IEEE Information Theory Society Newsletter

Vol. 44, No. 2, June 1994 Editor: Ramesh Rao ISSN 1059-2362

# 1993 Shannon Lecture

*Elwyn Berlekamp*

While preparing for this Shannon lecture, I tried to prepare a list of all the people in the IT Group to whom I feel indebted. That list soon grew so long that I could find no reasonable way to cut it off. At various times in the past 30 years, I've had the pleasure of getting to know and work with quite a few of you, and it's really been an awful lot of fun. We're all fortunate to be part of a dynamic intellectual community which has been able to formulate and solve a large number of interesting problems, and to support ourselves while doing so.

I eventually decided to dedicate this talk to the person who first introduced me to serious research, to information theory, and coding, and to game theory. He was my first boss and mentor at Bell Labs, when I began work there as an undergraduate. His name was John L. Kelly, Jr. After getting a PhD in mathematical physics from the University of Texas, John worked at Bell Labs for the rest of his life. He died of a heart attack in 1965 at the age of 41.

Today, I've decided to skim the surface of 4 different topics, all of which were of interest to John Kelly. I'm hoping that this will maximize the chance that I'll touch at least one topic of interest to each of you.

## Portfolio Theory

The paper for which John Kelly is most remembered today is better known in financial circles than in engineering ones. Although Kelly often chatted about this paper, much of what he said was well over my head at the time, and I never actually tried to READ this paper until after his death. Kelly originally entitled the paper INFORMATION THEORY AND GAMBLING. But some AT&T executives expressed concern that the press might misconstrue such a title as evidence that Bell Labs might be doing work on behalf of illegal bookies who were big customers of AT&T. So the paper appeared under the less colorful title. But Kelly fervently believed that gambling and investment differed only in one minus sign: Opportunities that offer FAVORABLE odds are called INVESTMENTS, but deals that involve unfavorable odds are called GAMBLING. Part of the problem is that it isn't always so easy to tell which is which.

Kelly's investment model included inside information and several probability distributions. There was an ensemble of possible future scenarios, occurring with various TRUE odds, which were known to the investor. There were also betting odds, as determined by the stocks and futures marketplaces. For this model, Kelly found the optimum investment portfolios, which yielded the maximum long-term rate of return that could be attained with probability approaching one. This rate of return could be interpreted as the capacity of the channel over which the investor received his noisy inside information.

Kelly's paper has attracted more attention in recent years than it did when it was first published.

continued on page 3

# From the Editor

*Ramesh Rao*

The "Reflections" of Meir Feder, Neri Merhav and Michael Gutman, that appeared in the March 1994 issue, elicited a number of compliments from our readers. The style and content of the article were very well received. More kudos to the authors. The article on the derivation of the mini-max criterion by Pyati and Joseph generated additional contributions on the topic. Budgetary and other constraints compel us to focus our resources on news and other society developments that are of the widest interest to our members. Along these lines, the primary articles in this issue are Elwyn Berlekamp's Shannon Lecture and Richard Olshen's Plenary Lecture from the 1993 IT Symposium.

The deadlines for receiving material for the next few issues are as follows.

| Issue | Deadline |
|---|---|
| September 1994 | July 15, 1994 |
| December 1994 | October 15, 1994 |
| March 1995 | January 15, 1995 |

Electronic submissions, especially TEX and LATEX are encouraged. I may be reached at the following address.

Ramesh Rao
Department of Electrical and Computer Engineering- 0407
University of California, San Diego
9500 Gilman Drive
La Jolla, CA 92093-0407
USA

Tel: +1 (619) 534-6433
Fax: +1 (619) 534-2486
e-mail: rrao@ucsd.edu

## Table of Contents



**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: 345 East 47th Street, New York, NY 10017.

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. Second-class 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.

## 1993 Shannon Lecture

continued from front cover

Some of the recent work it has inspired among economists is controversial, or even just plain wrong, and I believe that a large fraction about what is known and correct and relevant may be found in Kelly's original paper. I urge you to read it for yourselves. I have nothing more to add to it today.

### Erasure-Burst-Correcting Convolutional Codes

While I was working for John Kelly, I published my first paper. It didn't attract much attention then, nor at any time since. But some of the questions I began to address in that paper have retained my interest ever since.

Just as one can learn a great deal about a function by studying its singularities, so can the study of simplified models sometimes yield important insights into more general versions of the same problem. John Kelly encouraged me to begin my work in information theory by studying the simplest nontrivial channel we could imagine. This is the BINARY ERASURE-BURST CHANNEL, and more generally, the Q-ARY ERASURE-BURST CHANNEL. This channel makes no errors, only erasures. And the erasures occur only in bursts. The only things that are unpredicatable are when a burst starts and how long it lasts. In hopes of finding a solution that might be useful against most plausible distributions of erasure-burst-lengths, I selected the goal of correcting every erasure burst AS SOON AS POSSIBLE. This was intended to minimize the risk that another erasure burst might begin before the decoder had received enough correct channel symbols to correct the prior erasure burst.

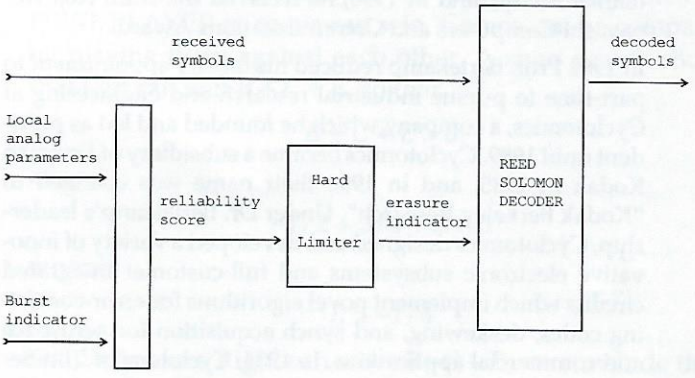
It is not hard to show that the best solution to this problem is a convolutional code whose generator polynomial must be chosen to make certain critical matrices nonsingular. The relevant array of parity check equations lie in a semi-infinite plane, whose upper left border is a quantized straight line of positive slope in the $x, y$ plane. If the code rate is $R$, border has slope $(1 - R)/R$. The crucial matrices are those whose upper left corners lie on the border. It is convenient to generalize the problem by allowing arbitrary monotonic boundaries, and to restrict it by requiring that the critical matrices all have determinant 1. Any solution to this problem is called a UNITARY ARRAY. It is convenient to study the problem in which the channel symbols and the coefficients of the generator polynomial can be any natural integers. Optimal solutions for a Q-ary channel can then be obtained by reducing everything modulo Q. Unitary arrays have many interesting properties. Pascal's triangle is one unitary array, although it is bounded by a vertical line to its left and a horizontal line across its top rather than by a single quantized straight line of slope $(1 - R)/R$. However, Pascal's triangle satisfies a simple well-known local recurrence, and an analogous property also holds for all unitary arrays. Many of the properties of unitary arrays that I discovered in the mid 1960s were independently discovered by Carlitz, Roselle and Scoville [1971].

Several questions about these codes remain open to this day. Even in the binary case, there are some code rates, including 2/5, for which we have formulas for only some, but not all, of the coefficients of the generator polynomial for the optimum erasure-burst-correcting convolutional code. But the more important problem is that the only decoding algorithm known for these codes is algebraic in only a relatively rudimentary sense: it inverts binary matrices. Although these codes have the capability to correct some isolated errors in addition to long erasure bursts, no one has yet devised any good decoding algorithm to do that. I'm hoping that some of you will now read my 1963 paper and and the paper by Carlitz, Roselle and Scoville, and perhaps come up with some new ideas.

### Reed-Solomon Decoding Algorithm

My next topic is "(yet another) REED-SOLOMON DECODING ALGORITHM" I'm continually surprised at how few people appreciate the richness and variety of Reed-Solomon codes. Many folks would like to identify some small part of the decoder as critical, and then identify some particular algorithm as the best, and then make that algorithm into the basis of a commodity product which would beat all contenders decisively in all respects. My experience led me to a diametrically opposite point of view. I've participated in over a dozen major RS decoding projects, and in almost every case, we were able to design a customized decoder that attained significant extra benefits by exploiting certain features that were peculiar to that problem.

The art of RS decoding now has a 32-year history of continual evolutionary improvements. I've listed some of the more significant such advances in the references. I'm pleased to have this opportunity today to announce yet-another evolutionary step forward.




Here is the block diagram of a conventional RS Decoder. In 1966 Forney showed that performance could be improved by integrating the hard limiter and the traditional RS Decoder. Instead of declaring erasures before attempting to decode, Forney's expanded decoder considers all possible thresholds for the hard limiter. With high prob-

ability, it decodes successfully if ANY such threshold yields $s$ erasures and $t$ errors and if $2t+s < d$, the minimum distance of the RS code.

Work at Cyclotomics in the 1980s yielded a variety of improvements in both speed and performance, including the capability to decode most patterns for which $2t+s = d$. These improvements are summarized in the following table:

Soon after I received the invitation to give this Shannon lecture, I began writing up these results. Unfortunately, the details were too technical to be suitable for inclusion in this lecture, so I'm putting them into a technical paper which I hope soon to complete and submit for publication. I hope that what I've said today will encourage you to read the paper, to find ways to extract soft decision symbol information out of the channels on which RS codes are used, and to find more ways to decode more errata patterns more quickly and more economically.

Jan 1993
BOUNDED DISTANCE+1 SOFT DECISION
REED-SOLOMON DECODING

| | Conventional | New |
|---|---|---|
| Finds min SCORE among errata patterns for which | $2t + s < d$ | $2t + s < d + 1$ |
| Max Code length | $n \le q - 1$ | $n \le q + 1$ |
| Worst Case Running Time | $\sim nd^2$ | $\sim nd$ |
| Running Time if $2t + s = w << d$ | $\sim nd^2$ | $\sim nw$ |
| Average Running Time | | even better |
| Probability of decoding error vs probability of decoding failure | | adjustable along improved frontier |

Elwyn Berlekamp was born in Dover, Ohio, on September 6, 1940. He received his BS, MS, and PhD degrees in EE from MIT in 1962, 1962, and 1964. After two years at UC Berkeley and 5 years at Bell Telephone Laboratories, he became Professor of Mathematics and of Electrical Engineering/Computer Science at UC Berkeley in 1971. He was Eta Kappa Nu's "Outstanding Young Electrical Engineer" in 1971. He was President of the IEEE Information Theory Group in 1973. He was associate chairman of EECS for computer science at UC Berkeley in 1975-1977, and in 1977 he was elected to the National Academy of Engineering. In 1984, Dr. Berlekamp received an IEEE Centennial Medal, and in 1990, he received the IEEE Koji Kobayashi Computers and Communications Award.

In 1982 Prof. Berlekamp reduced his faculty appointment to part-time to pursue industrial research and engineering at Cyclotomics, a company which he founded and led as president until 1989. Cyclotomics became a subsidiary of Eastman Kodak in 1985, and in 1990 their name was changed to "Kodak Berkeley Research". Under Dr. Berlekamp's leadership, Cyclotomics designed and developed a variety of innovative electronic subsystems and full-customer integrated circuits which implement novel algorithms for error-correcting codes, deskewing, and synch acquisition for aerospace and commercial applications. In 1984, Cyclotomics' "Bit-Serial" Reed-Solomon encoders were formally adopted as the NASA standard for deep space communications. On the commercial side, "Cinema Digital Sound", which was introduced in the movie film industry in 1990, is based on a prototype designed and developed under Dr. Berlekamp's leadership at Cyclotomics.

From 1967 through the late 1980s, Dr. Berlekamp and his colleagues introduced a series of major improvements in algorithms for decoding sophisticated algebraic codes, especially Reed-Solomon codes. NASA's Voyager communication system, for example, which reached Neptune in August 1989, uses a Reed-Solomon code with Berlekamp decoding. All compact disc players use RS codes with the earlier Berlekamp decoding algorithms, and some optical disk storage systems, including Kodak's, using the later refinements as well. The world's most advanced Reed-Solomon decoder, built by Cyclotomics in 1987, employed a radically new "hypersystolic" architecture to realize a one-board device which decodes the 5-character error-correcting (63,53) RS code continuously at 830 Megabits per second.

Prof. Berlekamp has supervised graduate student research in a wide range of topics in electrical engineering, computer science, and mathematics. His first graduate student was Ken Thompson (1966), who received the 1990 IEEE Hamming Award for his design of the Unix Operating System.

Dr. Berlekamp has 11 patented inventions and over 75 publications. He is author of "Algebraic Coding Theory" [McGraw-Hill 1968 and Aegean Park Press 1984], which received the IEEE Information Theory Group's "best research paper award" for 1968. He is also author of "Key Papers in Coding Theory" [IEEE Press 1973] and a coauthor of "Winning Ways" [Academic press 1982], a popular two-volume treatise on the combinatorial theory of two person perfect-information games. His two current principal technical interests are recent extensions of game theory which provide precise analyses of certain difficult endgame problems in the Oriental board game of "Go", and the use of statistical information theory to forecast stock and commodity prices. In 1990 he was president of a Commodity Trading Advisor firm, all of whose clients' accounts gained 55% in that calendar year.

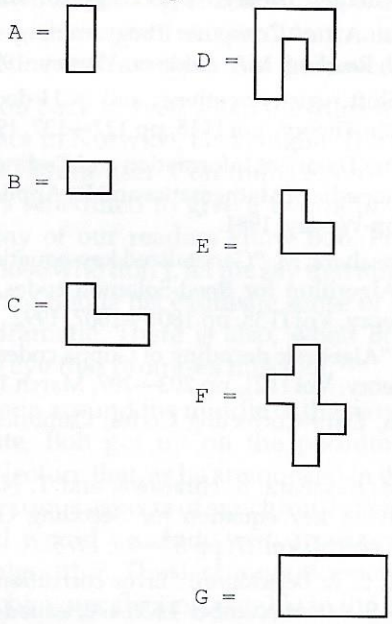
He and his wife, Jennifer, have three children: Persis, 25, Bronwen, 21; and David, 11. He has enjoyed juggling since the age of 10.

## Games

The next topic I'd like to talk about today is GAMES. Games DO relate to information theory in many ways. But I think that the intersection of information theory and game theory only scratches the surface of each subject. In addition to its applications, COMBINATORIAL GAME THEORY is a fascinating subject in its own right, and I'd now like to give you a quick introduction into this large and rapidly growing branch of mathematics.

I'd like to begin by volunteering Jim Massey to come up to the podium and help me demonstrate a game called DOMINEERING. This game can be played on a checkerboard of any size or shape. Each player has a bountiful supply of dominoes, each of which can cover two adjacent squares of the board. The players alternate placing dominoes onto pairs of adjacent unoccupied squares. But one player, called LEFT, must always play a domino vertically; the other player, called RIGHT, must always play a domino horizontally. The game ends when a player, at his turn, is unable to move. The game then ends and he loses.

As a Domineering game approaches its conclusion, the available playing areas typically split up into several small pieces such as the following:




As a demonstration, let's play the endgame $B + C + D + D + F + G + G$. Each player can make any available move in any piece of the game, and the game ends when a player cannot move anywhere.

Working back from the end of the game, it is not hard to find a position in which EVERY available piece looks like either $A$ or $B$. In such a position, it is easy to determine the winner by counting the "score", using these equations:

$$A = +1$$

$$B = -1$$

If the value is positive, then LEFT can win.

If the value is negative, then RIGHT can win.

If the value is zero, then the SECOND PLAYER to move can win.

Games such as $A + B$ and $3A + 3B$ have sum equal to zero. Intuitively, the first player cannot win such a game because he will exhaust his supply of available moves before his opponent exhausts hers. The fact is actually more general:

A GAME HAS VALUE ZERO IFF EITHER PLAYER, GOING SECOND, CAN WIN.

This leads to some provocative results. For example, by examining all lines of play, it is not difficult to show that the second player can win the game $C + C + A$. Therefore,

$$C + C + A = 0$$

and since $A = 1$, it is reasonable to suspect that $C = -1/2$. This turns out to be true. It can be similarly verified that $D = 3/4$, in the sense that $D+D+D+D - 3 = 0$. It is not hard to show that adding a game $Z$, of value 0, to another game $X$, has no affect on the outcome of $X$. Whoever can win $X$ can also win $X + Z$, and he can accomplish that by playing his winning strategy on $X$ and his second-player strategy on $Z$. The winner moves on $Z$ only immediately after his opponent has played there.

In particular, the demonstration example $B + C + D + D + F + G + G$ contains the subgame

$$B + C + D + D = -1 - 1/2 + 3/4 + 3/4 = 0,$$

so we have

$$B + C + D + D + F + G + G = 0 + F + G + G = F + G + G.$$

Evidently, whoever can win $F + G + G$ can also win $B + C + D + D + F + G + G$. Games $E$, $F$, and $G$ also have values, but the values of these games are more complicated than numbers. For example, $E$ satisfies the equation

$$E + E = 0$$

Yet $E$ is NOT 0, for when played all by itself, the game E is won by the FIRST player. Evidently, E belongs to a fourth outcome class, called fuzzy: If the value is FUZZY, then the FIRST PLAYER to move can win. Games can be compared by playing them against each other. A short search shows that Left can win $B + C + E$, so that

$$B + C + E > 0$$

or

$$-1/2 + 3/4 + E > 0$$

whence

$$E > -1/4$$

Similarly, since Right can win $-B - C + E$, we conclude that

$$E < 1/4$$

More generally, after defining games of values 1/8, 1/16, 1/32,... it can be shown that, for all values of $n$,

$$1/2^n > E > -1/2^n$$

Thus, even though $E$ is not zero, it is less than all positive numbers and greater than all negative numbers. E is an

INFINITESIMAL. It has a special name, "*", and is called "STAR". STAR is one example of a fuzzy infinitesimal.

The value of the game *F* turns out to be a POSITIVE INFINITESIMAL, called UP, and denoted by "^". Position *G* is a 2x4 rectangle. The value of *G* turns out to be a negative infinitesimal, called "Miny-2". $-G$ is a positive infinitesimal, of higher order than UP, in the sense that for any positive integer $n$, the sum of $n$ copies of *G* and one copy of *F* is still positive. Thus, the example is seen to be a win for LEFT, no matter who goes first. Jim Massey lost the demonstration game when he elected to play RIGHT instead of LEFT.

I hope that this talk has unveiled a tiny portion of the beautiful theory of combinatorial games. Combinatorial game theory now has a great deal to say about the endgame of almost any game in which the board tends to decompose into disjoint regions. That includes such traditional children's games as Dots and Boxes. Everything about Domineering in my talk today is part of the theory of PARTISAN games, which was discovered by John Conway in the 1970s. The objects which occur in this theory, including numbers, ups, stars, and many more fascinating values, are universal in the sense that they apply not only to a few positions in Domineering, but to many positions in many different games. The basic theory is presented in Conway [1975]; some additional theory, as well as the solutions of scores and scores of games appear in Berlekamp, Conway, and Guy [1982]. Some further results on Domineering appear in Berlekamp [1987] and Wolfe [1992]. For the past several years, David Wolfe and I have been working the applications of combinatorial game theory to the classic Asian board game called "Go".

I believe that research in combinatorial game theory holds promise of shedding light on some very important engineering questions:

"Where are the boundaries between subsystems?"

"What sort of interactions are there between subsystems?"

This same issue of modularity occurs frequently in Go endgames, and in that context it is possible to formulate and prove a variety of conditions that imply or refute "modularity".

Notes added in February 1994:

The book, "Mathematical Go" by Berlekamp and Wolfe was published in January 1994. The Mathematical Sciences Research Institute at Berkeley is sponsoring a workshop on Combinatorial Games on July 12-22, 1994. I hope that some of you will be able to attend.

## References


***Portfolio Theory:***

John L Kelly, "A New Interpretation of the Information Rate", Bell System Technical Journal, vol 35 #4, July 1956.

***Erasure-Burst-Correcting Convolutional Codes and Unitary Arrays:***

Elwyn R Berlekamp, "A Class of Convolution Codes", Information and Control vol 6, pp 1-13, 1963.

Carlitz, Roselle, and Scoville, Journal of Combinatorial Theory vol 11, pages 258-271, 1971

***Reed-Solomon Decoding:***

E. R. Berlekamp, Algebraic Coding Theory, New York: McGraw-Hill, 1968 and Laguna Hills, CA: Aegean Park Press, 1984.

E. R. Berlekamp, "Factoring polynomials over large finite fields," Math Computation, Vol 24, No 111, pp 713—735, July 1970.

E. R. Berlekamp and J. L. Ramsey, "Readable erasures improve the performance of Reed-Solomon codes," IEEE Trans Information Theory, Vol IT-24, pp 384—386, 1978.

E. R. Berlekamp, "The technology of error-correcting codes," Proceedings of the IEEE, Vol 68, pp 564—593, 1980.

E. R. Berlekamp, "Bit-serial Reed-Solomon encoders," IEEE Trans Information Theory, Vol IT28, pp 869—874, 1982.

E. R. Berlekamp, G. Seroussi, and P. Tong, "Hypersystolic Reed-Solomon decoder," U. S. Patent 4,958,348, issued September 18, 1990.

R. E. Blahut, Theory and Practice of Error Control Codes, Reading MA: Addison-Wesley, 1983.

G. D. Forney, "Generalized minimum distance decoding," IEEE Trans Information Theory, Vol IT12, pp 125—131, 1966.

J. Justesen, "On the complexity of decoding Reed-Solomon codes," IEEE Trans Information Theory, Vol IT22, pp 237—238, 1976.

D. E. Knuth, The Art of Computer Programming—Sorting and Searching, Vol 3, Reading, MA: Addison-Wesley, 1973.

J. L. Massey, "Shift register synthesis and BCH decoding," IEEE Trans Information Theory, Vol IT15, pp 122—127, 1969.

R. J. McEliece, The Theory of Information and Coding, Vol 3 of G-C Rota, ed., Encyclopedia of Mathematics and Its Applications, Reading MA: Addison-Wesley, 1981.

M. Morii and Kasahara, M, "Generalized key-equation of Remainder Decoding Algorithm for Reed-Solomon codes," IEEE Trans Information Theory, Vol IT38, pp 1801—1807, 1992.

N. J. Patterson, "Algebraic decoding of Goppa codes," IEEE Trans Information Theory, Vol IT21, pp 203—207, March 1975.

W. W. Peterson, Error-Correcting Codes, Cambridge, MA: MIT Press, 1961.

Y. Sugiyama, M. Kasahara, S. Hirasawa, and T. Namekawa, "A method for solving key equation for decoding Goppa codes," Information & Control, Vol 27, pp 87—99, 1975.

L. R. Welch and E. R. Berlekamp, "Error correction for algebraic black codes," U. S. Patent Number 4,633,470, issued Dec 30, 1986.

J. K. Wolf, "Adding two information symbols to certain nonbinary BCH codes and some applications," Bell System Tech J, Vol 48, No 7, pp 2405—2424, Sep 1969.

***Games:***

J. H. Conway, "On Numbers and Games", Academic Press, London & New York, 1976

E. R. Berlekamp, J. H. Conway, and R. K. Guy, "Winning Ways", Academic Press, 1982

E. R. Berlekamp, Blockbusting and Domineering, Journal of Combinatorial Theory, 49(1):67-116, September 1988.

E. R. Berlekamp and D. Wolfe, "Mathematical Go: Chilling Gets the Last Point", AK Peters Ltd, Wellesley, 1994.