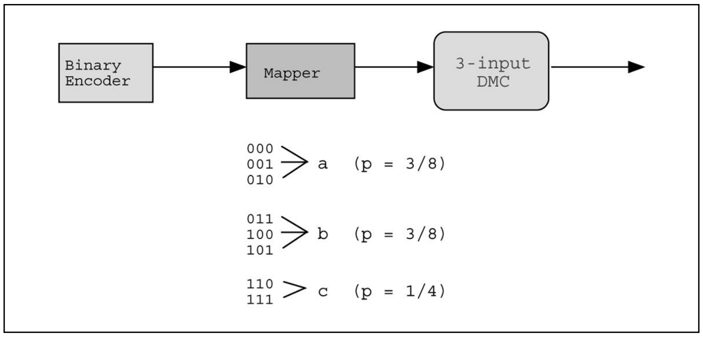


Figure 6. Gallager's Idea.

that if we transmit the binary encoded bits directly to the channel, good performance can be expected.

To test this expectation, we implemented a k =1000 rate 1/3 (regular) RA code using 50 iterations on a Z-channel. The results of this experiment are shown in Figure 5. (There are two curves, one for bit error probability and one for block error probability, each plotted against $-\log_{10}p$, where p is the channel crossover probability.) Note the "noise thresholds" marked $p^*$and p^*_0 on the horizontal axis. These correspond to the (negative logarithms of the) values of p for which the true capacity of the channel is exactly 1/3, and the "uniform input" capacity is 1/3.[2] Plainly, there is very little to be gained by choosing the optimal (rather than uniform) channel input distribution!

What happened in this example can perhaps be expected to happen in general. A theorem of Silverman and Rumsey [25][18, p. 70] says that for any memoryless binary-input, binary output DMC, the ratio of the uniform input capacity to the true capacity is a least $(e/2)$ ln 2 = 0.9421. Shulman [24] has recently proved that the same is true for an arbitrary binary-input DMC. Thus one can expect performance of at least 94% capacity with turbo-like codes on any binary input channel, symmetric or not.

If, however, one insists on rates arbitrarily close to capacity, it will be necessary to adopt a modified strategy. This is the subject of Section 5.

5. An Old Theorem of Gallager.

I believe that *binary* turbo-like codes, with their scalar message-passing decoding algorithm, can be used effectively on arbitrary *q-ary* input memoryless channels. I base this belief in part on an old result of Gallager [12, Section 6.2], who showed that one could, in principle, use binary linear codes to achieve capacity on an arbitrary discrete memoryless channel. Gallager's method is to convert the stream of bits output by the binary encoder into a sequence of symbols from the DMC's input alphabet by means of an abstract "mapper." We illustrate the idea in Figure 6 (Cf. Gallager [12, Fig. 6.2.1]).

[2] The actual values are p^*=0.4859 and p^*_0 =0.4726.

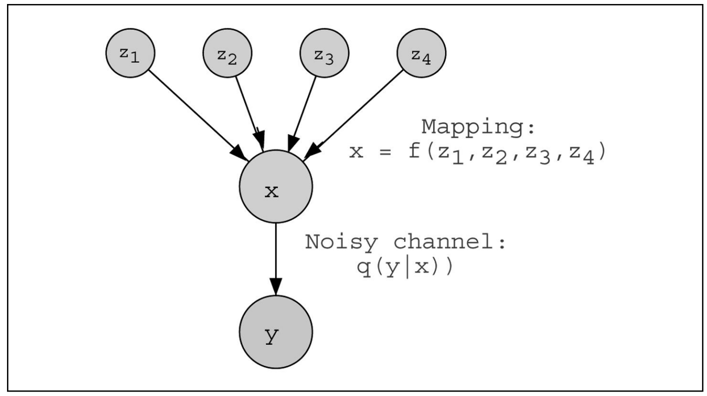


Figure 7. Bayesian Network For a 4:1 Mapper.

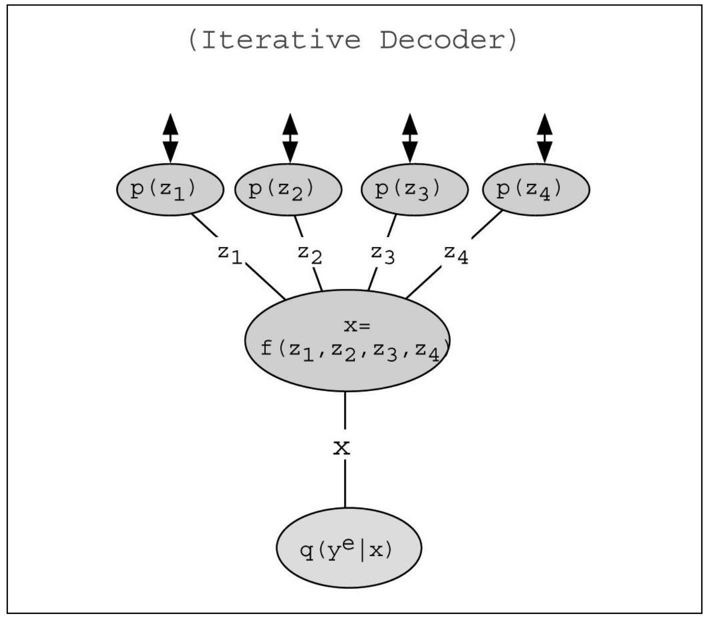


Figure 8. The Junction Tree For a 4:1 Mapper.

Here it is assumed the channel has three input symbols a, b, and c, and that the capacity-achieving input distribution is (1/3, 1/3, 1/3). The mapper maps each of the eight blocks of three code bits into one of the three channel input symbols, as shown. In this way, the original binary code becomes a ternary code, in which the symbols occur with probabilities (3/8, 3/8, 2/8), which is a reasonably good approximation to (1/3, 1/3, 1/3). By elaborating on this simple idea, Gallager was able to prove that the ensemble of codes of the form described in Figure 6 could be used to prove the coding theorem. In conclusion, Gallager wrote:

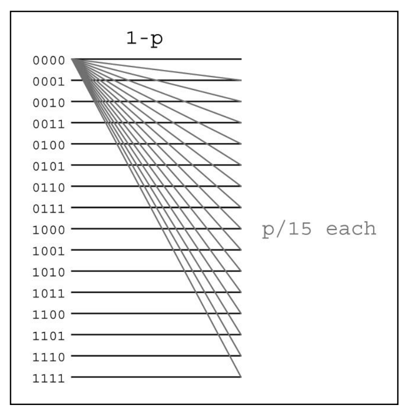


Figure 9. 16-ary Symmetric Channel.

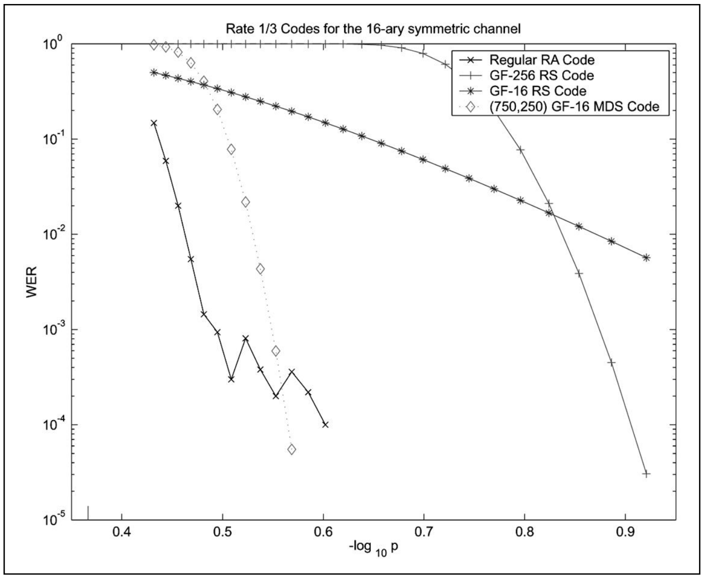


Figure 10. An Experiment on the 16-ary Symmetric Channel (R =1/3, k =1000).

> "...we have demonstrated a simple [encoding] algorithm by which codewords can be generated in such a way as to approximately achieve the results of the coding theorem. *Unfortunately, the problem of finding decoding algorithms is not so simple.*" (Emphasis added.)

Our hope is that the problem of finding decoding algorithms can be solved by replacing the generic binary encoder in Figure 6 with a "turbo-like" encoder, and by combining the demodulation process with the iterative message-passing decoding algorithm for the turbo-like code. We briefly illustrate this by considering a simple 4:1 mapper, shown in the form of a Bayesian network [21, Chapter 3], in Figure 7.

By an application of Bayes' rule [21, Chapter 4], we have the following formula for the *a posteriori* probability distribution of the random variable Z_n after Y has been observed to have the value y^e (there is a similar formula for each of Z_1, Z_2, Z_{n-1}):

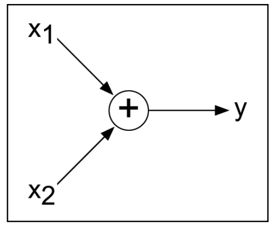


Figure 11. The Binary Adder Channel.

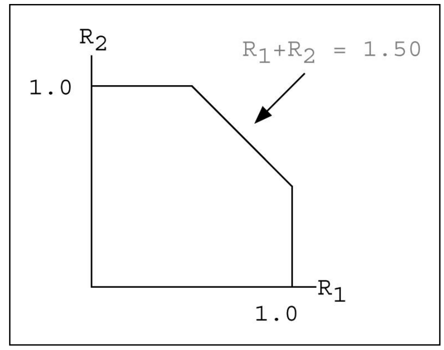


Figure 12. The Capacity Region for the BAC [3, Chapter 14].

$$\text{(5.1)}\quad \Pr\left\{Z_n = a \middle| Y = y^e\right\} = \alpha p_n(a) \times \sum_{\substack{z_1,\ldots,z_{n-1}\in\{0,1\}^{n-1} \\ x=f(z_1,\ldots,z_{n-1},a)}} p_1(z_1)\cdots p_{n-1}(z_{n-1})\,q\left(y^e|x\right),$$

where α is a constant determined by the formula $\Pr\left\{Z_n = 0 \middle| Y = y^e\right\} + \Pr\left\{Z_n = 1 \middle| Y = y^e\right\} = 1.$

We can use (5.1) to make the needed modifications to the iterative sum-product algorithm. One way is to use the methodology of [1], in which the Bayesian network of Figure 7 is converted into a "junction tree," as shown in Figure 8. The junction tree represents a message-passing device that acts as an intermediary between the nonbinary channel evidence y^e and the binary iterative decoder. After each iteration of the binary decoder, the junction tree updates the log-likelihood ratios based on the evidence y^e provided by the channel about each block of four binary code bits. In the next section we will describe a numerical experiment using the general ideas of this section.

6. A Nonbinary Experiment.

Figure 9 shows a 16-ary symmetric channel, with symbol error probability p. If we want to communicate reliably on this channel using binary codes, then the obvious mapping (cf. Figure 6) is to use four bits to represent each 16-ary channel symbol. If the rate of the binary code is R_0, then since the mapper groups the binary code bits into sets of 4, the overall code rate is $R = 4R_0$ bits per channel input symbol. We chose binary rate $R_0 = 1/3$ (overall rate $R = 4/3$) for our experiment; in particular, a rate 1/3 (regular) RA code with k =1000 information bits. The resulting decoded word error rate is shown in Figure 10, compared to the

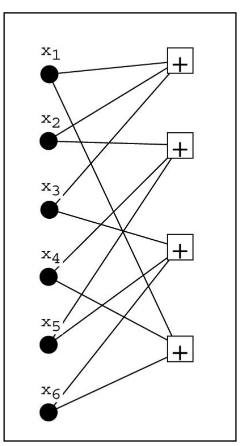


Figure 13. A Tanner Graph for a (2,3) LDPC Code.

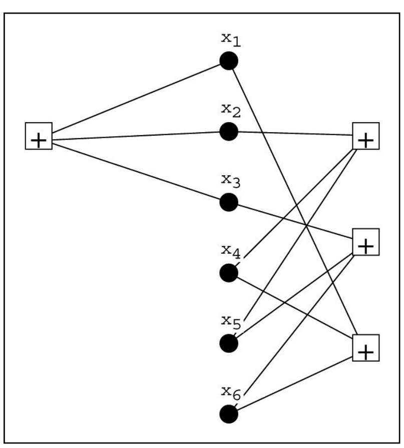


Figure 14. Splitting the Graph (I).

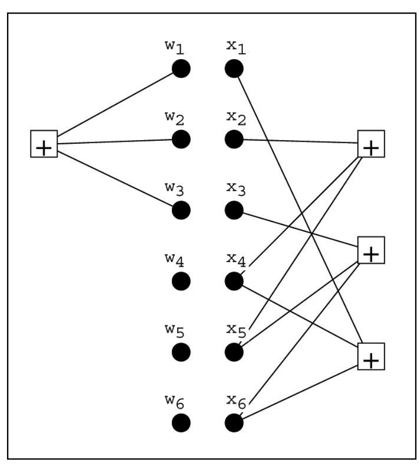


Figure 15. Splitting the Graph (II).

Shannon limit (the tick mark on the horizontal axis at p = .430206, i.e., $-\log_{10}(p)$ = .446684). Also shown in Figure 10 is the performance of two R = 1/3 Reed-Solomon codes: a (15, 5) code over $GF(16)$, and a (255, 85) code over $GF(2^8)$. Finally, Figure 10 also shows the "performance"of a non-existent (750, 250) MDS code over $GF(16)$, assuming bounded distance decoding. Note that the performance of the binary RA code is near the Shannon limit, superior to the RS codes, and comparable to the mythical MDS code.

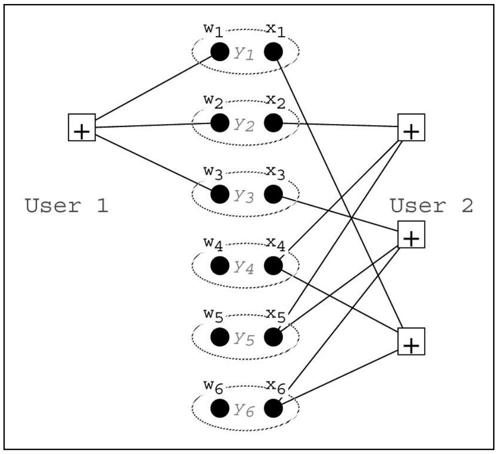


Figure 16. A Tanner Graph for a Multiaccess LDPC Code.

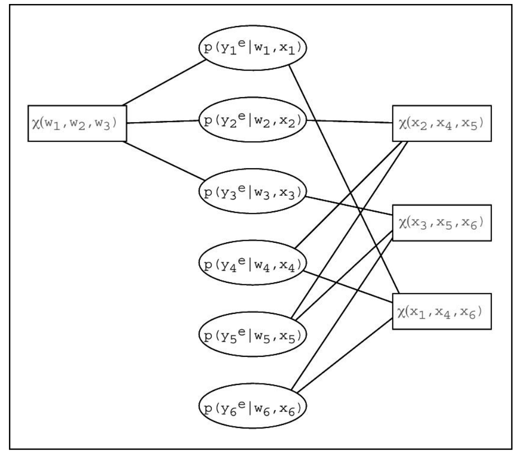


Figure 17. The Corresponding Junction Graph.

Based on this limited evidence, we suggest that binary turbo-like codes are good candidates for near Shannon limit performance on nonbinary channels, at least if the channels are symmetric. In particular, turbo-like codes look like they may soon provide strong competition for Reed-Solomon codes in storage applications. (Another successful application of binary turbo-like codes to symmetric nonbinary channels, is to the two-dimensional AWGN channel with high-order signal constellations [5].)

In the next section we will investigate the possibility of using turbo-like codes on multiaccess channels.

7. Multiaccess channels.

A Multiple Access Channel (MAC) is a channel in which two or more senders send information to the same receiver. In these channels, the senders must not only contend with the receiver noise, but also interference from each other. Stating this observation mathematically: a (two-input memoryless) MAC has 2 inputs (x_1, x_2) and produces an output y according to a probability transition matrix $p(y|x_1, x_2)$, i.e., the output is a probabilistic function of all the inputs.

A simple example of a MAC is the Binary Adder Channel (BAC) (see Figure 11). This channel has binary inputs $x_1, x_2 \in \{0, 1\}$ and a ternary output $y = x_1 + x_2$ where the addition is over the real field. The capacity region of the BAC is shown in Figure 12, which tells us that it is theoretically possible to achieve a joint rate of $R_1 + R_2 = 1.5$ bits per channel use, provided $R_1 \le 1$ and $R_2 \le 1$. How can we do this practically, using turbo-like codes? One possible way is shown in Figures 13 –17.

In Figure 13, we see the Tanner graph for "(2, 3)" regular LDPC code. There are 6 variable nodes and 4 check nodes, so the code rate is 1/3. To adapt the code for use on the BAC, we need to "share" the check nodes between the two users. In Figure 14 we have assigned one of the check nodes to the first user,and the remaining three to user 2. Then in Figure 15, by a sort of mitosis, each of the variable nodes becomes a a pair, one for each user. In this way, the original single-user LDPC

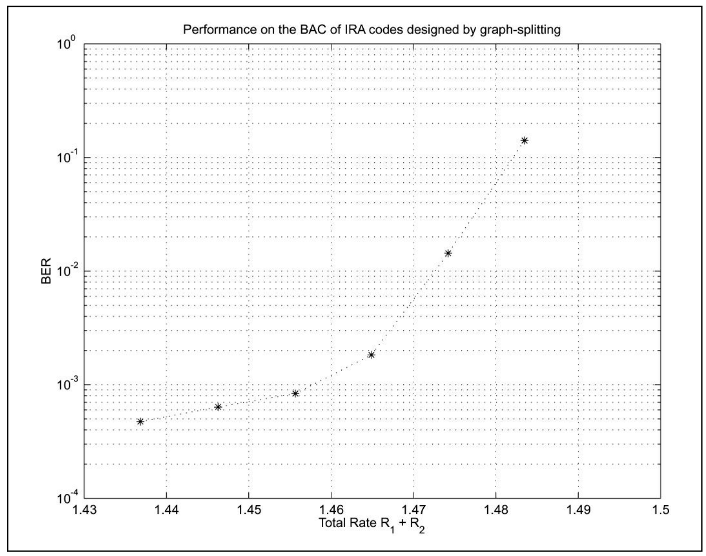


Figure 18. Experimental Results Based on Graph Splitting.

code becomes a two-user code with R_1 = 5/6 and R_2 = 1/2 suitable for use on the BAC (Figure 16). Then if (w_1,...,w_n) is the codeword sent by user 1, and (x_1,...,x_n) is the second user's codeword, these codewords are received jointly as (y_1,...,y_n). The decoder's job is then to infer the values of the w_i's and the x_i's based on the evidence provided by the y_i's. Using the junction graph shown in Figure 17, and the methodology of the generalized distributive law ['AM001'], it is then a routine matter to devise an iterative decoding algorithm for the BAC.

In an experiment whose details are reported in [20], we used irregular repeat accumulate (IRA) codes [14] to test our graph-splitting code design and decoding algorithm on the BAC. (IRA codes are similar to LDPC codes, but have the advantage that they can be encoded in linear time.) We used IRA codes of length k = 10000 and constant right-degree 5. The simulations show that the decoder probability of error does not depend on the individual R_1 and R_2, but only on the joint rate $R_1 + R_2$, i.e., it depends only on the graph and not the way it is split. The numerical results are shown in Figure 18.

It is tempting to conjecture that this simple graph-splitting technique will be effective on more general multiple access channels, but unfortunately this is not the case, as will be reported in [20]. The problem can be seen in Figure 15, where three of user 1's message bits are left completely unprotected. The special nature of the BAC allows the code to recover from this anomaly, but for a general MAC, it is clear that modifications will be needed.

8. Conclusions.

This paper has two messages:

- On "standard" channel models, i.e., SBIC's, Shannon's problem has effectively been solved, though there do remain some thorny theoretical and implementational issues.
- On "nonstandard" models, it looks as though binary turbo-like codes will ultimately solve Shannons' problem, especially if graph-based iterative decoding is used. Applications to nonbinary (storage) channels and multiuser channels look especially ripe for further work.

Finally, I should mention that another kind of nonstandard channel model is a channel with *memory*. Although I have not discussed applying turbo-like codes to channels with memory in this paper, there has been a lot of impressive work done in this area [13]. Again, iterative message-passing on the appropriate graphical model is the key.

Acknowledgements.

I was assisted immeasurably in the preparation of this paper (and the talk on which is is based) by my students Aamod Khandekar and Ravi Palanki (see refs. [10] and [20] for proof).

References.

1. S.M. Aji and R.J. McEliece, "The generalized distributive law," *IEEE Trans. Inform.Theory*, vol. IT-46 (March 2000), pp. 325–343.

2. S.-Y. Chung, G.D. Forney, Jr., T.J. Richardson, and R. Urbanke, "On the design of low-density parity-check codes within 0.0045 dB of the Shannon limit," *IEEE Comm.Letters* vol. 5 (Feb. 2001), pp.58–60.

3. T.M. Cover and J.A. Thomas, *Information Theory*. New York: Wiley, 1991.

4. D. Divsalar, S. Dolinar, and F. Pollara, "Low-complexity turbo-like codes," pp.73–80 in Proc. *2nd International Symposium on Turbo Codes and Related Topics*, Brest France, Sept. 2000.

5. D .Divsalar and F. Pollara, "Turbo trellis coded modulation with iterative decoding for mobile satellite communications, "Proc. International Mobile Satellite Conference, June 1997.

6. D. Divsalar, H. Jin, and R.J. McEliece, "Coding theorems for 'turbo-like' codes," pp. 201–210 in *Proc. 36th Allerton conf. on Communication, Control, and Computing*. (Allerton, Illinois, Sept. 1998.)

7. G.D. Forney, Jr., *Concatenated Codes*.Cambridge, Mass.: MIT Press, 1966.

8. B.J. Frey and D.J.C. MacKay, "Irregular turbo-like codes," pp. 67–72 in *Proc. 2nd International Symposium on Turbo Codes and Related Topics*, Brest France, Sept. 2000.

9. A. Khandekar and R. McEliece, "On the complexity of reliable communication on the erasure channel," Proc. ISIT 2001, p. 1.

10. A. Khandekar and R. McEliece, "Are turbo-like codes effective on non-standard channels?," Proc. 6th Int. Symp. Comm.Theory and Appl. (Ambleside, UK, July 2001), pp. 293–298.

11. R.G. Gallager, *Low Density Parity-Check Codes*. Cambridge. Mass.: MIT Press, 1963.

12. R.G. Gallager, *Information Theory and Reliable Communication*. New York: John Wiley and Sons, 1968.

13. *Iterative Decoding for Channels with Memory*, pp. 70–74 in Proc. ISIT 2001. (Session MOd. 1)

14. H. Jin, A. Khandekar, and R. McEliece, "Irregular repeat-accumulate codes," pp. 1–8 in *Proc. 2nd International Symposium on Turbo Codes and Related Topics*, Brest France, Sept. 2000.

15. M.G. Luby, M. Mitzenmacher, M.A. Shorrollahi, and D.A. Spielman, "Effcient erasure correcting codes," *IEEE Trans. Inform. Theory*, vol.47 (Feb. 2001), pp. 569–584.

16. M.G. Luby, M. Mitzenmacher, M.A. Shorrollahi, and D.A. Spielman, "Improved low-density parity-check codes using irregular graphs," *IEEE Trans. Inform. Theory*, vol. 47 (Feb. 2001), pp. 585–598.

17. D.J.C. MacKay, "Good error-correcting codes based on very sparse matrices." *IEEE Trans. Inform. Theory*, vol. 45 (March 1999), pp. 399–431.

18. E. Majani, *A Model for the Study of Very Noisy Channels, and Applications*. Caltech Ph.D. thesis, 1988.

19. P.C. Massey and D.J. Costello, Jr., "New developments in asymmetric turbo codes," pp. 93–100 in *Proc. 2nd International Symposium on Turbo Codes and Related Topics*, Brest France, Sept. 2000.

20. R. Palanki, A. Khandekar, and R.J. McEliece, "Graph based codes for synchronous multiple access channels," submitted to Allerton 2001.

21. J. Pearl, *Probabilistic Reasoning in Intelligent Systems*. San Francisco: Morgan Kaufmann, 1988.

22. Li Ping, W.K. Leung, and K.Y. Wu, "Very low rate turbo-Hadamard codes," Proc. 6th Int. Symp. Comm. Theory and Appl. (Ambleside, UK, July 2001), pp. 310–315.

23. L. Ping and K.Y. Wu, "Concatenated tree codes," pp. 161–164 in *Proc. 2nd International Symposium on Turbo Codes and Related Topics*, Brest France, Sept. 2000.

24. N. Shulman, "Universal encoding—the prior problem," preprint dated June 26, 2001.

25. R. Silverman, "On binary channels and their cascades," *IRE Trans. Inform. Theory*, vol. IT-1 (December 1955), pp. 19–27.

26. S. ten Brink, "Design of serially concatenated codes based on iterative decoding convergence," pp. 319–322 in *Proc. 2nd International Symposium on Turbo Codes and Related Topics*, Brest France, Sept.2000.

27. S. ten Brink, "Code doping for triggering iterative decoding convergence," *Proc. ISIT 2001*, p. 235

A Juggler's Tribute to Claude Shannon

By Professor Arthur Lewbel

March, 2001.

Claude Elwood Shannon 1916-2001. Survived by his wife Mary Elizabeth (Betty) Shannon, a son, Andrew Shannon, and a daughter, Margarita "Peggy" Shannon.

Among the many branches of mathematics and science that Claude Shannon essentially invented, the least well known may be the science of juggling. In 1990, Scientific American called Claude's paper on information theory, "The Magna Carta of the Information Age," but among jugglers, Claude is better known for having invented the first juggling robot. For jugglers, "Shannon's theorem" refers to an equality he derived regarding the timing of throws and catches in juggling patterns.

Any encyclopedia will provide a short biography of Claude's life, and thousands of books, articles, and webpages exist describing his work in mathematics and computer science. I will therefore skip most of that, and instead provide my own recollections and impressions of an extraordinary man.

Shannon with his juggling toys.

Occasionally, the juggling and information theory sides of Claude's life came together. In the 1980's Claude quietly showed up at a computer science lecture (after having been away from the field for many years). One attendee said, "It was as if Isaac Newton had showed up at a physics conference." When people realized who he was they pushed him on stage. He gave a very short speech, but then he juggled for the crowd. Afterwards, attendees lined up to get his autograph.

I first met Claude at the MIT Juggling club. One nice thing about juggling at MIT is that you never know who will show up. For example, one day Doc Edgerton, inventor of the strobe light, stopped by the juggling club and asked if he could photograph some of us juggling under strobe lights. So it wasn't a great surprise when a cheerful, gray haired professor stopped by the club one afternoon and said to me, "Can I measure your juggling?" That was my introduction to Claude Shannon.

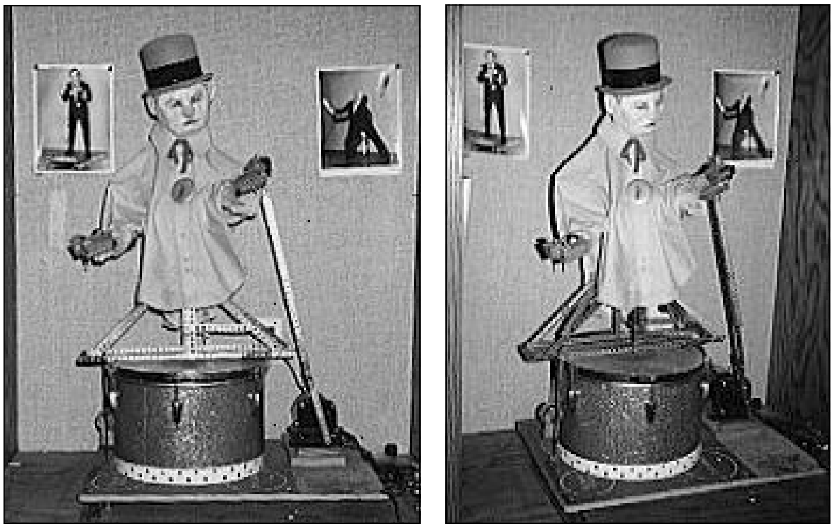
Not long after, the MIT juggling club decided to have a video and pizza night, and needed someone with a big TV, in a room large enough to hold dozens of jugglers. We all ended up in Claude's living room, in a stately home (originally owed by Thomas Jefferson's great granddaughter) overlooking a lake in Winchester, Massachusetts. Another time he invited me to dinner at his house, saying only that, "he had another juggler coming over as well." The other guest turned out to be Albert Lucas.

Unlike most brilliant theoretical mathematicians, Claude was also wonderfully adept with tools and machines, and frequently built little gadgets and inventions, usually with the goal of being whimsical rather than practical. "I've always pursued my interests without much regard to financial value or value to the world. I've spent lots of time on totally useless things," Shannon said in 1983. These useless things would include his juggling robot, a mechanical mouse that could navigate a maze, and a computing machine that did all its calculations in roman numerals.

Claude never did care about money. He never even put his paycheck into a bank account that paid interest, until he married and his wife Betty suggested it to him. Still, he became a very wealthy man, partly as a result of early investments with some of his computer scientist pals, including the founders of Teledyne and of Hewlett Packard. When he did think about finance, Claude was as brilliant at that as with anything else he set his mind to. Knowing I was an economist, he once explained to me his thoughts on investing. Some were wonderfully practical, as when he said he'd always buy stocks rather than gold, because companies grow and metals don't. Some were more esoteric, for example, he had ideas regarding mean-variance analysis that jibe well with many aspects of modern portfolio theory.

Some of the juggling artifacts that Claude had in his large 'toy room:' A zoetrope made of a dozen little still figures of juggling clowns. Spin it, and they look like one clown juggling. A sculpture of a juggler, juggling 3 jugglers, each of whom is juggling three jugglers. His famous juggling robot, complete with the head of W. C. Fields stuck on top. A mechanical diorama that shows three clowns, juggling many balls rings and clubs. The props move so realistically that the clubs even rotate and land correctly (triple spins, if I remember right). In the basement was an air hockey table, mounted at an angle, for two dimensional, low gravity juggling. And in the garage, a collection of exotic unicycles.

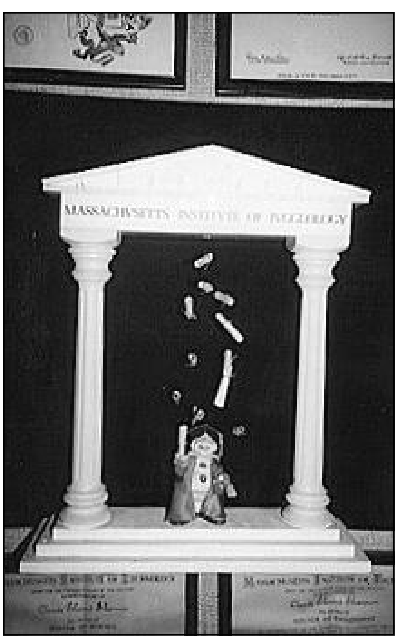
Note: excerpts of this tribute appeared in the May/June 2001 issue of 'Juggle' magazine. Reprinted by permission.



Two pictures of Claude Shannon's W. C. Fields juggling machine.

In addition to his famous juggling theorem, Claude came close to inventing site swaps. In the 1970's, he was asked by Scientific American magazine to write an article about juggling. In addition to including his juggling theorem, the draft of his article contained an attempt to count the number of different possible juggling patterns. Scientific American asked him to revise the article, but by then he was doing other things and never bothered to finish it. (A copy of his draft article can be found in the book, "Claude Elwood Shannon Collected Papers," edited by N.J.A. Sloane and A. D. Wyner, New York, IEEE Press, 1993, pages 850-864). He made an offhand remark that maybe I should write an article for them instead. Years later, I took his advice (see, "The Science of Juggling, Scientific American, Nov. 1995).

Claude told me this story. He may have been kidding, but it illustrates both his sense of humor and his delightfully self deprecating nature, and it certainly could be true. The story is that Claude was in the middle of giving a lecture to mathematicians in Princeton, when the door in the back of the room opens, and in walks Albert Einstein. Einstein stands listening for a few minutes, whispers something in the ear of someone in the back of the room, and leaves. At the end of the lecture, Claude hurries to the back of the room to find the person that Einstein had whispered too, to find out what the great man had to say about his work. The answer: Einstein had asked directions to the men's room.

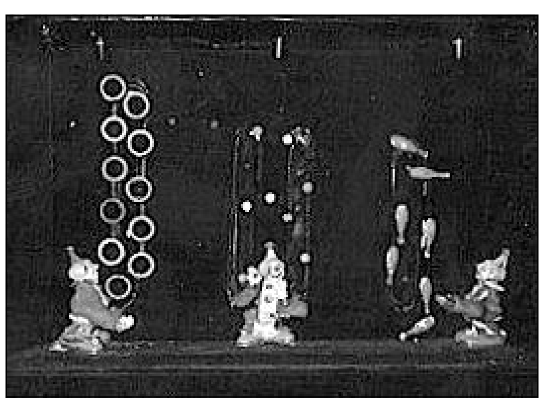


The Massachussetts Institute of Juggliology

Claude wrote the first paper describing how one might program a computer to play chess. He wrote, "Communication Theory of Secrecy Systems, " which the Boston Globe newspaper said "transformed cryptography from an art to a science." Yet neither one of these were his greatest works.

Here's my own interpretation of Claude's two most famous and important papers. His 1937 thesis basically said, "if we could someday invent a computing machine, the way to make it think would be to use binary code, by stringing together switches and applying Boole's logic system to the result." This work, done while he was still a student at MIT, has been called the most important master's thesis of the twentieth century. The idea was immediately put to use in the design of telephone switching systems, and is indeed how all modern computers think.

But that was only Claude's second most important idea. His most famous paper, written in 1948 at Bell Labs, created what is now known as information theory. In "A Mathematical Theory of Communication," Shannon proposed the idea of converting any kind of data, (such as pictures, sounds, or text) to zeroes and ones, which could then be communicated without errors. Data are reduced to bits of information, and information transmission is then measured in terms of the amount of disorder or randomness the data contains (entropy). Optimal communication of data is achieved by removing all randomness and redundancy (now known as the Shannon limit). In short, Claude basically invented digital communication, as is now used by computers, CD's, and cell phones. In addition to communications, fields as diverse as computer science, neurobiology, code breaking, and genetics have all been revolutionized by the application of Shannon's information theory. Without Claude s work, the internet as we know it could not have been created.



Shannon's juggling diorama

Some of Claude's honors include the National Medal of Science, Japan's Kyoto Prize, the IEEE Medal of Honor, and about a dozen honorary degrees. In 1998, the two building AT&T labs complex in Florham Park, N.J., was named the Shannon Laboratory.

One day, almost immediately after I'd arrived at his house, Claude said to me, "Do you mind if hang you upside down

The zoetrope in Shannon's toy room.

by your legs?" He had realized that while bounce juggling is much easier than toss juggling in terms of energy requirements, throwing upward as in toss juggling is physiologically easier, and so he wanted to try combining the two, which meant bounce juggling while hanging upside down.

For every one invention he built or theorem he proved, he had a hundred other ideas that he just never got around to finishing. One juggling example: He showed me a vacuum cleaner strapped to a pole, pointing straight up, with the motor reversed to blow instead of suck. He turned it on, and placed a styrofoam ball in the wind current. It hovered about a foot above the vacuum. He then varied the speed of the motor, and the ball drifted up and down as the speed changed. "Now," he said, "Imagine three balls and two blowers, with the blowers angled a bit towards each other, and the motors timed to alternate speeds."

The last time I saw Claude, Alzheimer's disease had gotten the upper hand. As sad as it is to see anyone's light slowly fade, it is an especially cruel fate to be suffered by a genius. He vaguely remembered I juggled, and cheerfully showed me the juggling displays in his toy room, as if for the first time. And, despite the loss of memory and reason, he was every bit as warm, friendly, and cheerful as the first time I met him. Billions of people may have benefited from his work, but I, and thousands of others who knew him a little bit, are eternally grateful to have known him as a person.

"Shannon's juggling theorem" and "Shannon's juggling robot" below reprinted with permission from The Science of Juggling, By Peter J. Beek and Arthur Lewbel, Scientific American, November, 1995, Volume 273, Number 5, pages 92-97. Copyright (c) 1995 by Scientific American, Inc. All rights reserved. The entire Science of Juggling article (except for some copyrighted photos) may be found here: The Science of Juggling.

Claude Shannon's wife, Betty, in the toy room of Shannon's home.

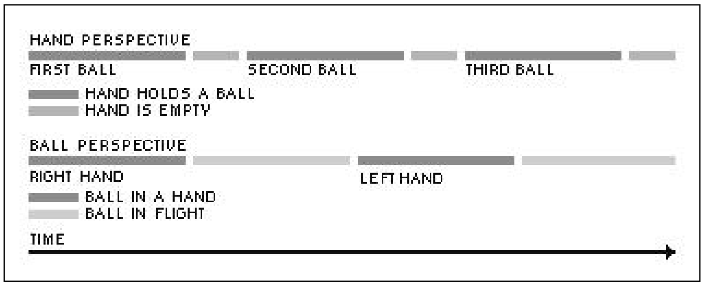
Shannon's juggling robot.

Shannon pioneered juggling robotics, constructing a bounce-juggling machine in the 1970s from an Erector set. In it, small steel balls are bounced off a tightly stretched drum, making a satisfying "thunk" with each hit. Bounce juggling is easier to accomplish than is toss juggling because the balls are grabbed at the top of their trajectories, when they are moving the slowest.

In Shannon's machine, the arms are fixed relative to each other. The unit moves in a simple rocking motion, each side making a catch when it rocks down and a toss when it rocks up. Throwing errors are corrected by having short, grooved tracks in place of hands. Caught near the zenith of their flight, balls land in the track; the downswing of the arm rolls the ball to the back of the track, thus imparting sufficient energy to the ball for making a throw. Shannon's original construction handled three balls, although Christopher G. Atkeson and Stefan K. Schaal of the Georgia Institute of Technology have since constructed a five-ball machine along the same lines.

Shannon's juggling theorem

JUGGLING THEOREM proposed by Claude E. Shannon of the Massachusetts Institute of Technology is schematically



represented for the three-ball cascade. The exact equation is (F+D)H=(V+D)N, where F is the time a ball spends in the air, D is the time a ball spends in a hand, V is the time a hand is vacant, N is the number of balls juggled, and H is the number of hands. The theorem is proved by following one complete cycle of the juggle from the point of view of the hand and of the ball and then equating the two.

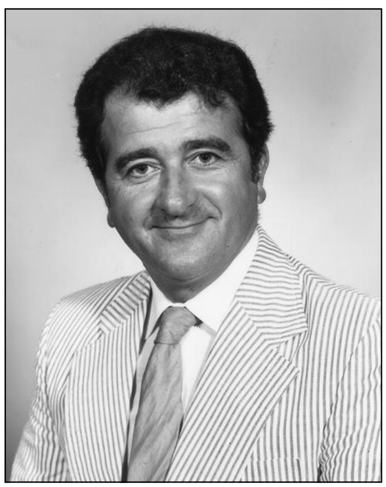
Arthur Lewbel, a professor of Economics at Boston College, co-authored, "The Science of Juggling," Scientific American, 1995, among other works on Juggling (see http://www2.bc.edu/~lewbel/). He founded the MIT Juggling Club, and can juggle up to eight balls.

Historian's Column

A. Ephremides

This column is being written under the dark shadow of the horrific events of September 11, 2001. Their momentous impact could not but affect also the focus of this column. So, I tried to think how, in the past, our Society has been affected by other events of terror, war, and calamity that have similarly transgressed the boundaries of freedom and peace.

One of the first and dominant ones has been of course the Cold War. For several decades since the founding of Information Theory, the conflict between the United States (and its allies) and the Soviet Union (and its allies), or between free economies and communism, dominated the sources of discomfort for our Society. The invitations of scientists from one side to meetings held in the other side were marred by visa disputes, mechanisms of selection, transparency of procedures, etc. For those who find the meetings of our Board of Governors dull and unexciting nowadays, should have been around in the early seventies, when heated discussions, that rode the fine line between scientific matters and world politics, drove the meetings into the wee hours of the morning. The 1975 workshop in Moscow (preceded by the USSR Symposium in Tallinn, Estonia in 1973), and the on-and-off contacts between the two sides until the biannual Swedish-USSR workshops from 1985 to 1991 punctuated the efforts of researchers from both sides to overcome the heavy obstacles of political pressure.



A. Ephremides

But this was, by far, not the only instance of our Society being embroiled in the whirlwind of world events. In 1967, the International Symposium on Information Theory was scheduled to take place in Athens, Greece. In April of 1967 a gang of caricature colonels staged a coup in Greece, however, and installed a dictatorship that lasted until 1974 and threw the country into one of its blackest periods of the 20th century. Our Society stood up to the challenge and moved the symposium to San Remo, Italy, with remarkable fortitude and swiftness. The accomplishment (performed without the acceleration benefits of the Internet) was stunning and indicative of the resourcefulness of our members.

Many of us remember that the Middle East conflict flared up in 1973 with the Yom Kippur war. Yet, in June 1973 our Symposium was held in Ashkelon, Israel, and, later on, in 1984, an Information Theory workshop was held in Caesaria, Israel. On both instances, our meetings went on completely unmarred by the heaviness that surrounded the region and by the potential for catastrophic events. Perhaps Information Theorists were too exotic a target for terrorist attacks. However, the meticulous security precautions of the Israelis were perhaps the real reason. I still remember when I was leaving Israel in 1973 and was being checked and interviewed by security personnel at the airport. I admit guiltily that I was a cigarette smoker at the time. So much so, that I was carrying two cartons of Marlboros in my hand luggage. The cheerful, and incredibly youthful, interviewer opened up each carton, proceeded to open up cigarette pack (twenty in total) and carefully examined one cigarette from every pack! I was truly amazed. Maybe because of this, for those who care to know, I ended up smoking my last cigarette on Friday, January 27, 1978 at around 5 pm!

There were frequent debates concerning the safety and wisdom of holding meetings in various "hot-spots" around the world. Some of you (rather few) know that we had serious plans of holding a workshop in Nepal in 2002. Unfortunately, the plans were cancelled after the massacre that took place in the royal court of Nepal about a year ago. And wisely so, since the situation has progressively deteriorated in that country.

But we braved various milder threats (like crime incidence, inaccessibility, or uncertainty) and held workshops in Salvador, Brazil, in Killarney, Ireland, in Kruger Park, South Africa, in Longyearbyen, Svalbard (at 80 degrees North!), in Metsove, Greece (just 50 km south of the Albanian border), and in Sante Fe, New Mexico (at 7000 ft of altitude!).

The adventuresomeness of our group took as to China during the evocative period that preceded the famous Tian An Men Square massacre and to Cairns, Australia, just a few months ago.

Who knows what the future will bring? Who knows what world events will bear an impact on our activities? Perhaps the best (indirect) defiance of the workings of fate is to continue planning and executing our meetings, contacts, and exchanges with a healthy disregard for fear, but with a measure of common sense. During the summer of 1974, as the dictatorship in Greece collapsed, Turkish forces invaded Cyprus, and a general mobilization of armed forces was taking place on both sides of the Aegean, I proceeded with my plans that included attending some memorable opera performances in Verona, Italy, and then getting married in Athens, Greece. My honeymoon in Corfu overlapped with the few days of warfare on Cyprus and with general turmoil on Greece. Yet, I enjoyed the uncrowded hotels, the empty airports, and the excitement of matching the unfolding of momentous world events, while, at the same time, trying to get to know my spouse (of twenty-seven years by now!). Perhaps I was lucky to emerge unscathed from that boiling pot. But what is the choice?

IEEE Information Theory Society Annual Meeting

Omni Shoreham Hotel, Washington, DC
Sunday June 24, 2001

Aaron Gulliver

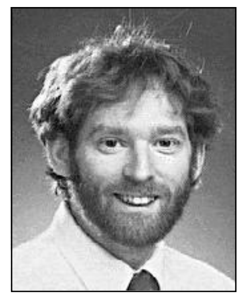
Attendees: Erik Agrell, John Anderson, Tom Cover, Michelle Effros, Anthony Ephremides, Marc Fossorier, Thomas E. Fuja, Aaron Gulliver, Joachim Hagenauer, Al Hero, Michael Honig, Hideki Imai, Torleiv Kløve, Ryuji Kohno, Bob McEliece, Steven W. McLaughlin, Lance C. Pérez, Nela Rybowicz, Bixio Rimoldi, Paul H. Siegel, Alexander Vardy, Han Vinck, Stephen B. Wicker, Raymond Yeung

1. The meeting was called to order at 12:30 PM by Society President Joachim Hagenauer. The members of the Board were welcomed. The new Newsletter Editor, Lance C. Pérez, was introduced. IEEE Editor, Nela Rybowicz, and Signal Processing Society Treasurer, Al Hero, were also welcomed to the meeting. The Agenda was approved as distributed.

2. The minutes of the previous meeting held in Baltimore, MD on March 23, 2001, were approved as distributed.

3. Society President Joachim Hagenauer reviewed the correspondence and events regarding the passing of Claude Shannon. He noted that an obituary written by Bob Lucky was published in IEEE Spectrum. Tom Fuja announced that as part of ISIT 2001, a commemorative session would be held today at 5:00 PM and a moment of silence will be observed before the Shannon Lecture on Thursday. The President attended the TAB meetings as representative for the IT society. He made a 10 minute presentation on the Society at the meeting in New Brunswick, NJ. A review of this presentation was made to the board. There are presently 5980 members (320 Fellows), which represents a 4.7% increase.

   He stated that the IEEE would like the IT Society to publish a magazine. Although this was viewed as desirable, given our current financial situation, it is not possible at present. Al Hero (Treasurer of SP Society) said that the Signal Processing Magazine just breaks even.



Aaron Gulliver

   The society currently has two major problems. The first is the financial situation. Joachim read a letter to the IEEE President dated May 10 which contained the message approved at the Baltimore BOG meeting. There has been no reply as yet. This was followed by a long debate about the relationship between IEEE and the Societies, and the control of Society finances. The perception is that IEEE uses the Societies as a financial resource, and would rather do this than increase fees. It was noted that the IEEE appears to be too active in money making ventures, and has not been fiscally responsible. It should concentrate more on providing services to the membership. An ad hoc Committee consisting of Marc Fossorier, Han Vinck, Stephen Wicker and Tom Fuja was created to investigate ways that the society can deal with IEEE corporate. The Society President thanked Marc Fossorier for his patience in preparing the 2002 budget.

   A questionnaire will be distributed during ISIT to obtain feedback on fees and services.

   The second major problem is the newsletter, which is now over 6 months behind in publication. A new Editor has been appointed, and the situation will be cleared up soon.

4. Marc Fossorier gave an overview of the current financial status of the society. He noted that it is difficult to deal with IEEE, budget targets move according to their objectives and they have unusual financial practices. They

have control over the society money, and can exert pressure on the societies because of this. In 2000, $165K was withdrawn from the Society reserves to cover IEEE infrastructure development expenses. Ways to gain some control over society finances were discussed.

The IEEE has a freeze on new staff and new initiatives. Tom Fuja stated that IEEE Conference Services had been chosen for ISIT 2001. The organizers have not been satisfied with their performance, due largely to inexperience and high staff turnover.

The rising editorial costs for the Transactions were discussed. One solution is to hire an administrator to oversee the paper correspondence, however this eliminates much of the interaction between the associate editors and the reviewers. Al Hero indicated that the same situation arose in the Signal Processing Society, and their solution was to hire an editorial assistant. It was decided that the Editor-in-Chief and Treasurer will develop some guidelines for editorial costs.

A motion was made to reduce the number of Transactions issues from 13 to 12. This will balance the workload of publications staff. The motion was approved unanimously.

5. Aaron Gulliver presented the report on the IT Society website. He stated that the December Newsletter (and those since Summer 1998) are available as PDF files. File transfer volume on the website is up 100% from the last report in March. The number of file transfers is up 30% to 1225/day, amounting to 35 MB/day. Much of this increase is due to newsletter downloads. Access this year has been from 82 countries.

   The age and organization of the website was reviewed, and a case made for updating the structure and format. A motion to spend $5,000 to hire a web designer was approved by the board.

6. Lance Pérez presented the Newsletter Editor's Report. The March issue has been compiled, and this will be the last with Kim Wasserman as Editor. The June issue will be a minimal one to reduce publication time, and it is now nearly complete. The deadline for the September issue is July 23, and October 15 for the December issue. Input from the ISIT 2001 Shannon and Plenary speakers has been requested for the September issue. The President thanked Lance for taking on the job of Newsletter Editor at very short notice, and for his prompt attention which will soon eliminate the publication delay.

7.1. The Transactions Report was given by Alexander Vardy and Paul Siegel. Publication of the January issue was delayed, but the July issue was out on time. A copy of the July issue was distributed at the meeting. Five new appointments to the Editorial Board were presented to the Board for approval: Jonathan J. Ashley, Coding Theory (replacing Ron M. Roth), Aleksandar Kavcic Detection and Estimation (replacing Joseph A. O'Sullivan), Leandros Tassiulas, Communication Networks (replacing Venkat Anantharam), Gérard Battail, At Large (replacing Thomas E. Fuja), and Bruce E. Moision, Publications Editor (replacing Ramesh Rao). The appointments were approved unanimously.

7.2. The growth in the size of the Transactions was discussed. The number of submissions this year is already 270, so the total for the year will exceed 500. Meanwhile, the acceptance rate is down to 46%. To account for this increase, the page budget has been raised to 3150. The Publications Editor, Erik Agrell, stated that the Transactions is projected to be more than 200-300 pages over budget this year, or approximately 8%. There is a penalty by the IEEE if the Transactions is outside ± 5% of the budget, which could amount to $30,000. The November issue could be shortened to fall within this window, but this will create a backlog and increase the average time to publication. The consensus of the board was to allow the budget to be exceeded this year.

8. Steven McLaughlin presented the Electronics Publications Committee Report. Deja Vu is being added to the Digital Library and there is also the possibility of producing a single CD version of the Transactions. Creating the Digital Library costs about $15,000 per year. At present the library is free for society members, and there was some discussion of charging for its use. It was decided to keep it free of charge for now. There has also been some discussion on adding the Transactions to IEEE Xplore.

8.1. Use of the ArXiv preprint server creates intellectual property issues, so there can be no official society endorsement. Members will be informed of this server in the Newsletter so they can make use of it.

9. There was no report from the ad hoc Committee on Education.

10. & 16. Han Vinck presented the Report from the ad hoc Committee on Membership Issues and the Membership and Chapters Committee. The members of the Membership and Chapters Committee have been chosen to provide global representation. At list of members is posted on the society website. To date, no requests have been received for free affiliate memberships. The decision on these requests by the Membership and Chapters Committee is final. Four new chapters have been established, Hong Kong, Brazil, Australia and Denmark. The Best Chapter Award has been created and TAB approval is now being sought.

   The Society no longer provides free memberships to Russians, but they can apply for free Affiliate memberships. A limit on the number of these memberships has been set at 20.

7. Society Secretary, Aaron Gulliver, presented the results of the Electronic Vote on Fees:

   (a) Increase the nonmember fee from $445 to $520.

   YES 24 NO 0

   (b) Increase the member fee from $15 to $30.

   YES 22 NO 2

Both items are therefore approved by the board. 24 of the 25 board members cast votes. It was noted that the member fee has not changed in six years. Marc Fossorier will write a rationale for these increases for inclusion in the September Newsletter.

12. A change to the Bylaws for the Paper Award was distributed to the board members prior to the Annual Meeting, as per the Society Constitution. After some discussion, two minor amendments to the revised wording were made. The final wording of the proposed changes to **Article VIII. Paper Award, Section 2**. is as follows:

    Section 2. *An open call for nominations to this award shall be published in the Newsletter.*

    By March 15, the chair of the Publications Subcommittee or designee shall forward to the First Vice President a list of at least nine articles, published in the previous calendar year, for the consideration of the Awards Subcommittee. Each nomination shall be accompanied by a statement outlining the contribution of the paper.

    The Awards Subcommittee shall take into account (a) all nominations submitted in response to the open call for nominations in the last two years; (b) the nominations supplied by the Publications Committee in the last two years; (c) any nomination that its members may want to submit for consideration.

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

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

    The changes were approved by the board.

13. Nominations for Society Officers for 2002 were made. The candidates for President, 1st VP and 2nd VP were approved. The Society President will conduct the voting in July.

14. A list of 12 candidates from the Nominations Committee for new Board Members was presented. In addition, Henrik Ferreira was nominated by the Board. The 13 candidates were approved unanimously.

15. Stephen Wicker presented the Report on Symposia and Workshops.

15.1. The 2001 Canadian Workshop on Information Theory was a success. There were 55 attendees during the 2 1/2 day event. A financial report is pending.

15.2. A report on ISIT 2001 was distributed. It was noted that there are a large number of travel grants this year, due largely to the surplus from ISIT 2000. The move to yearly symposia has resulted in fewer papers being submitted. Concern was raised about the high rejection rate ($\approx$ 40%) this year. In past years, the rejection rate has typically been in the 20% - 30% range. It was felt that there should be a policy/philosophy on the acceptance/rejection of papers.

15.3. It was reported that preparations for the 2001 Information Theory Workshop in Cairns, Australia are in great shape. The Board of Governors Meeting has been scheduled for Wednesday morning.

15.4. Bixio Rimoldi reported on ISIT 2002 in Lausanne, Switzerland. He stated that an excellent team has been assembled. The banquet will be held in the Olympic Museum. The costs are projected to be $180,000. An advance of $40,000 was approved unanimously by the board.

15.5. Alexander Vardy was informed by Vijay Bhargava that due to the current unrest in Nepal, the 2002 Information Theory Workshop cannot be held there. Since there is no alternative venue, the workshop was cancelled.

15.6. The ITG conference in Berlin is progressing as scheduled.

15.7. Ryuji Kohno reported on the organization of ISIT 2003. A new website has been created, and the Call for Papers will be distributed during ISIT 2001. Excursions and destinations were discussed. The proposed registration fee is $550.

15.8 There are no proposals for a 2003 Workshop.

15.9. There was no report on the proposed 2004 Symposium to be held in Chicago. A detailed budget is being prepared.

17. The Awards Subcommittee report was presented by Tom Fuja.

17.1 The joint COMSOC/IT paper award was discussed by the board, in particular the relationship between it and the IT Best Paper Award. Guidelines for selection were discussed, and these will be considered when the joint committee meets.

17.2 The report on the Paper Award by the Awards Subcommittee was distributed. Seventeen papers were nominated. Four rounds of balloting reduced the number of candidates to nine, six, three and finally two. The names of these final two papers and the rationale for their selection were previously distributed to the board members. The Society President requested that the Secretary conduct the voting for the Paper Award.

17.3 The Society President stated that five requests have been made for endorsements for IEEE awards. He will ensure that these are personal endorsements, and not society endorsements.

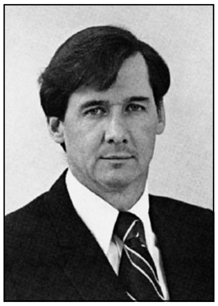
18. Joachim Hagenauer presented an update on the ongoing Society review. An update is due by the end of June.

19. The next board meeting will take place on Wednesday, September 5, 2001, in Cairns, Australia during the IT workshop. Joachim Hagenauer thanked Tom Fuja for making arrangements for the Annual Meeting.

21. The meeting was adjourned at 4:40 PM.

Blake Fest — Symposium

by Vijay Bhargava, H. Vincent Poor and Vahid Tarokh



Ian Blake

A symposium on coding and information theory in honour of Ian F. Blake on the occasion of his 60th birthday was held in Victoria, British Columbia on June 7 & 8, 2001.

A prolific scholar, Ian has made fundamental contributions to statistical communication theory, algebraic coding theory, trellis codes, sequences and spread sprectrum communications, cryptography and computations in Galois Fields. He is also responsible for the education of great many students and scholars. During the period that he served as the Chairperson at the Department of Electrical and Computer Engineering at the University of Waterloo, the department underwent a renaissance and grew significantly through the addition of many outstanding faculty members and staff people.

Ian has served the IT Society in numerous capacities, including as Co-Chair of ISIT'83 (St. Jovite) and as Technical Program Chair of ISIT'95 (Whistler). In 1989, he became the first President of the IEEE Information Theory Society to come from outside of Regions 1-6 (USA).

The Symposium featured twenty presentations, and a "festschrift" is planned to be published during next year. The technical program was organized by Vijay Bhargava, Vincent Poor and Vahid Tarokh, who are also editing the festschrift. The speakers and titles of the symposium papers are listed below:

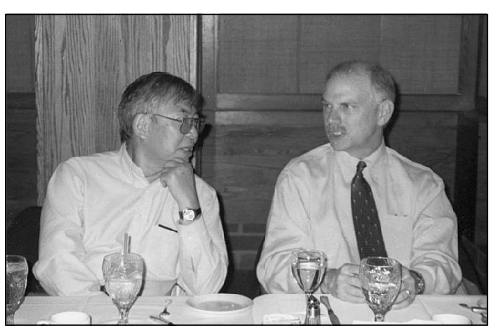
Speaker	**Title**
Joachim Hagenauer	*Some Promises that Shannon Made are Now Fulfilled*
H. Vincent Poor	*Quantum Multiuser Detection*
Sergio Verdu	*Multiuser Diversity*
Jon W. Mark	*Power Distribution and Control in CDMA Systems*
Norman C. Beaulieu	*On Level-Crossing Rates and Fade Duration of Diversity Systems*
Prakash Narayan	*Time-Varying Multiple Access Channels with Channel State Information*
Raymond Yeung	*Network Coding Theory: An Overview*
David Haccoun	*Space-Time Convolutional Coding*
T. Aaron Gulliver	*Asymptotic Analysis of SPC Product Codes*
M. Anwarul Hasan	*Computations Over Very Large Finite Fields With Resource Constrained Devices*
Vahid Tarokh	*Two Constructions of 16-QAM Golay Sequences*
Wai Ho Mow	*A Unifying Approach for Constructing Detecting Matrices for Multiuser Coding*
Shu Lin	*DTIB (Doubly Tricky Ian Blake) Codes*
Daniel Joseph Costello, Jr .	*Low Density Parity Check Codes Derived From Quasi Cyclic Block Codes*
Michael Tanner	*A Class of Group-Structured (3,5) LDPC Codes*
Tom Hoeholdt	*News on the Polynomial Approach to Coding*
Frank Kschischang	*The Poisson Sum Formula and Duality in Factor Graphs*
Richard Blahut	*From Yaghoobian-Blake to Sakata-Koetter algorithms*
Hamid Jafarkhani	*Multiple Antenna Differential Detection from Generalized Orthogonal Designs*
Vijay K. Bhargava	*Codes Based on Combinatorial Designs*

The symposium was held in the magnificent Dunsmuir Lodge, some 30 km north of Victoria. Perched on Mount Newton, the Lodge commands sweeping views of the Pacific Ocean, Gulf Islands and coastal mountains. These views were the backdrop for the Symposium technial presentations and social events.

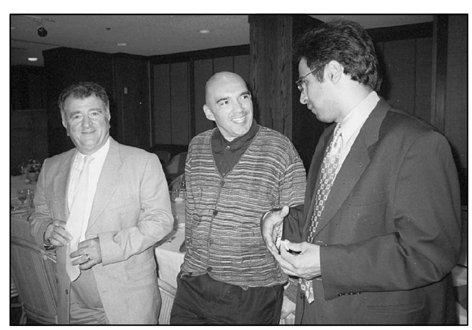
The highlight of the social program was an outstanding banquet on June 7, with Vince Poor serving as the Master of Ceremonies. Participants shared stories about Ian, President Hagenauer brought greetings on behalf of the Information Theory Society, and an operetta was sung by Tony Ephremides, Michael Tanner and Sergio Verdu.

The local arrangements were made by T. Aaron Gulliver, while Raymond Yeung served as the official photographer. The Symposium publication duties were handled by Zeljko Blazek.

At Blake Fest: Vijay Bhargava, Ian Blake and David Haccoun



At Blake Fest: Shu Lin and Vince Poor



At Blake Fest: Tony Ephremides, Sergio Verdù and Vahid Tarokh

The symposium website is located at:

http://www.ece.uvic.ca/~agullive/blakefest/

A poem composed by David Haccoun in honor of the occasion is as follows:

Mon cher Ian

Soixante ans déjà, c'est à peine croyable!
Je te revois encore tout jeune et si affable,
Cachant derrière ton air de bon aloi,
Ta grande expertise des Corps de Galois.

Et qui aurait sans ambages,
Oser t'affronter en Théorie du Codage?
Que ces codes soient Convolutionnels, en Blocs ou Turbo,
Bien obligés sommes nous de te lever chapeau.

Et même avec ta grande amabilité,
Place à personne tu ne laisses en Théorie des Probabilités,

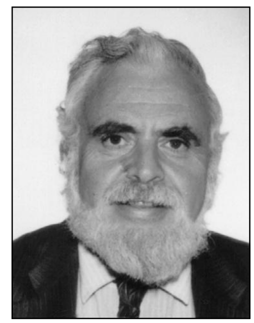
Mais, ne serait ce point te porter offense,
Si on devait passer sous silence
Tes nombreuses autres contributions?

Que ce soit en cryptographie,
Ou autres des Nombres la Théorie,
Ou combien plus important,
Au labo ou en classe avec tes étudiants.

Soixante ans déjà, c'est à peine croyable
D'être resté si jeune et toujours aimable!
Je t'en souhaite encore, des années,
Heureuses, nombreuses, prospères et en santé.

GOLOMB'S PUZZLE COLUMN™

WHAT COLOR IS MY HAT?



–Solomon W. Golomb

Each of the n members of a team will be assigned a hat, either black or white in each case. No team members will see or be told the colors of their own hats, but each will have some information about the colors of the other members' hats. Different sets of rules for this are enumerated below. The team will know in advance what the rules are, and will have an opportunity to agree on a strategy before the contest begins. In general, when asked "What color is your hat?", a team member can answer either "White" or "Black" or "Pass". If any team member gives an incorrect answer ("Black" instead of "White", or "White" instead of "Black") the entire team loses. Also, if **every** team member says "Pass", the entire team loses. The objective is to maximize the probability that the team will *win*, which requires at least one correct answer and no incorrect answers.

Case 1. The n contestants will be lined up single file, and then will be assigned hats. Each will see all the hats in front of him/her, but not his/her own or those behind. They will be given the additional information: "Not all the hats are the same color". The last contestant in line will be the first to be asked "What color is your hat?", then the next-to-last, and so on. What strategy should the team adopt to guarantee a win?

Case 2. The n contestants will be assembled in a room where each one will see the color of every hat but his/her own. They will be asked "What color is your hat?" in random order, and each will hear all the answers. If they are assured that not all the hats are the same color, what winning strategy can the team adopt?

Case 3. Each contestant will be in a different hotel room (rooms numbered 1 to n), and will be told the colors of the hats of the contestants in each of the other n - 1 rooms, but not the color of his/her own hat. There will be no communication of any sort (verbal, visual, auditory, etc.) among the contestants once the hat colors are assigned, and no contestant will hear the answer of any other contestant to the question "What color is your hat?"

The n hat colors will be assigned independently and at random. Thus, all hats *might* be the same color, though this is unlikely if n is large. The objective, in the team's planning session, is to develop a strategy which will maximize the probability that the team will win. What strategy should they adopt, and what probability of winning will it achieve?

Notes and Hints.

1. The team could agree in advance that all but one of them will say "Pass", and the designated guesser will guess randomly (or could even specifically guess "White"), to give the team a 50% chance of winning. This strategy gives a lower bound, but surprisingly it can be improved upon for $n \geq 3$.

2. There is a non-trivial connection between this problem and a major topic in Information Theory.

3. Given any $\epsilon > 0$, there is an integer $N = N_\epsilon$ such that the optimum strategy will win with probability $\geq 1 - \epsilon$ provided that the number of team members n exceeds N_ϵ. (If $\epsilon = 2^{-k}$, then $N\epsilon$ is easily calculated!)

2001 IEEE Information Theory Workshop

Cairns, Australia
2-7 September 2001.

Alex Grant

The 2001 IEEE Information Theory Workshop was held in Cairns, Australia on September 2-7 2001. This workshop was hosted by the Joint Australian Chapter of the IEEE Information Theory Society, which was recently formed in response to growing activity in Information Theory in Australia.

On the boat to Green Island LR Unknown, Giuseppe Caire,and Hesham El Gamal on their way to Green Island.

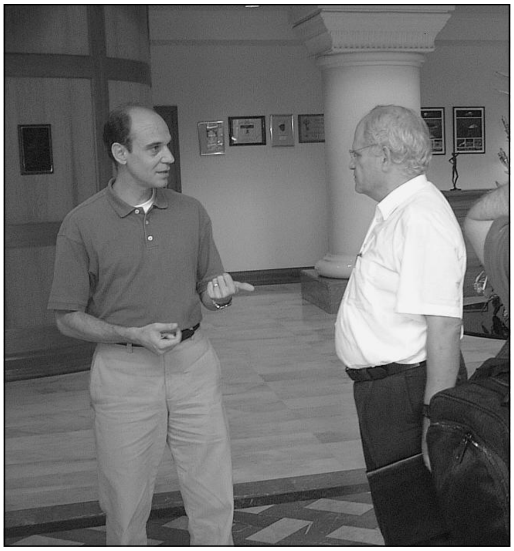
Almost 100 participants enjoyed the relaxed environment of Far North Queensland, as they discussed many interesting problems in Information Theory. Despite its southerly location, the workshop was well supported by delegates from around the world, with representatives from USA, Japan, Europe, Korea, Israel, Canada, China, Singapore and of course Australia.

The workshop consisted of 43 invited papers, and 14 contributed papers (extra copies of the proceedings are available through the IEEE). The session organisers did an excellent job in putting together sessions on Iterative Decoding, Iterative Receivers, Multiple Access, Turbo Coding, Shannon Theory, Space-Time Coding, and Topics in Coding. It was a testament to the high quality presentations that despite the lure of the Great Barrier Reef, only an hour away by boat, that the final Friday afternoon "Recent Results" session was so very well attended.

A highlight of the social program was the Wednesday half-day excursion. After a not-altogether smooth sailing trip of about 40 minutes, over 90 Information Theorists, their spouses and children spilled onto the beautiful beaches of tropical Green Island. Whether it was walking around the lush island, snorkelling among the coral with tropical fish, turtles and stingrays, windsurfing or simply sunbathing on the sand, by all reports the trip was an adventure that will be remembered by everyone.

On the boat to Green Island. In the foreground, Tom Cover and his wife. In the background, 2001 Information Theory Workshop organizers, Iain Collings, Alex Grant and Jamie Evans.

Sergio Verdu, Suzanne Loeliger, and Andi Loeliger on the boat to Green Island.



Robert Morelos-Zaragoza and IT Society President Joachim Hagenauer at the conference hotel.

"Bush Remedy" playing at the 2001 Information Theory Workshop banquet.

The Thursday evening banquet (subject to a ban on the wearing of ties) was a lively affair. A traditional Australian bush band, "Bush Remedy" treated the diners to many Australian folk songs, which were enjoyed along with the delicious Australian food and wines. The band was joined at times by various workshop participants who assisted musically on the lagerphone and washboard. Highlights included the ensemble of representatives from the Workshop Sponsors, who sang Give Me a Home Among the Gum Trees, which was followed later by an all-Australian rendition of Waltzing Matilda.

The workshop concluded on Friday with a poolside farewell reception. Details on the technical program may still be found on the workshop web site: http://www.itr.unisa.edu.au/itw2001.

WORKSHOP REPORT:

German Workshop on Convolutional Codes

Essen, Germany
October 3-5, 2001

The IEEE German Chapter on Information Theory organized a workshop on convolutional codes at the Institute for Experimental Mathematics, October 3-5, 2001. The program contained the following 11 lectures:

Daniel J. Costello (Notre-Dame, USA and Technical University of München, Germany)
A New Look at Quick-Look-In Codes

Ralph Jordan (University of Ulm)
On Woven Convolutional Codes with Outer Warp and Unequal Error Protection

Peter Sweeney (University of Surrey, UK)
SOVA in Iterative Decoding of Serial Turbo Codes

Oyvind Ytrehus (University of Bergen, Norway)
Fast algorithms for determining the weight distribution of Turbo Codes

Martin Bossert, Chairman IT German Chapter, Han Vinck Organizer of the Workshop and Daniel J. Costello, Jr.

The workshop banquet with Peter Sweeney in front.

A. Geyer and A.J. Han Vinck (IEM, Essen, Germany)
Equivalent Convolutional Codes and Decoding Complexity

Tadashi Wadayama (Okayama Prefecture University, Japan)
Calculating the Exact Bit Error Probability of a Binary Liner Code over the BSC

Volker Braun and Marceau Coupechoux (Alcatel, Germany)
Viterbi Equalization of Space-Time Coded Signals in GSM-like Systems

Kees Schouhamer Immink (Turing Machines Inc., Eindhoven, the Netherlands)
Sliding encoding of constrained sequences

Vladimir Balakirsky (Leningrad, Russia)
Recursive Decoding Procedures for Minimizing the Bit Error Probability for Block and Convolutional Codes

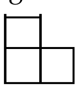
Viktor Parlouchkov (University of Ulm, Germany)
On Transfer Function Methods for Convolutional Codes

Axel Hübner (University of Ulm, Germany)
On Interleaver Design for Concatenated Convolutional Codes

The workshop attracted some 22 scientists from 11 countries and was held in a very informal way, leading to many discussions and even a joint singing during the banquet. Proceedings containing abstracts and full papers (75 Euro) can be obtained from the organizer Han Vinck, vinck@exp-math.uni-essen.de, or Fax: +49-201-1837663.

GOLOMB'S PUZZLE COLUMN ™

TILINGS WITH RIGHT TROMINOES SOLUTIONS

1. To prove, by mathematical induction on n, that a single square (a "monomino") can be removed from anywhere on the $2^n \times 2^n$ board and then the rest can be tiled with "right trominoes" (three quadrants of a 2×2 square, ), we start at $n = 1$, and observe that whichever square is removed from a $2^1 \times 2^1$ board, what is left is a single right tromino. (It is more sophisticated to start the induction at $n = 0$, where after removing a monomino from the $2^0 \times 2^0$ board *nothing* is left, which can be tiled using zero right trominoes!)

The inductive assumption is then that when a single square is removed from anywhere on the $2^k \times 2^k$ board, the rest can be tiled with right trominoes. Now consider the $2^{k+1} \times 2^{k+1}$ board. Divide it into four $2^k \times 2^k$ quadrants. Wherever a monomino is removed from the original $2^{k+1} \times 2^{k+1}$ board, the rest of that quadrant can be tiled with right trominoes by the inductive assumption. From each of the other three quadrants, remove the square touching the center of the $2^{k+1} \times 2^{k+1}$ board. The rest of those quadrants can be tiled with right trominoes by the inductive assumption, and the three removed squares can be replaced by a single right tromino. (See Figure 1.)

Note. This first appeared in December, 1954, in [1], which was the text of a talk I gave in November, 1953, to the Harvard Math Club. This result has reappeared so often that to many people it now has the status of a "folk theorem".

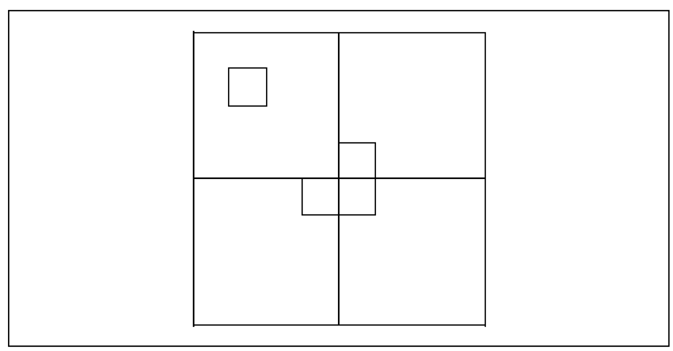


Figure 1: $2^{k+1} \times 2^{k+1}$ board partitioned into quadrants.

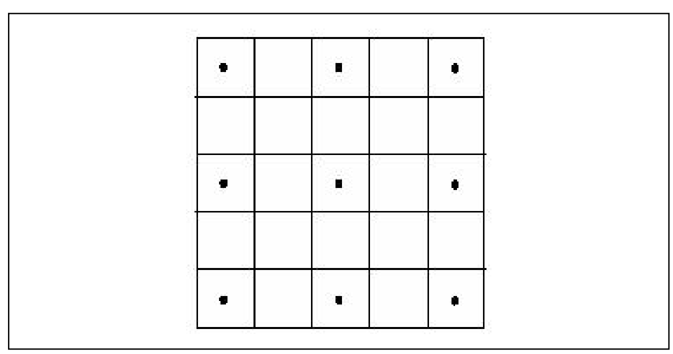


Figure 2: The 9 locations where a monomino can be removed.

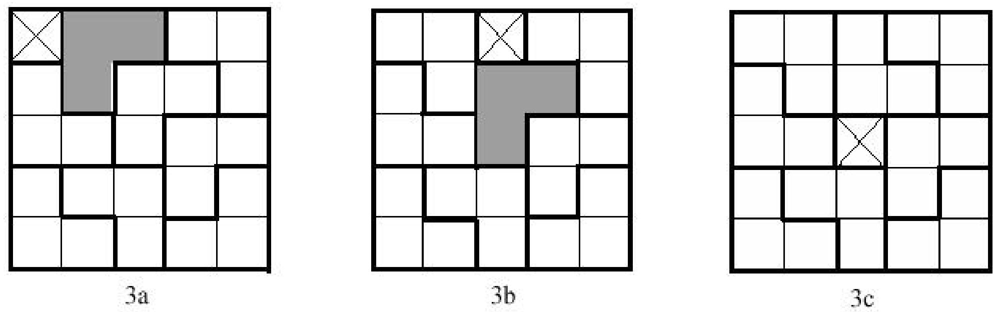


Figure 3: Tilings of the 5 × 5 board with a monomino removed.

2. There are nine locations on the 5 × 5 board where a single square (monomino) can be removed such that the rest of the board can be tiled with right trominoes. These 9 locations are marked by dots in Figure 2. Note that no two of the dotted squares can be covered by the same right tromino. Therefore, if none of these squares is removed, a tiling will require 9 right trominoes, for a total area of 9 × 3 = 27, which is impossible on a board whose total area is 25.

To show that all 9 of these locations are possible, we note that only 3 locations are inequivalent relative to the symmetries of the 5 × 5 square. Examples of the three tilings are shown in Figure 3.

Note the similarity of these three examples. To get from 3*a* to 3*b*, flip the shaded monomino in 3*a*. To get from 3*b* to 3*c*, flip the shaded monomino in 3*b*.

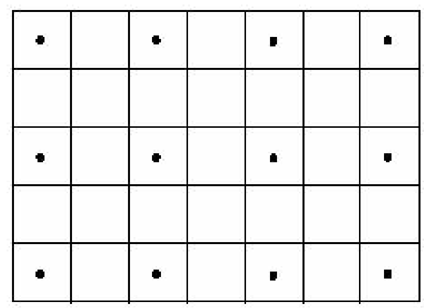


Figure 4: The "dotted" squares on the 5 × 7 board.

3. There are 9 inequivalent locations (relative to the symmetries of the 5 × 7 rectangle) where a domino can be removed, such that the rest can be tiled by right trominoes.

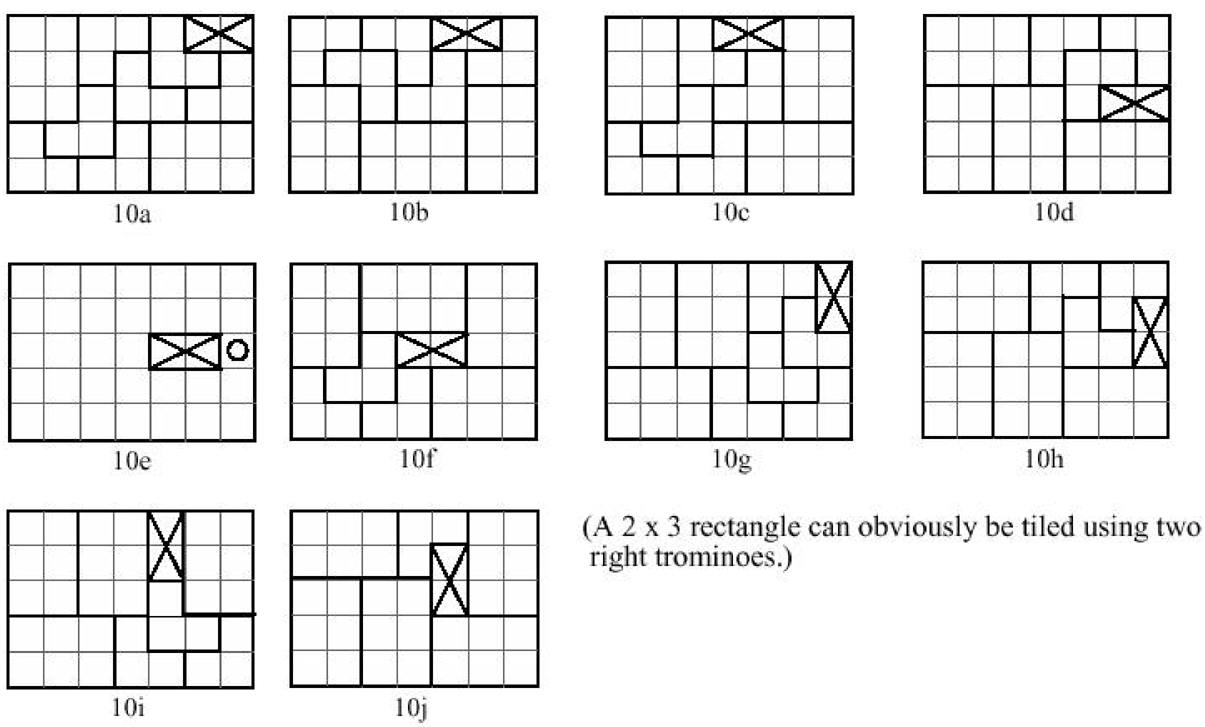


Figure 5: The ten inequivalent locations for a domino that covers a dotted square on the 5 × 7 board.

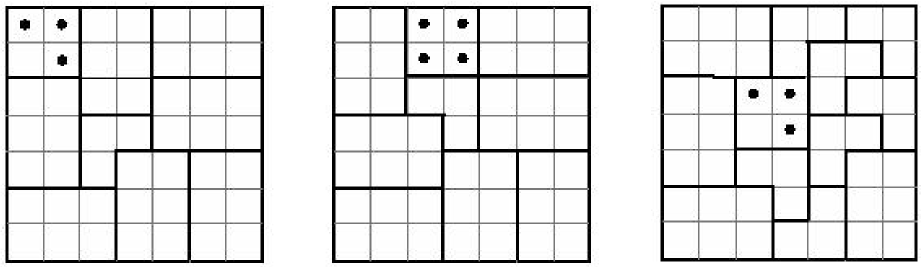


Figure 6: Wherever a monomino is removed from the 7 × 7 board, the rest can be tiled with right trominoes.

Note that for a successful tiling, the removed domino must cover one of the 12 "dotted" squares in Figure 4.

Since no two of the dotted squares can be covered by the same right tromino, if all 12 remain unremoved, a tiling will require at least 12 right trominoes, for a total area of 3 × 12 = 36, which exceeds the area of the 5 × 7 board.

There are 10 inequivalent locations for a single domino that covers one of the 12 dotted squares, as shown in Figure 5, with tilings by right trominoes on 9 of them.

Note that in figure 10e, the square containing "0", to the right of the domino, cannot be filled in by part of a right tromino without creating an impossible situation for completing the tiling.

4. A monomino can be removed from *anywhere* on the 7 × 7 board, and the rest can be tiled with right trominoes! The three cases in Figure 6 suffice to show this, where the ten dotted squares represent all the inequivalent positions for the monomino.

5. For the proof that "for all $m > 5$ with m not a multiple of 3, a monomino can be removed from anywhere on the $m \times m$ board and the rest can be tiled by right trominoes", see [2].The proof is inductive, but not nearly so simple and elegant as the inductive proof in problem 1.

6. For an $a \times b$ board to be tiled by right trominoes, it is clearly necessary that at least one of a and b must be a multiple of 3. This necessary condition is also sufficient except when one dimension (either a or b) is 3 and the other is odd, or when either a or b equals 1. (This result is Theorem 1 in [3], and the proof is not difficult, though dealing with the special cases may seem a bit tedious.)

References

[1] S.W. Golomb, "Checkerboards and Polyominoes", *American Math. Monthly*, vol.61, no. 10, December, 1954, 675-682.

[2] I.P. Chu and R. Johnsonbaugh, "Tiling deficient boards with trominoes", *Math. Mag*. 59 (1986), 34-40.

[3] J.M. Ash and S.W. Golomb, "Tiling rectangles and deficient rectangles with trominoes", in preparation.

New Books

Raymond Yeung

Adaptive Antennas for Wireless Communications,
by George V. Tsoulos. IEEE Press, 2001, 776 pp., US$ 119.95 (List Price), US$ 102 (IEEE Member Price), ISBN 0-7803-6016-8.

Contents:
Introduction; Channel Models; Adaptive Algorithms; Performance Issues; Implementation Issues; Experiments; Applications and Planning Issues.

Software Radio Technologies: Selected Readings,
by Joseph Mitola III and Zoran Zvonar. IEEE Press, 2001, 544 pp., US$ 119.95 (List Price), US$ 102 (IEEE Member Price), ISBN 0-7803-6022-2.

Contents:
Concept of Software Radio, Historical and Theoretical Foundations; Enabling Technologies for Realization of Software Radio (Radio Frequency Design, Converter Technologies, Digital Signal Processing, Reconfigurable and Programmable Hardware Structures); Systems and Architectures Based on Software Radio Concepts; Emerging Technologies; Software Radio Applications and Economics.

Voice Compression and Communications,
by Lajos Hanzo, Clare Sommerville, and Jason Woodward. IEEE Press, 2001, 770 pp., US$ 119.95 (List Price), US$ 102 (IEEE Member Price), ISBN 0-7803-6033-8.

Contents:
Standardized and Proprietary Speech Codes and Transceivers; The Mobile Propagation Environment; Modulation and Transmission Techniques; Channel, Classic Waveform,

Synthesis Based, and Predictive Coding; Narrow and Wide-band Spectral Quantization.

Introduction to 3G Mobile Communications,
by Juha Korhonen. Artech House, 2001, 620 pp., pounds64, ISBN 1-58053-287-X.

Contents:
Overview; CDMA Principles; WCDMA Air Interface — Physical Layer; Modulation Techniques and Spread Spectrum; Spreading Codes; Channel Coding; WCDMA Air Interface Protocol Stack; Network; Network Planning; Network Management; New Concepts in the UMTS Network; Procedures; 3G Services; 3G Applications; The Future; Standardization Organizations and Industry Groups.

Wireless LAN Standards and Applications,
edited by Asunción Santamaria and Francisco López-Hernández. Artech House, 2001, 302 pp., £59, ISBN 0-89006-943-3.

Contents:
Introduction; The IrDa Standard; The IEEE 802.11 Standard; The HIPERLAN Standard; Application Scenarios; Upcoming Standards and Future Trends.

Principles of Modern Communications Technology,
by A. Michael Noll. Artech House, 2001, 320 pp., £45, ISBN 1-58053-284-5.

Contents:
Audio Technology; Video Systems; Speech Communication Systems; Written Communication Systems.

Electronic Payment Systems for E-Commerce, 2nd Ed.,
by Donal O'Mahony, Michael Peirce and Hitesh Tewarir. Artech House, 2001, 356 pp., £52, ISBN 1-58053-268-3.

Contents:
Motivation for Electronic Payment; Characteristics of Current Payment Systems; Cryptographic Techniques; Credit Card Based Systems; Account Transfers and Electronic Checks; Electronic Cash Payment Systems; Micropayment Systems; Mobile Commerce; Payment Systems — Prospects for the Future.

Digital and Analog Communication Systems, 6th Ed.,
by Leon W. Couch II. Prentice Hall, 2001, 750 pp., US$ 107, ISBN 0-13-081223-4.

Contents:
Introduction; Signals and Spectra; Baseband Pulse and Digital Signaling; Bandpass Signaling Principles and Circuits; AM, FM and Digital Modulated Systems Random Processes and Spectral Analysis; Performance of Communication Systems Corrupted by Noise; Wire and Wireless Communication Systems.

Data and Computer Communications,
by William Stallings. Prentice Hall, 2000, 810 pp., US$ 86, ISBN 0-13-084370-9.

Contents:
Overview; Data Communications; Wide-Area Networks; Local Area Networks; Communications Architecture and Protocols.

Introduction to Digital Communications, 2nd Ed.,
by Rodger E. Ziemer and Roger W. Peterson. Prentice Hall, 2001, 905 pp., US$ 107, ISBN 0-13-896481-5.

Contents:
Introduction to Digital Data Transmission; Signals, Systems, Modulation, and Noise: Overview; Basic Digital Communication Systems; Signal-Space Methods in Digital Data Transmission; Channel Degradations in Digital Communications; Fundamentals of Information Theory and Block Coding; Fundamentals of Convolutional Coding; Fundamentals of Repeat Request Systems; Spread-Spectrum Systems; Introduction to Cellular Radio Communications; Satellite Communications.

Video Coding for Wireless Communication Systems,
by King N. Ngan, Chi W. Yap, and Keng T. Tan. Kluwer, 2001, 560 pp., US$ 175 (US$ 69.95 on orders of five or more, for classroom use only), ISBN 0-8247-0489-4.

Contents:
Source Coding; MPEG-4 — Standard for Multimedia Applications; Channel Coding; Radio Channel Modelling; Error Resilient Combined Source Channel Image Coder; Error Resilient Combined Source Channel Video Coder; Multiple Access in Spread Spectrum Communications; Future Generation Wireless Video Communication Systems.

Multicarrier Modulation with Low PAR,
by Jose Tellado. Kluwer, 2000, 176 pp., £69, ISBN 0-7923-7988-8.

Contents:
Introduction; Multicarrier Modulation; Peak to Average Ratio; PAR Reduction by Tone Reservation; PAR Reduction by Tone Injection; Maximum Likelihood Detection of Distorted Multicarrier Signals; Summary and Conclusions.

Computer Science and Communications Dictionary,
by Martin Weik. Kluwer, 2001, ISBN 0-7923-8425-3.

Mobile Channel Characteristics,
by James K. Cavers. Kluwer, 2000, 240 pp., £77, ISBN 0-7923-7926-8.

Space-Time Processing for CDMA Mobile Communications,
by Pieter van Rooyen, Michiel P. Lötter, and Danie van Wyk. Kluwer, 2000, 336 pp., £90, ISBN 0-7923-7759-1.

Multi-Carrier Spread Spectrum and Related Topics,
edited by Khaled Fazel and Stefan Kaiser. Kluwer, 2000, 376 pp., £90, ISBN 0-7923-7740-0.

Wireless Personal Communications: Bluetooth Tutorial and Other Technologies,

edited by William H. Tranter, Brian E. Woerner, Jeffery H. Reed, Theodore S. Rappaport, and Max Robert. Kluwer, 2001, pounds102, ISBN 0-7923-7214-X.

Wireless Communication Technologies: New Multimedia Systems,
edited by Norihiko Morinaga, Ryuji Kohno, and Seichi Sampei. Kluwer, 2000, 344 pp., £77, ISBN 0-7923-7900-4.

Nonuniform Sampling: Theory and Practice,
edited by Farokh Marvasti. Kluwer, 2001, ISBN 0-306-46445-4.

Numbers, Information and Complexity,
edited by Ingo Althöfer, Ning Cai, Gunter Dueck, Levon Khachatrian, Mark S. Pinsker, Andras Sárközy, Ingo Wegener, and Zhen Zhang. Kluwer, 2000, 672 pp., £107, ISBN 0-7923-7765-6.

The Mobile Communications Handbook, 2nd Ed.,
edited by Jerry D. Gibson. CRC Press, 1999, 720 pp., US$ 95, ISBN 0-8439-8597-0.

The Telecommunications Handbook,
edited by Kornel Terplan and Patricia Morreale. CRC Press, 2000, 424 pp., US$ 99.95, ISBN 0-8439-3137-4.

Hargrave's Communications Dictionary,
by Frank Hargrave. IEEE Press, 2001, 1056 pp., US$ 129.95 (List Price), US$ 110 (IEEE Member Price), ISBN 0-7803-6020-6.

Intelligent Signal Processing,
edited by Simon Haykin and Bart Kosko. IEEE Press, 2001, 576 pp., US$ 109.95 (List Price), US$ 93 (IEEE Member Price), ISBN 0-7803-6010-9.

A Field Guide to Dynamical Recurrent Networks,
by John F. Kolen and Stefan C. Kremer. IEEE Press, 2001, 496 pp., US$ 109.95 (List Price), US$ 93 (IEEE Member Price), ISBN 0-7803-5369-2.

Cable Modems: Technologies and Applications,
edited by Executive Editor, Venkata C. Majeti and Editors, John Fijoleck, Michelle Kuska, and Kotikalapudi Sriram. IEEE Press and IEC (International Engineering Consortium), 2000, 800 pp., US$ 79.95 (List Price), US$ 72 (IEEE Member Price), ISBN 0-7803-5395-1.

Wireless Video Communications: Second- and Third-Generation Systems and Beyond,
by Lajos Hanzo, Peter Cherriman, and Jurgen Streit. IEEE Press, 2001, 1056 pp., US$ 119.95 (List Price), US$ 102 (IEEE Member Price), ISBN 0-7803-6032-X.

WCDMA for UMTS: Radio Access for Third Generation Mobile Communications, Revised Edition,
edited by Harri Holma and Antti Toskala. Wiley, 2000, 352 pp., US$ 85, ISBN 0471720518.

UMTS Mobile Communications for the Future,
edited by Flavio Muratore. Wiley, 2000, 240 pp., US$ 65, ISBN 0471498297.

CDMA: Access and Switching: For Terrestrial and Satellite Networks
by Diakoumis Gerakoulis and Evaggelos Geranitois. Wiley, 2000, 320 pp., US$ 105, ISBN 0471491845.

Wireless Video Communications: Second to Third Generation and Beyond,
by Lajos Hanzo, William Webb, and Thomas Keller. Wiley, 2000, 762 pp., US$ 120, ISBN 078036032X.

Principle of Mobile Communication, 2nd Ed.,
edited by Gordon L. Stüber. Kluwer, 2000, 776 pp., £61, ISBN 0-7923-7998-5.

Turbo Codes: Principles and Applications,
by Branka Vucetic and Jinhong Yuan. Kluwer, 2000, 344 pp., £81, ISBN 0-7923-7868-7.

CALL FOR PAPERS

2002 IEEE International Symposium on Information Theory

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

General Co-Chairs:
James L. Massey
Bixio Rimoldi

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

Sponsor Liaisons:
David Tse
Martin Vetterli

Finance:
Serge Vaudenay

Local Arrangements:
Rüdiger Urbanke

Publications:
Hans-Andrea Loeliger

Publicity:
Ueli Maurer
Michael Gastpar

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

Previously unpublished contributions to the following areas are solicited:

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

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

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

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

`http://isit02.epfl.ch`

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

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

General Co-Chairs:
Hideki Imai
Robert McEliece
Ryuji Kohno

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

International Advisory Committee Chair:
Vijiay Bharagava

Executive Committee Secretary:
Motohiko Isaka
Hideki Ochiai

Finance:
Takeshi Hashimoto
Hirohito Suda
Toyoo Takata

Registration:
Kouichiro Wakasugi
Toshiyasu Matsushima
Keiichi Iwamura

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

Publications:
Ikuo Oka
Atsuko Miyaji
Masayoshi Ohashi

Publicity:
Toru Fujiwara
Masahiko Hattori
Akihisa Ushirokawa
Atsuhiro Yamagishi
Nobukazu Doi
Shinichi Kawamura

CONFERENCE ANNOUNCEMENT

2003 IEEE International Symposium on Information Theory

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

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

Previously unpublished contributions to the following areas are solicited

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

The first call for papers will be published in January 2002.

Detailed information on the technical program, special events, accommodations, travel arrangements, excursions and applications for travel grants will be included in subsequent mailings, and will be posted at Symposium web site: http://www.kohnolab.dnj.ynu.ac.jp/~isit2003/

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

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

Conference Calendar

DATE	CONFERENCE	LOCATION	CONTACT/INFORMATION	DUE DATE
June 30- July 5, 2002	**2002 IEEE International Symposium on Information Theory**	Lausanne, Switerland	Palais de Beaulieu, Prof. Bixio Rimoldi Communication Systems Department Swiss Federal Institute of Technology CH-1015 Lausanne, Switzerland E-mail: isit02chair@epfl.ch Phone: +41 21 693 76 62 Fax: +41 21 693 43 12	
March 17-21, 2002	**2002 IEEE Wireless Communications and Networking Conference (WCNC 2002)**	Orlando, Florida, USA	Dick Lynch Verizon Wireless, USA www.wcnc.org/2002	August 15, 2001
April 28- May 2, 2002	**2002 IEEE International Conference on Communications (ICC 2002)**	New York, New York, USA	Mark Karol Avaya Inc., USA mk@avaya.com www.icc2002.com	August 15, 2001
February 19-22, 2002	**2002 International Zurich Seminar on Broadband Communications**	ETH Zurich, Zurich, Switzerland	Prof. Dirk H. Dahlhaus Swiss Federal Inst. of Tech. Comm. Technology Laboratory Sternwartstr. 7 CH-8092 Zurich SWITZERLAND +41 1 63 22788 +41 1 63 21209 (Fax) dahlhaus@nari.ee.ethz.ch http://www.izs2002.ethz.ch	September 15, 2001
May 19-22, 2002	**2002 IEEE Communications Theory Workshop**	Naples Beach Hotel & Golf Club, Sanibel Island, FL	Mr. Gordon Stuber GCATT, Room 571 250 14th Street, NW Atlanta, GA 30318 +1 404 894 2923 +1 404 894 7883 (Fax) stuber@ece.gatech.edu	TBA
November 18-22, 2002	**GLOBECOM 2002 - 2002 IEEE Global Telecommunications Conference**	Taipei International Conventional Center, Taipei, Taiwan	Mr. Douglas S. J. Hsiao 12, Lane 551 Min-Tsu Road Sec. 5, Yang-Mei, Taoyuan 326 TAIWAN +886 3 424 5210 +886 3 424 4168 (Fax) sjhsiao@chttl.com.tw	TBA

IEEE
IEEE Information Theory Society Newsletter
445 Hoes Lane, P.O. Box 1331
Piscataway, NJ 08855-1331 USA