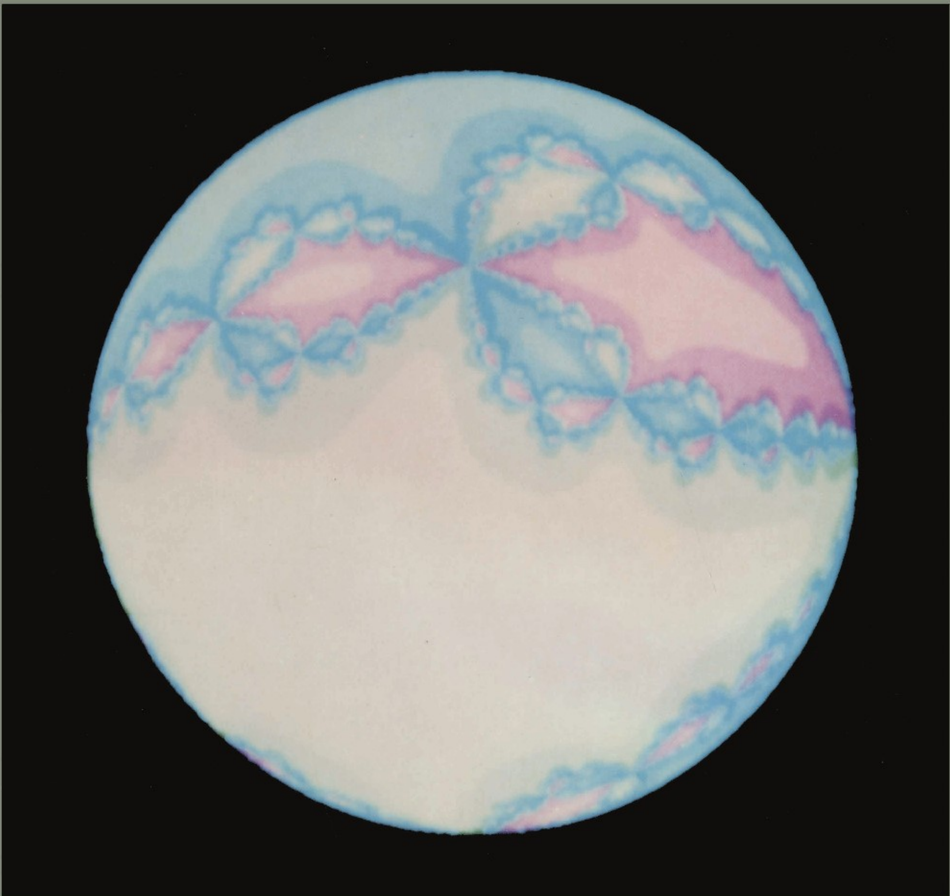
Thomas M. Cover / B. Gopinath

Editors

Open Problems in Communication and Computation



Springer-Verlag

Open Problems in Communication and Computation

Thomas M. Cover B. Gopinath
Editors

Open Problems in Communication and Computation

With 28 Illustrations

Springer-Verlag
New York Berlin Heidelberg
London Paris Tokyo

Thomas M. Cover
Departments of Electrical
Engineering and Statistics
Stanford University
Stanford, California
USA

B. Gopinath
Systems Principles Research
Bell Communications Research
Morristown, New Jersey
USA

Cover illustration: A Julia set mapped onto the unit sphere from the complex plane; generated by Christian Götze in IC* Laboratory at Bellcore.

Library of Congress Cataloging in Publication Data
Open problems in communication and computation.
Includes index.
1. Statistical communication theory. 2. Information theory. 3. Computational complexity.
I. Cover, T.M. II. Gopinath, B.
TK5102.5.O243 1987 001.53'9 87-23326

The text was prepared by the editors using software available on a Vax 11/780 running the UNIX™ operating system.
Printed and bound by R.R. Donnelley & Sons, Harrisonburg, Virginia.
Printed in the United States of America.

9 8 7 6 5 4 3 2 1

ISBN-13: 978-1-4612-9162-6 e-ISBN-13: 978-1-4612-4808-8
DOI: 10.1007/978-1-4612-4808-8

CONTENTS

CHAPTER I.
INTRODUCTION

Thomas M. Cover and B. Gopinath

The papers in this volume are the contributions to a special workshop on problems in communication and computation conducted in the summers of 1984 and 1985 in Morristown, New Jersey, and the summer of 1986 in Palo Alto, California. The structure of this workshop was unique: no recent results, no surveys. Instead, we asked for outstanding open problems in the field. There are many famous open problems, including the question

$$P = NP?,$$

the simplex conjecture in communication theory, the capacity region of the broadcast channel, and the two-helper problem in information theory.

Beyond these well-defined problems are certain grand research goals. What is the general theory of information flow in stochastic networks? What is a comprehensive theory of computational complexity? What about a unification of algorithmic complexity and computational complexity? Is there a notion of energy-free computation? And if so, where do information theory, communication theory, computer science, and physics meet at the atomic level? Is there a duality between computation and communication? Finally, what is the ultimate impact of algorithmic complexity on probability theory? And what is its relationship to information theory?

The idea was to present problems on the first day, try to solve them on the second day, and present the solutions on the third day. In actual fact, only one problem was solved during the meeting -- El Gamal's problem on noisy communication over a common line. This was solved by Gallager. Shortly thereafter, however, Hajek solved two of Cover's problems. Also, a number of partial solutions were achieved. Nonetheless, most of the open problems remain open. The solved problems are included in this volume in the special section at the end. The reader will note that some of the contributions actually consist of open and shut problems. Perhaps that is as it should be. It can't be helped that some of these researchers are able to solve their own problems.

The list of authors includes some of the outstanding contributors to the theory of communication and computation. This list includes many young researchers as well.

The open problems are presented by topic, roughly divided into communication and computation problems, with appropriate introductory notes where needed. A section of solutions follows.

Perhaps the most entertaining of all the contributions is Conway's fascinating article on FRACTRAN, a strange collection of numbers, which when operated on in a simple way, yield all possible computations. We begin with his article.

Acknowledgment: The editors wish to thank Lauren Suess for coordinating the submissions of the open problems for this book and for her part in organizing SPOC'84 and '85, and Anne Oakley for her help during 1986 and 1987.

Special thanks go to Kathy Adams for putting the manuscript in final book form, the handling of the final author communications, and her part in organizing SPOC'86.

We also wish to thank Bell Communications Research and Stanford University for financial support of the meetings.

CHAPTER II.

FRACTRAN

FRACTRAN is not really an open problem. Nonetheless, its recreational spirit typifies the ideas in this collection.

FRACTRAN: A SIMPLE UNIVERSAL PROGRAMMING LANGUAGE FOR ARITHMETIC

J.H. Conway

Department of Mathematics
Princeton University
Princeton, NJ 08544

1. Your Free Samples of FRACTRAN.

To play the *fraction game* corresponding to a given list

$$f_1, f_2, \ldots, f_k$$

of fractions and starting integer N, you repeatedly multiply the integer you have at any stage (initially N) by the earliest f_i in the list for which the answer is integral. Whenever there is no such f_i, the game *stops*.

(Formally, we define the sequence $\{N_n\}$ by $N_0 = N$, $N_{n+1} = f_i N_n$, where i $(1 \le i \le k)$ is the least i for which $f_i N_n$ is integral, as long as such an i exists.)

Theorem 1: When PRIMEGAME:

$$\frac{17}{91}\ \frac{78}{85}\ \frac{19}{51}\ \frac{23}{38}\ \frac{29}{33}\ \frac{77}{29}\ \frac{95}{23}\ \frac{77}{19}\ \frac{1}{17}\ \frac{11}{13}\ \frac{13}{11}\ \frac{15}{2}\ \frac{1}{7}\ \frac{55}{1}$$

is started at 2, the other powers of 2 that appear, namely,

$$2^2, 2^3, 2^5, 2^7, 2^{11}, 2^{13}, 2^{17}, 2^{19}, 2^{23}, 2^{29}, \ldots,$$

are precisely those whose indices are the prime numbers, in order of magnitude.

Theorem 2: When PIGAME:

$$\frac{365}{46}\ \frac{29}{161}\ \frac{79}{575}\ \frac{679}{451}\ \frac{3159}{413}\ \frac{83}{407}\ \frac{473}{371}\ \frac{638}{355}\ \frac{434}{335}\ \frac{89}{235}\ \frac{17}{209}\ \frac{79}{122}$$

$$\frac{31}{183}\ \frac{41}{115}\ \frac{517}{89}\ \frac{111}{83}\ \frac{305}{79}\ \frac{23}{73}\ \frac{73}{71}\ \frac{61}{67}\ \frac{37}{61}\ \frac{19}{59}\ \frac{89}{57}\ \frac{41}{53}\ \frac{833}{47}\ \frac{53}{43}$$

$$\frac{86}{41}\ \frac{13}{38}\ \frac{23}{37}\ \frac{67}{31}\ \frac{71}{29}\ \frac{83}{19}\ \frac{475}{17}\ \frac{59}{13}\ \frac{41}{291}\ \frac{1}{7}\ \frac{1}{11}\ \frac{1}{1024}\ \frac{1}{97}\ \frac{89}{1}$$

is started at 2^n, the next power of 2 to appear is $2^{\pi(n)}$, where for

n =	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	...
$\pi(n)$ =	3	1	4	1	5	9	2	6	5	3	5	8	9	7	9	3	2	3	8	4	6	...

For an arbitrary natural number n, $\pi(n)$ is the nth digit after the point in the decimal expansion of the number π.

Theorem 3: Define $f_c(n) = m$ if POLYGAME:

$$\frac{583}{559}\ \frac{629}{551}\ \frac{437}{527}\ \frac{82}{517}\ \frac{615}{329}\ \frac{371}{129}\ \frac{1}{115}\ \frac{53}{86}\ \frac{43}{53}\ \frac{23}{47}\ \frac{341}{46}$$

$$\frac{41}{43}\ \frac{47}{41}\ \frac{29}{37}\ \frac{37}{31}\ \frac{37}{31}\ \frac{299}{29}\ \frac{47}{23}\ \frac{161}{15}\ \frac{527}{19}\ \frac{159}{7}\ \frac{1}{17}\ \frac{1}{13}\ \frac{1}{3}$$

when started at $c2^{2^n}$, stops at 2^{2^m}, and otherwise leave $f_c(n)$ undefined. Then every computable function appears among $f_0, f_1, f_2, \ldots$.

2. The Catalogue.

We remark that the "catalogue numbers" c are easily computed for some quite interesting functions. Table 1 and its notes give f_c for any c whose largest odd divisor is less than $2^{10} = 1024$.

Table 1. The Catalogue

c	All defined values of f_c
0	none
1	$n \to n$
2	$0 \to 1$
4	$0 \to 2$
8	$1 \to 2$
16	$2 \to 3$
64	$1 \to 3$
77	$n \to 0$
128	$0 \to 3$
133	$0 \to 0$
255	$n+1 \to n+1$
256	$3 \to 4$
847	$n \to 1$
37485	$0 \to 0,\ n+1 \to n$
2268945	$n \to n+1$
2^k	$a \to b$ if $2^b - 2^a = k$
$7 \cdot 11^{2^k}$	$n \to k$
$\frac{15}{7} \cdot 1029^{2^{k-1}}$	$n \to n+k$
c_π	$n \to \pi(n)$

In this Table, n denotes an arbitrary non-negative integer.

We also have

$$f_{2^kA} = f_0 \ ;$$

$$f_{2^kB} = f_{2^k} \ ; \ f_{2^kB'} = f_{2^{k+1}} \ ;$$

$$f_{2^kC} = f_{77} \ ; \ f_{2^kC'} = f_{847} \ ;$$

$$f_{2^kD} = f_{133} \ \ (k=0) \ \text{ or } \ f_0 \ \ (k>0) \ ;$$

$$f_{2^kE} = f_{255} \ \ (k=0) \ \text{ or } \ f_{2^k} \ \ (k>0) \ ;$$

where

A	is	any odd number < 1024 not visible below:
B	is	1,3,9,13,17,27,39,45,51,81,105,115,117,135,145,153,155, 161,169,185,195,203,205,217,221,235,243,259,287,289,315, 329,345,351,405,435,459,465,483,507,555,585,609,615,651, 663,705,729,777,861,945,975,987,1017, . . .
B'	is	165,495, . . .
C	is	77,91,231,273,385,455,539,1015, . . .
C'	is	847, 1001, . . .
D	is	133, 285, 399, 665, 855, . . .
E	is	255, ...

Figure 1 gives a c for which $f_c(n)$ is the above function $\pi(n)$

$$
\begin{aligned}
&2^{100!} + 2^{\frac{365}{46}101\cdot 100!} + 2^{\frac{29}{161}101^{2}100!} + 2^{\frac{79}{575}101^{3}100!} + 2^{\frac{7}{451}101^{4}100!}\\
&+ 2^{\frac{3159}{413}101^{5}100!} + 2^{\frac{83}{407}101^{6}100!} + 2^{\frac{473}{371}101^{7}100!} + 2^{\frac{638}{355}101^{8}100!} + 2^{\frac{434}{335}101^{9}100!}\\
&+ 2^{\frac{89}{235}101^{10}100!} + 2^{\frac{17}{209}101^{11}100!} + 2^{\frac{79}{122}101^{12}100!} + 2^{\frac{31}{183}101^{13}100!} + 2^{\frac{41}{115}101^{14}100!}\\
&+ 2^{\frac{517}{89}101^{15}100!} + 2^{\frac{111}{83}101^{16}100!} + 2^{\frac{305}{79}101^{17}100!} + 2^{\frac{23}{73}101^{18}100!} + 2^{\frac{73}{71}101^{19}100!}\\
&+ 2^{\frac{61}{67}101^{20}100!} + 2^{\frac{37}{61}101^{21}100!} + 2^{\frac{19}{59}101^{22}100!} + 2^{\frac{89}{57}101^{23}100!} + 2^{\frac{41}{53}101^{24}100!}\\
&+ 2^{\frac{833}{47}101^{25}100!} + 2^{\frac{53}{43}101^{26}100!} + 2^{\frac{86}{41}101^{27}100!} + 2^{\frac{13}{38}101^{28}100!} + 2^{\frac{23}{37}101^{29}100!}\\
&+ 2^{\frac{67}{31}101^{30}100!} + 2^{\frac{71}{29}101^{31}100!} + 2^{\frac{83}{19}101^{32}100!} + 2^{\frac{475}{17}101^{33}100!} + 2^{\frac{59}{13}101^{34}100!}\\
&+ 2^{\frac{41}{3}101^{35}100!} + 2^{\frac{1}{7}101^{36}100!} + 2^{\frac{1}{11}101^{37}100!} + 2^{\frac{1}{1024}101^{38}100!} + 2^{101^{39}100!}
\end{aligned}
$$

$$3 \times 5^{2^{89\cdot 101!}+2^{90\cdot 101!}} \times 17^{101!-1} \times 23$$

Figure 1. The constant c_π .

3. Avoid Brand X.

Works that develop the theory of effective computation are often written by authors whose interests are more logical than computational, and so they seldom give elegant treatments of the essentially computational parts of this theory. Any effective enumeration of the computable functions is probably complicated enough to spread over a chapter, and we might read that "of course the explicit computation of the index number for any function of interest is totally impracticable." Many of these defects stem from a bad choice of the underlying computational model.

Here we take the view that it is precisely because the particular computational model has no great logical interest that it should be carefully chosen. The logical points will be all the more clear when they don't have to be disentangled by the reader from a clumsy program written in an awkward language, and we can then "sell" the theory to a wider audience by giving simple and striking examples explicitly. (It is for associated reasons that we use the easily comprehended term "computable function" as a synonym for the usual "partial recursive function.")

4. Only FRACTRAN Has These Star Qualities.

FRACTRAN is a simple theoretical programming language for arithmetic that has none of the defects described above.

- *Makes workday really easy!*

FRACTRAN needs no complicated programming manual - its entire syntax can be learned in 10 seconds, and programs for quite complicated and interesting functions can be written almost at once.

- *Gets those functions really clean!*

The entire configuration of a FRACTRAN machine at any instant is held as a single integer - there are no messy "tapes" or other foreign concepts to be understood by the fledgling programmer.

- *Matches any machine on the market!*

Your old machines (Turing, etc.) can quite easily be made to simulate arbitrary FRACTRAN programs, and it is usually even easier to write a FRACTRAN program to simulate other machines.

- *Astoundingly simple universal program!*

By making a FRACTRAN program that simulates an arbitrary other FRACTRAN program, we have obtained the simple universal FRACTRAN program described in Theorem 3.

5. Your PRIMEGAME Guarantee!

In some ways, it is a pity to remove some of the mystery from our programs such as PRIMEGAME. However, it is well said [2] that "A mathematician is a conjurer who gives away his secrets," so we'll now prove Theorem 1.

To help in Figure 2, we have labeled the fractions:

A	B	C	D	E	F	G	H	I	J	K	L	M	N
$\frac{17}{91}$	$\frac{78}{85}$	$\frac{19}{51}$	$\frac{23}{38}$	$\frac{29}{33}$	$\frac{77}{29}$	$\frac{95}{23}$	$\frac{77}{19}$	$\frac{1}{17}$	$\frac{11}{13}$	$\frac{13}{11}$	$\frac{15}{2}$	$\frac{1}{7}$	$\frac{55}{1}$

and we note that $AB = \dfrac{2 \times 3}{5 \times 7}$, $EF = \dfrac{7}{3}$, $DG = \dfrac{5}{2}$.

We let n and d be numbers with $0 < d < n$ and write $n = qd + r \quad (0 \le r < d)$. Figure 2 illustrates the action of PRIMEGAME on the number $5^n\, 7^d 13$. We see that this leads to $5^n\, 7^{d-1}\, 13$ or $5^{n+1}\, 7^n\, 13$ according as d does or does not divide n . Moreover, the only case when a power of 2 arises is as the number $2^n\, 7^{d-1}$ when $d = 1$.

$$
\begin{array}{c}
5^n\, 7^d\, 13 \\
\downarrow (AB)^d\, J \\
2^d\, 3^d\, 5^{n-d}\, 11 \\
\downarrow (EF)^d\, K \\
2^d\, 5^{n-d}\, 7^d\, 13 \\
\downarrow (AB)^d\, J \\
2^{2d}\, 3^d\, 5^{n-2d}\, 11 \\
\downarrow (EF)^d\, K \\
2^{2d}\, 5^{n-2d}\, 7^d\, 13 \\
\downarrow (AB)^d\, J \\
\vdots \\
\downarrow (EF)^d\, K \\
2^{qd}\, 5^r\, 7^d\, 13 \\
\downarrow (AB)^r\, A \\
2^n\, 3^r\, 7^{d-r-1}\, 17
\end{array}
$$

$$
\begin{array}{cc}
r > 0 \swarrow C & I \searrow r = 0 \\
2^n\, 3^{r-1}\, 7^{d-r-1}\, 19 & 2^n\, 7^{d-1} \\
\downarrow (DG)^n\, H & \downarrow L^n\, M^{d-1}\, N \\
3^{r-1}\, 5^n\, 7^{d-r}\, 11 & 3^n\, 5^{n+1}\, 11 \\
\downarrow (EF)^{r-1}\, K & \downarrow (EF)^n\, K \\
5^n\, 7^{d-1}\, 13 & 5^{n+1}\, 7^n\, 13
\end{array}
$$

Figure 2. The action of PRIMEGAME.

It follows that when the game is started at $5^n\, 7^{n-1}\, 13$, it tests all numbers from $n-1$ down to 1 until it first finds a divisor of n, and then continues with n increased by 1. In the process, it passes through a power of 2^n of 2 only when the largest divisor of n that is less than n is $d = 1$, or in other words, only when n is prime.

6. FRACTRAN - Your Free Introductory Offer.

A FRACTRAN program may have any number of lines, and a typical line might have the form

$$\text{line } 13 : \frac{2}{3} \to 7 , \ \frac{4}{5} \to 14 .$$

At this line, the machine replaces the current working integer N by $\frac{2}{3}N$, if this is again an integer, and goes to line 7. If $\frac{2}{3}N$ is not an integer, but $\frac{4}{5}N$ is, we should instead replace N by $\frac{4}{5}N$, and go to line 14. If neither $\frac{2}{3}N$ nor $\frac{4}{5}N$ is integral, we should *stop* at line 13.

More generally, a FRACTRAN program line has the form

$$\text{line } n : \frac{p_1}{q_1} \to n_1 , \ \frac{p_2}{q_2} \to n_2, \ldots , \frac{p_k}{q_k} \to n_k .$$

The action of the machine at this line is to replace N by $\frac{p_i}{q_i}N$ for the least i $(1 \leq i \leq k)$ for which this is integral, and then go to line n_1 ; or, if no $\frac{p_i}{q_i}N$ is integral, to *stop* at line n. (A line with $k = 0$ is permitted and serves as an unconditional stop order.)

A FRACTRAN program that has just n lines is called a FRACTRAN-n program. We introduce the convention that a line that cannot be jumped to counts as a $\frac{1}{2}$-line. (Sensible programs will contain at most one $\frac{1}{2}$-line, the initial line.)

We write

$$[\ \frac{p_1}{q_1} \ \frac{p_2}{q_2} \ \cdots \ \frac{p_k}{q_k} \ ]$$

for the FRACTRAN-1 program

$$\text{line } 1 : \frac{p_1}{q_1} \to 1 \ , \ \frac{p_2}{q_2} \to 1, \ldots, \frac{p_k}{q_k} \to 1 \ .$$

We shall see that every FRACTRAN program can be simulated by a FRACTRAN-1 program which starts at a suitable multiple of the original starting number. With a FRACTRAN-$1\frac{1}{2}$ program, we can make this multiple be 1.

The FRACTRAN-$1\frac{1}{2}$ program

$$\text{line } 0 : \frac{P_1}{Q_1} \to 1 \ , \ \frac{P_2}{Q_2} \to 1, \ldots, \frac{P_j}{Q_j} \to 1$$

$$\text{line } 1 : \frac{p_1}{q_1} \to 1 \ , \ \frac{p_2}{q_2} \to 1, \ldots, \frac{p_k}{q_k} \to 1$$

is symbolized by

$$\frac{P_1}{Q_1} \, \frac{P_2}{Q_2} \ \cdots \ \frac{P_j}{Q_j} \left[\frac{p_1}{q_1} \, \frac{p_2}{q_2} \ \cdots \ \frac{p_k}{q_k} \right] .$$

Note that the FRACTRAN-$1\frac{1}{2}$ program

$$m[\, f_1 f_2 \ \cdots \ f_k \,]$$

started at N, simulates the FRACTRAN-1 program

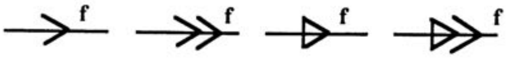
$$[\, f_1 f_2 \ \cdots \ f_k \,]$$

started at mN .

We shall usually suppose tacitly that our FRACTRAN programs are only applied to working numbers N whose prime divisors appear among the factors of the numerators and denominators of the fractions mentioned.

7. Beginners' Guide to FRACTRAN Programming.

It's good practice to write FRACTRAN programs as flowcharts, with a node for each program line and arrows between these nodes marked with the appropriate fractions. We use the different styles of arrowhead



for the options with decreasing priorities from a given node, and if several options with fractions f, g, h at a node have adjacent priorities, we often amalgamate them into a single arrow:

The different primes that arise in the numerators and denominators of the various fractions may be regarded as storage registers, and in a state in which the current working integer is

$$N = 2^a\, 3^b\, 5^c\, 7^d \ldots,$$

we say that

register 2 holds a, or $r_2 = a$
register 3 holds b, or $r_3 = b$
register 5 holds c, or $r_5 = c$
register 7 holds d, or $r_7 = d$
etc.

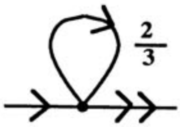
FRACTRAN program lines are then regarded as instructions to change the contents of these registers by various small amounts, subject to the overriding requirement that no register may ever contain a negative number. Thus the line

$$\text{line } 13 : \frac{2}{3} \to 7,\ \frac{4}{5} \to 14$$

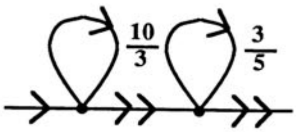
either	*replaces*	r_2 *by* $r_2 + 1$, r_3 *by* $r_3 - 1$	(if $r_3 > 0$)
or	*replaces*	r_2 *by* $r_2 + 2$, r_5 *by* $r_5 - 1$	(if $r_5 > 0$)
or	*stops*		(if $r_3 = r_5 = 0$).

In our figures, unmarked arrows are used when the associated fractions are 1. A tiny incoming arrow to a node indicates that that node will be used as a starting node; a tiny outgoing arrow marks a node that may be used as a stopping node. A few simple examples should convince the reader the FRACTRAN really does have universal computing power. (Readers familiar with Minsky's register machines will see that FRACTRAN can trivially simulate them.)

The program

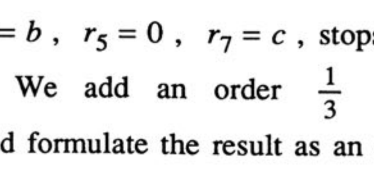


is a destructive adder: when started with $r_2 = a$, $r_3 = b$, it stops with $r_2 = a + b$, $r_3 = 0$. We can make it less destructive by using register 5 as working space: the program



when started with $r_2 = a$, $r_3 = b$, $r_5 = 0$, stops with $r_2 = a + b$, $r_3 = b$, $r_5 = 0$.

By repeated addition, we can perform multiplication: the program



started with $r_2 = a$, $r_3 = b$, $r_5 = 0$, $r_7 = c$, stops with $r_2 = a + bc$, $r_3 = b$, $r_5 = r_7 = 0$. We add an order $\frac{1}{3}$ ("clear 3") at the starting/finishing node and formulate the result as an official FRACTRAN program:

$$\text{line } 1 : \frac{1}{7} \to 2, \ \frac{1}{3} \to 1$$

$$\text{line } 2 : \frac{10}{3} \to 2, \ \frac{1}{1} \to 3$$

$$\text{line } 3 : \frac{3}{5} \to 3, \ \frac{1}{1} \to 1.$$

When started at line 1 with $N = 3^b \, 7^c$, it stops at line 1, with $N = 2^{bc}$. The program obtained by preceding this one by a new

$$\text{line } 0 : \frac{21}{2} \to 0, \ \frac{1}{1} \to 1 \ ,$$

when started at line 0 with $N = 2^n$, stops at line 1 with $N = 2^{n^2}$.

8. How to Use the FRACTRAN-1 Model.

You can use a FRACTRAN-1 machine to simulate arbitrary FRACTRAN programs. You must first clear the given program of loops, in a way we explain later, and then label its lines (nodes) with prime numbers $P, Q, R, \ldots$ larger than any of the primes appearing in the numerators and denominators of any of its fractions. The FRACTRAN-1 program simulates

$$\text{line } P : \frac{a}{b} \to Q, \ \frac{c}{d} \to R, \ \frac{e}{f} \to S, \ldots$$

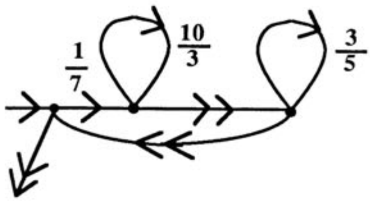
by the fractions

$$\frac{aQ}{bP} \ \frac{cR}{dP} \ \frac{eS}{fP} \quad \ldots$$

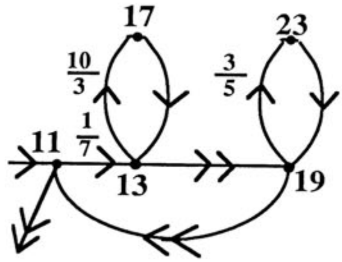
in that order. If the FRACTRAN-0 program when started with N in state P stops with M at line Q , the simulating FRACTRAN-1 program when started a PN stops at QM .

Manufacturer's note. Our guarantee is invalid if you use your FRACTRAN-1 machine in this way to simulate a FRACTRAN program that has loops at several nodes. Such loops may be eliminated by splitting nodes into two.

The third of our examples



becomes



when each of the two nodes with a loop is split in this way, and the new nodes are labeled with the primes 11, 13, 17, 19, 23. Accordingly, it is simulated by the FRACTRAN-1 program

$$[\ \frac{13}{77}\ \frac{170}{39}\ \frac{19}{13}\ \frac{13}{17}\ \frac{69}{95}\ \frac{11}{19}\ ].$$

If started with $N = 2^a\, 3^b\, 7^c\, 11$, this program stops with $N = 2^{a+bc}\, 3^b\, 11$. (The factors of 11 here correspond to the starting and stopping states of the simulated machine.)

We note that it is permissible to label one of the states with the number 1, rather than a large prime number. The fractions corresponding to transitions from this state should be placed (in their proper order) at the *end* of the FRACTRAN-1 program. If this is done, loops, provided they have lower priority than any other transition, are permitted at node 1. Thus the FRACTRAN-1 program

$$[\ \frac{170}{39}\ \frac{19}{13}\ \frac{13}{17}\ \frac{69}{95}\ \frac{1}{19}\ \frac{13}{7}\ \frac{1}{3}\ ]$$

simulates the previous program with a loop order $\frac{1}{3}$ adjoined at the starting/stopping node, which has been relabelled 1. This program, started at $3^b 7^c$, stops at 2^{bc}.

A given FRACTRAN program can always be cleared of loops and adjusted so that 1 is its only stopping node. It follows that we can simulate it by a FRACTRAN-1 program that starts at PN and stops at M when the original program started at N and stopped at M. As we remarked in Section 6, we can simulate this by a FRACTRAN-$1\frac{1}{2}$ program

$$P[\ \cdots\ ]$$

which starts at N and stops at M.

9. Your PIGAME Guarantee.

We now prove Theorem 2, which is equivalent to the assertion that the program

$$[\ \frac{365}{46}\ \frac{29}{161}\ \cdots\ \frac{1}{11}\ \frac{1}{1024}\ ]$$

(obtained by ignoring factors of 97 and dropping the final fraction $\frac{89}{1}$ of PIGAME), when started at $2^n \cdot 89$, stops at $2^{\pi(n)}$. This FRACTRAN-1 program has been obtained from the FRACTRAN program of Figure 3 by the method outlined in the last section. The pairs of nodes 13 & 59, 29 & 71, 23 & 73, 31 & 67, and 43 & 53 were originally single nodes with loops.

We shall only sketch the action of this program, which we separate into three phases. The first phase ends when the program first reaches node 37, the second phase when it first reaches node 41, and the third phase when it finally stops, at node 1.

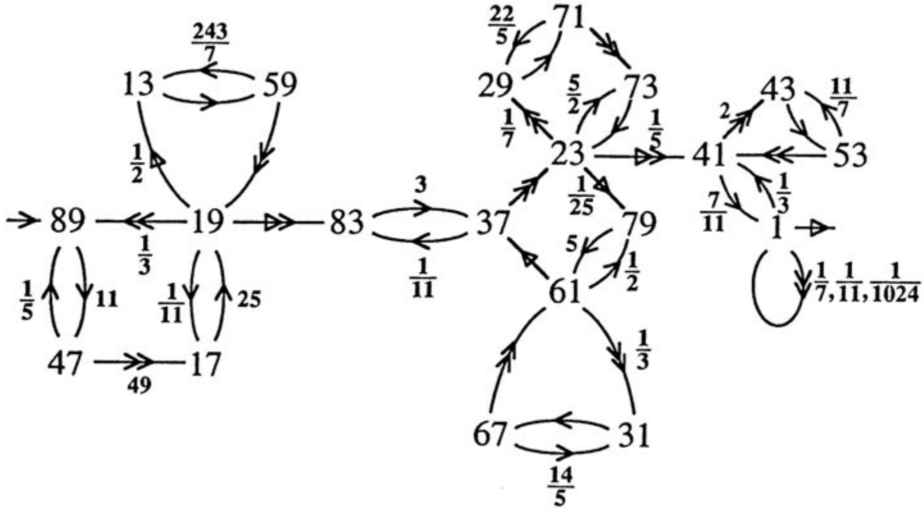


Figure 3. A FRACTRAN program for digits of π .

The first phase, started at 89 with register contents

$$r_2 = n, \;\; r_3 = r_5 = r_7 = r_{11} = 0,$$

reaches 37 with contents

$$r_2 = 0, \;\; r_3 = 1, \;\; r_5 = E, \;\; r_7 = 2 \cdot 10^n, \;\; r_{11} = 0,$$

where E is a very large even number. To see this, ignore the 5 and 11 registers for a moment, and see that it initially sets $r_7 = 2$. Then each pass around the triangular region multiplies r_7 by 5 and puts it into r_3 and is followed by passes around the square region which double r_3 and put it back into r_7. This is done n times, so that at the end of this phase we have $r_7 = 2 \cdot 10^n$, as desired.

The first pass around the square ends with 4 in r_5, and each subsequent pass at least doubles this number, while keeping it even. At the last stage we pass around this region 10^n times and finish with an even number $E \geq 4 \times 2^{10^n}$ in r_5 . It's easy to check that registers 2, 3, and 11 end with the indicated values.

At the end of the second phase, we shall have

$$r_2 = r_5 = r_7 = 0 \ ,$$

$$r_3 = 2 \times 10^n \times E(E-2)(E-2)(E-4)(E-4)(E-6) \cdots 4 \cdot 4 \cdot 2 \cdot 2 \triangleq N \ ,$$

$$r_{11} = 1 \times (E-1)(E-1)(E-3)(E-3)(E-5)(E-5) \cdots 5 \cdot 3 \cdot 3 \cdot 1 \triangleq D \ .$$

This is fairly easy to check, the essential point being that each sojourn in the upper region multiplies r_7 by r_5 and puts it into r_{11} (preserving the value of r_5 but clearing r_7), while in the lower region, we multiply r_3 by r_5 into r_7 in a similar way, and then (at the left) transfer r_{11} back to r_3. Register 5 is decreased by 1 as we pass from the upper to the lower region; but when $r_5 = 1$ we instead clear it and pass to node 41, entering the third phase.

Now *Wallis' product* is

$$\frac{\pi}{2} = \frac{2}{1}\,\frac{2}{3}\,\frac{4}{3}\,\frac{4}{5}\,\frac{6}{5}\,\frac{6}{7}\,\frac{8}{7}\,\frac{8}{9}\,\frac{10}{9}\,\frac{10}{11}\cdots ,$$

in which the successive fractions are obtained by alternately increasing the denominator and numerator. If we truncate it so as only to include all factors whose numerator and denominator are at most K, we obtain an approximation π_K for π which is within at most $\frac{\pi}{K}$ of π. So our $\frac{N}{D} = 10^n \cdot \pi_E$, where π_E is a very good approximation indeed to π. It is in fact so good that the nth decimal digit of π_E is the same as that of π. This digit can be obtained by reducing the integer part of $\frac{N}{D}$ modulo 10, and it is easy to check that the third phase of our program does just this, putting the answer in register 2 and clearing all other registers.

The assertion about the nth decimal digit of π_E is not trivial. For $n = 0$, our approximation π_E is $\pi_4 = \frac{32}{9}$. For $n = 1$ or 2, we have $|\pi_E - \pi| < \frac{\pi}{4 \times 2^{10}}$ which is less than $\frac{1}{1000}$, and since $\pi = 3.141 \cdots$

the nth digits ($n = 1$ and 2) after the decimal point in π_E must both be correct.

For $n \geq 3$, the error in π_E is at most

$$\frac{\pi}{4 \times 2^{10^n}} < \frac{1}{(1000)^{10^{n-1}}} = 10^{-3 \times 10^{n-1}} < 10^{-42n}.$$

The desired assertion now follows from Mahler's [4] famous irrationality measure for π : if $\frac{p}{q}$ (in least terms) is any nonintegral rational number, then

$$| \pi - \frac{p}{q} | > \frac{1}{q^{42}}.$$

10. How to Use Our Universal Program.

In this section, we prove Theorem 3, using an ingenious lemma due to John Rickard. We shall call a FRACTRAN-1 program $[f_1, f_2, \ldots, f_k]$ *monotone* if $f_1 < f_2 < f_3 < \cdots < f_k$.

Lemma: Any FRACTRAN-1 program can be simulated by a monotone one that starts and stops with the same numbers.

Proof. Choose a new prime P that is bigger than the ratio between any two of the f_i and bigger than the inverse of any f_i. Then $[\frac{1}{P}, Pf_1, P^2f_2, P^3f_3, \ldots, P^kf_k]$ simulates $[f_1, f_2, f_3, \ldots, f_k]$ and is monotone. The new program behaves exactly like the old one, except that at each step a power of P is introduced, only to be immediately cleared away before we copy the next step.

We shall call a FRACTRAN-$1\frac{1}{2}$ program

$$f_1^*, f_2^*, \ldots, f_j^* \; [f_1, f_2, \ldots, f_k]$$

monotone if

$$f_1^* < f_2^* < \cdots < f_j^* \text{ and } f_1 < f_2 < \cdots < f_k.$$

Then our universal program simulates monotone FRACTRAN-1$\frac{1}{2}$ programs. It codes such a program by three numbers, M^*, M, and d, defined as follows.

We take d to be any common denominator of all the fractions mentioned and suppose the given FRACTRAN-1$\frac{1}{2}$ program is

$$\frac{m_1^*}{d}\ \frac{m_2^*}{d}\ \cdots\ \frac{m_j^*}{d}\ [\ \frac{m_1}{d}\ \frac{m_2}{d}\ \cdots\ \frac{m_k}{d}\ ].$$

We then adjoin dummy numbers m_{j+1}^* and m_{k+1}, which are both multiples of d and which satisfy

$$m_1^* < m_2^* < \cdots < m_j^* < m_{j+1}^*\ ,\ \ m_1 < m_2 < \cdots < m_k < m_{k+1},$$

$$\text{and}\quad [\ \tfrac{1}{2}\ M^*\ ] \le M$$

where

$$M^* = 2^{m_1^*} + 2^{m_2^*} + \cdots + 2^{m_{j+1}^*}$$

$$M = 2^{m_1} + 2^{m_2} + \cdots + 2^{m_{k+1}}\ .$$

The universal program POLYGAME, started at

$$2^N\ 3^M\ 5^{M^*}\ 17^{d-1}\ 23$$

will simulate the given FRACTRAN-1$\frac{1}{2}$ program, started at N. This universal FRACTRAN-1 program was obtained from the FRACTRAN program shown in Figure 4, and accordingly, we consider starting the latter with $r_2 = N$, $r_3 = M$, $r_5 = M^*$, $r_{17} = d-1$, at the node 23.

This works roughly as follows. After a new N has been found, the program computes successive multiples $N, 2N, 3N, \ldots, mN$, and simultaneously repeatedly halves M to get $[\ M/2\ ], [M/4\ ], \ldots, [\ M/2^m\ ]$. If $[\ M/2^m\ ]$ is odd, so that m is one of the m_i, it sees whether Nm is a multiple of d, and if so resets M and takes a new $N = mN/d$, *unless* m was m_{k+1} (i.e., $[\ M/2^m\ ] = 1$), when it arranges to stop at node 1 with register 2 containing N and all other registers empty. For the first pass, it uses M^* in place of M.

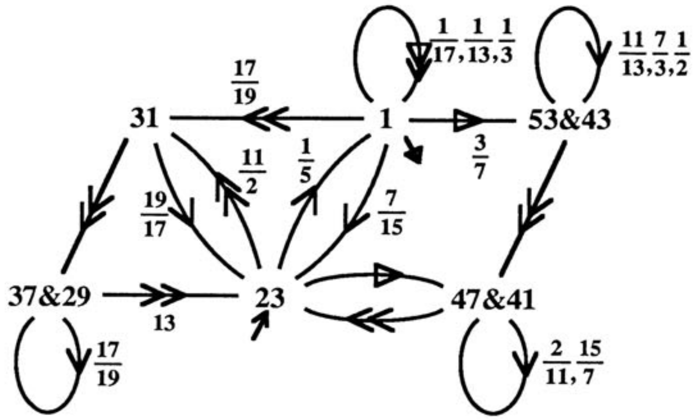


Figure 4. A flowchart for POLYGAME.

Registers 13, 17, 19 function as a counter, whose count is stored in a form from which we can see at once if it is a multiple of d. If

$$r_{13} = q, \ r_{19} = r, \ r_{17} = d - 1 - r, \ \text{with} \ 0 \le r < d ,$$

then *the count* is the number $qd + r$. If the machine arrives at node 31 ("enters the counter") with these values, then when it next arrives at node 23 ("leaves the counter"), we shall have

$$r_{13} = q, \ r_{19} = r + 1, \ r_{17} = d - 1 - (r + 1), \quad \text{if} \ r < d - 1 ,$$

$$r_{13} = q + 1, \ r_{19} = 0, \ r_{17} = d - 1, \quad \text{if} \ r = d - 1 .$$

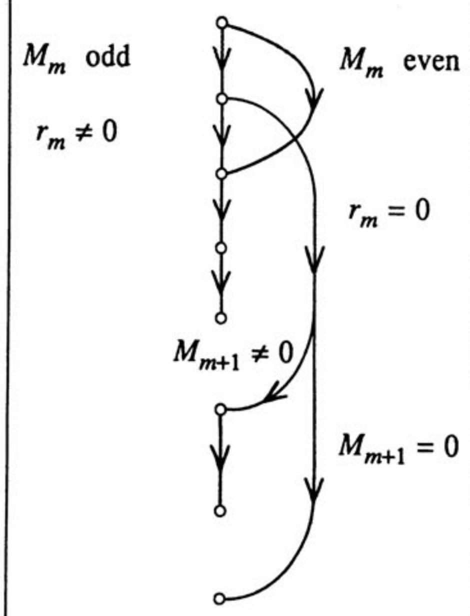
In other words, the value of the count will have increased by 1.

So if the machine is started at 23, with $r_5 = r_{11} = 0$ and $r_2 = N$, it will increase the count by N while transferring N from register 2 to register 11, and then go to node 47 (where its first action will be to retransfer N from register 11 back to register 2).

Table 2. The Action of POLYGAME

node	Contents of registers: 2	3	5	7	11	13	17	19
23	N	M	M_m	0	0	q_m	$d-1-r_m$	r_m
1	N	$M-M_{m+1}$	0	M_{m+1}	0	q_m	$d-1-r_m$	r_m
23	N	$M-M_{m+1}$	0	M_{m+1}	0	q_m	$d-1-r_m$	r_m
47 & 41	0	$M-M_{m+1}$	0	M_{m+1}	N	q_{m+1}	$d-1-r_{m+1}$	r_{m+1}
23	N	M	M_{m+1}	0	0	q_{m+1}	$d-1-r_{m+1}$	r_{m+1}
47 & 41	0	0	0	M	$\frac{mN}{d}$	0	$d-1$	0
23	$\frac{mN}{d}$	M	M	0	0	0	$d-1$	0
1	N	0	0	0	0	0	0	0

action



$$mN = q_m \cdot d + r_m \ (0 \le r_m < d) \qquad M_m = [\, M_0 / 2^m \,]$$

After these remarks, the reader should have little difficulty in verifying the transitions between particular configurations shown in Table 2.

We suppose that for particular positive numbers d, N, M, and M_0 with $[\frac{1}{2} M_0] \leq M$ we define for varying values of m the numbers M_m, q_m, r_m by

$$M_m = [M_0/2^m]$$

$$mN = q_m d + r_m \quad (0 \leq r_m < d).$$

Then Table 2 shows that unless M_m is odd and $r_m = 0$, the special type of configuration in the first line of the table leads to a similar one (in the fifth line) with m increased by 1. In the excepted case, if $M_{m+1} \neq 0$, we obtain another such special configuration (in the seventh line), but with m (and the count) reset to 0, the new initial value $M_0 = M$ for M_m, and $\frac{mN}{d}$ as the new N. If instead M_{m+1} was 0, we arrive at the last line of the table, and *stop* at node 1, with N in register 2 and all other registers empty. The cases with M_m odd and $r_m = 0$ are called *resets*.

Now suppose we start the machine in the special configuration in the top line of the table, with $m = 0$, and the initial value M_0 of M_m set to the number

$$2^{m_0} + 2^{m_1} + \cdots + 2^{m_{k+1}},$$

where

$$m_0 < m_1 < \cdots < m_{k+1}$$

and m_{k+1} is divisible by d. Then before the next reset, we have the equivalences

$$\begin{aligned} M_m \text{ odd} &\iff m \text{ is one of the } m_i \\ r_m = 0 &\iff mN/d \text{ is an integer} \\ M_{m+1} = 0 &\iff m = m_k . \end{aligned}$$

So the next reset will be at the first of the m_i for which $m_i N/d$ is integral, and will *either* replace N by $m_i\, N/d$, and reset m to 0 and M_m to M (if $i < k$), or *stop* at node 1, with N in register 2 and the rest empty $(i = k)$.

This completes the required verifications. Initially, we set $m = 0$ and $M_0 = M^*$, but all subsequent resets will put $M_0 = M$, in accordance with the rules for FRACTRAN-$1\frac{1}{2}$ programs.

A FRACTRAN-1 program is a FRACTRAN-$1\frac{1}{2}$ program with $M = M^*$. For this we can use the alternate catalogue number $7^M\, 17^{d-1}\, 41$.

11. Applications, Improvements, Acknowledgments.

For the function

$$g(N) = \begin{cases} \frac{1}{2}\, N & (N \text{ even}) \\ 3N + 1 & (N \text{ odd}), \end{cases}$$

the *Collatz problem* asks whether for every positive integer N there exists a k for which $g^k(N) = 1$. See [3] for a survey of this problem.

We can ask similar questions for more general *Collatz functions*

$$g(N) = a_N\, N + b_N\ ,$$

where a_N and b_N are rational numbers that only depend on the value of N modulo some fixed number D . We proved in [1] that there is no algorithm for solving arbitrary Collatz problems. Indeed, for any computable function $f(n)$, there is a FRACTRAN-1 program $[f_1\, f_2 \cdots f_k\,]$ with the property that when we start it at 2^n , the first strictly later power of 2 will be $2^{f(n)}$. In other words, we can define f by

$$2^{f(n)} = g^k\, (2^n),$$

where k is the smallest positive integer for which $g^k\, (2^n)$ is a power of 2, and the function $g(N)$, which has the above form, is just $f_i\, N$ for the least i which makes this an integer. This result is an explicit version of *Kleene's Normal Form Theorem*.

We note that $g(N)/N$ is a periodic function with rational values, so that $g(N)$ is a Collatz function for which b_N is always 0. So even for Collatz functions of this special type there can be no decision procedure. By applying the argument to a universal fraction game, we can get a *particular* Collatz-type problem with no decision procedure.

(We remark that of course Collatz problems with arbitrary b_N are harder to solve, rather than easier. We might, for instance, define one that simulates a program written in 10 segments, each segment using only the numbers ending in a given decimal digit, and in which control is transferred between the segments only at certain crucial--and recursively unpredictable--times.)

John Rickard tells me that he has found a seven fraction universal program of type $2^{2^n} \cdot c \to 2^{2^{f(n)}}$ and a nine fraction one of type $2^n \cdot c \to 2^{f(n)}$. However, it seems that his fractions are much too complicated ever to be written down. I used one of Rickard's ideas in Section 10. Mike Guy gave valuable help in computing the catalogue numbers in Section 2. Of course, the responsibility for any errors in these numbers rests entirely with him.

REFERENCES

[1] J.H. Conway, "Unpredictable Iterations," in Proceedings of the Number Theory Conference, Boulder, Colorado, pp. 49-52 (1972).

[2] J.H. Conway, "FRACTRAN - A Simple Universal Programming Language for Arithmetic," *Open Problems Commun. Comput.*, pp. 4-26 (1986).

[3] J.C. Lagarias, "The $3x + 1$ Problem and Its Generalizations," *Am. Math. Monthly*, 92, No. 1, pp. 3-25 (1985).

[4] K. Mahler, "On the Approximation of π," *Indagnationes Math.*, 15, pp. 30-42 (1953).

CHAPTER III.

PROBLEMS IN COMMUNICATION

In this chapter on communication we find many information theoretic problems. Perhaps this is as it should be, since information theory yields some of the extreme points of the theory of communication. Extreme cases tend often to be theoretical and therefore to lend themselves to crisp problem formulation.

Two of the problems have been partially solved. Wyner's problem on the spectra of bounded functions has led to the contribution by Boyd and Hajela in the solution section. Also, Abbas El Gamal's problem on reliable communication of highly distributed information has led to a solution by Gallager, "Computing Parity in a Broadcast Network," appearing in Chapter VI.

Contents

3.1 SOME BASIC MATHEMATICAL PROBLEMS OF MULTIUSER SHANNON THEORY

I. Csiszár

Mathematical Institute of the
Hungarian Academy of Sciences
Budapest, Hungary

At the present state of development of multiuser Shannon theory, the main interest is in single-letter characterizations of achievable rate regions (capacity regions) of various source (channel) networks, such as source coding with side information, multiple descriptions, and broadcast channels. The mathematical background of most such problems is very similar, namely, an entropy or image size characterization in the sense of [1].

1. Entropy Characterization Problem.

For a discrete memoryless multiple source with generic variables $(X, Y_1, \ldots, Y_k)$, find a single-letter characterization of the closure of the set of all $(k+1)$-dimensional vectors of the form

$$\left[\frac{1}{n} H(X^n \mid f(X^n)),\ \frac{1}{n} H(Y_1^n \mid f(X^n)), \ldots, \frac{1}{n} H(Y_k^n \mid f(X^n))\right].$$

Here $n = 1, 2, \ldots$ and f is any function defined on the nth Cartesian power of the range of X.

2. Image Size Characterization Problem.

The η-image size $g_W(A, \eta)$ of a set $A \subset X^n$ over a discrete memoryless channel (DMC) $\{W : X \to Y\}$ is the minimum cardinality of $B \subset Y^n$ such that $W^n(B \mid \mathbf{x}) \geq \eta$ for each $\mathbf{x} \in A$. The problem is to find, for a distribution P on X and DMCs $\{W_i : X \to Y_i\}$, $i = 1, \ldots, k$, a single-letter characterization of the limit of the sets of all $(k+1)$-dimensional vectors

$$\left[\frac{1}{n} \log |A| , \frac{1}{n} \log g_{W_1}(A, \eta), \ldots , \frac{1}{n} \log g_{W_k}(A, \eta) \right] .$$

Here $A \subset X^n$ is any set of P-typical sequences, and $0 < \eta < 1$ is fixed (the result is independent of η).

Both problems are solved for $k = 2$ (cf. [1]) but not for $k \geq 3$. An interesting (unsolved) special case of Problem 2 for $k = 3$ is the following: consider sets $A \subset X^n \times Y^n \times Z^n$ consisting of triples of sequences which are jointly typical with respect to a given distribution on $X \times Y \times Z$. Let A_1, A_2 , and A_3 be the projections of A on X^n, Y^n , and Z^n, respectively. Characterize the vectors (for $n \to \infty$) of form

$$\left[\frac{1}{n} \log |A| , \frac{1}{n} \log |A_1| , \frac{1}{n} \log |A_2| , \frac{1}{n} \log |A_3| \right]$$

or at least those without the first component.

3. Divergence-Characterization Problem.

The analogue of the entropy-characterization problem for Kullback-Leibler divergence is relevant for hypothesis testing problems with communication constraints (cf. [2]). In case $k = 1$, the problem is to characterize, for two double sources with generic variables (X, Y) and $(X, \tilde{Y})$, the closure of the set of all two-dimensional vectors

$$\left[\frac{1}{n} H(f(X^n)), \frac{1}{n} D(P_{f(X^n)\, Y^n} \,\|\, P_{f(X^n)\, \tilde{Y}^n}) \right] .$$

4. Communication Problems with Unfriendly Participants.

This, up to now, less investigated problem area includes jammer problems, Wyner's wiretap channel (cf.[1], p.407), and so on. Entropy and image size characterization problems underly many problems of this kind, as well.

REFERENCES

[1] I. Csiszár and J. Körner, *Information Theory: Coding Theorems for Discrete Memoryless Systems,* Academic, New York, 1981.

[2] R. Ahlswede and I. Csiszár, ''Hypothesis Testing with Communication Constraints,'' *IEEE Trans. Inf. Theory,* July 1986.

3.2 THE INFORMATION THEORY OF PERFECT HASHING

János Körner

Mathematical Institute of the
Hungarian Academy of Sciences
Budapest, Hungary

Fredman and Komlós [1] have used an interesting information-theoretic technique to derive the hitherto sharpest converse (nonexistence) bounds for the problem of perfect hashing. It seems to me that this is the first use of "hard core information theory" in combinatorics.

In a recent paper [2], we have shown that implicit in the Fredman-Komlós proof technique is the concept of graph entropy [3]. This might be interesting because a straightforward use of graph entropy reduces their proof to a few lines. It is convincing to use the example of perfect hashing to discuss possible applications of information theory to combinatorics. Furthermore, I will show that the bound in [1] is not tight.

During the last decade the information theory of discrete memoryless models has become increasingly combinatorial in spirit. It was somewhat disappointing to see that even deep-looking Shannon theory results such as the exponential error bounds can be derived in short order by elementary counting arguments. It is therefore good news that a genuinely information-theoretic technique (not just the subadditivity of entropy) yields new results in combinatorics.

1. Perfect Hash Functions.

Let X be a set of n elements. We shall say that a function $f : X \to B$ separates A if f takes $|A|$ different values on A. The family $\{ f_\pi \}$, $\pi \in \Pi$, of mappings of X into B is a (b,k)-family of perfect hash functions if $|B| = b$ and every k-element subset A of X is separated by at least one function f_π, $\pi \in \Pi$.

What is the minimum size $Y(b, k, n)$ of a (b,k)-family of perfect hash functions for X ? Note that logarithms are to the base 2.

Standard random selection of the hash functions yields

$$Y(b, k, n) \le \frac{b^k}{b^{\underline{k}}} k \log n \ ,$$

where $b^{\underline{k}} \triangleq \prod_{i=0}^{k-1} (b - i)$. Fredman and Komlós [1] have proved that

$$Y(b, k, n) \ge \frac{b^{k-1}}{b^{\underline{k-1}}} \cdot \frac{\log n}{\log (b - k + 2)} \ .$$

It is instructive to study the special case $Y(n) \triangleq Y(3, 3, n)$. Random selection, followed by expurgation, yields

$$Y(n) \le \frac{2 \log n}{\log \frac{9}{7}} \ .$$

The Fredman-Komlós lower bound is

$$Y(n) \ge \frac{3}{2} \log n \ .$$

However, I can prove by elementary counting that

$$Y(n) \ge \frac{\log n}{\log \frac{3}{2}} \ . \tag{1}$$

Indications are strong that even this bound is poor. A combination of the two lower bounding techniques should be possible.† None is uniformly better than the other, but the counting bound can be obtained also by the graph entropy technique, as pointed out by Kati Marton, who was the first to derive bound (1) using that technique.

† It is indeed possible, as shown subsequently by the Körner and Marton [4].

2. Proof of the Counting Bound.

Let a (3,3)-family of perfect hash functions be represented by a set C of ternary sequences of length t. For an arbitrary ternary sequence $\mathbf{x}$ of length t, let $A(\mathbf{x})$ denote the set of all sequences in $\{0, 1, 2\}^t$ that are at maximum distance t from $\mathbf{x}$. Clearly C has the property

$$|A(\mathbf{x}) \cap C| \leq 2. \tag{2}$$

Now, let us count the pairs $\{A(\mathbf{x}), \mathbf{y}\}$, $\mathbf{x} \in \{0, 1, 2\}^t$, $\mathbf{y} \in C$, $\mathbf{y} \in A(\mathbf{x})$. By (2), their number, $|C|$, satisfies

$$|C| \cdot 2^t \leq 2 \cdot 3^t ;$$

hence,

$$t \geq \frac{\log |C|}{\log \frac{3}{2}}$$

which is the desired bound (1).

REFERENCES

[1] M. Fredman and J. Komlós, "On the Size of Separating Systems and Perfect Hash Functions," *SIAM J. Algebraic Discrete Meth.,* 5, No. 1, pp. 61-68 (1984).

[2] J. Körner, "Fredman-Komlós Bounds and Information Theory, *SIAM J. Algebraic Discrete Meth.,* 7, No. 4, pp. 560-570 (1986).

[3] J. Körner, "Coding of an Information Source Having Ambiguous Alphabet and the Entropy of Graphs," Transactions of the 6th Prague Conference on Information Theory, Academia, Prague 1973, pp. 411-425.

[4] J. Körner and K. Marton, "New Bounds for Perfect Hashing via Information Theory," submitted to *Eur. J. Combinatorics.*

3.3 THE CONCEPT OF SINGLE-LETTERIZATION IN INFORMATION THEORY

János Körner

Mathematical Institute of
the Hungarian Academy of Sciences
Budapest, Hungary

Inherent in the definition of Shannon theory problems is an asymptotic characterization of the performance, rates and error probabilities of all possible code constructions in the given context. Then the results one is looking for give so-called single-letter characterizations of these performance measures. Yet nobody has put forward a mathematically valid explanation of the key notion of *single-letter characterization.*

One way of approaching the problem is to speak about *computable* characterizations. Roughly speaking, a characterization is computable if it gives rise to a nice algorithm that computes the underlying quantities to any defined degree of accuracy. This, however, is less than satisfactory for intuition. One of the purposes of Shannon theory is to give a systematic account of all the quantities that can serve as information measures in various contexts and to clarify their relations by identities and inequalities. Because of these formulas, information theory can put an intuitively appealing order into the wealth of facts needed in asymptotic counting arguments often encountered in combinatorial arguments. It is one of the main interests of multiuser information theory to shed light on these relations.

It seems that the theory of association schemes as developed by Bose, Mesner, Delsarte, Schrijver, Babai, and so on or suitable generalizations thereof might provide a structural description for what I believe to be the essence of single-letter characterizations. Theorems involving such a characterization in the book by Csiszár and the author seem to suggest that for the particular problem under consideration, optimal constructions exist in any association scheme isomorphic to the given one; this is true in a somewhat vague asymptotic sense. Then, since the parameters of the underlying association schemes are given above by single-letter quantities, depending as they do only on the joint types, that is, the joint letter frequency distributions of finitely many finite sequences, one will obtain the kind of characterizations one needs.

I would like to see whether there is any hope of converting this into a logically sound theory.

3.4 IS THE MAXIMUM ENTROPY PRINCIPLE OPERATIONALLY JUSTIFIABLE?

I. Csiszár

Mathematical Institute of the
Hungarian Academy of Sciences
Budapest, Hungary

Let X be a random variable originally believed to have distribution Q. When new information is obtained suggesting that the distribution of X actually belongs to a set of distributions Π not containing the original guess Q, this should be updated to conform with the new information. Intuitively a proper updating should be that element of Π which is closest to the original guess Q. It remains to specify the measure of distance between distributions to be used to find this closest element.

The maximum entropy (ME) principle, also called minimum discrimination information principle, suggests use of the Kullback-Leibler informational divergence, defined by $D(P \parallel Q) = \Sigma\, P(x) \log \dfrac{P(x)}{Q(x)}$ in the discrete case and by the corresponding integral in general. Thus ME updating results in that $P^* \in \Pi$ (providing it exists and is unique) which minimizes $D(P \parallel Q)$ subject to $P \in \Pi$. If Q is the uniform distribution, this P^* is just the element of Π having maximum entropy, hence the name. The ME principle has been used successfully in various fields ranging from statistical physics to speech recognition, and it has also been derived axiomatically from some natural postulates. The following result of Csiszár (1984) leads in an operational (rather than postulational) manner to the ME principle and also gives a hint in what situations simple ME updating is justified.

Theorem: Let $X_1, X_2, \ldots$ be i.i.d. random variables with common distribution Q and let Π be a given set of distributions on the common range of the X_i's (satisfying some regularity conditions omitted here). Let

A_n be the event that the empirical distribution of the sample $X_1, \ldots, X_n$ belongs to Π. Then for any fixed m, the conditional joint distribution of $X_1, \ldots, X_m$ under condition A_n approaches for $n \to \infty$ the joint distribution of m i.i.d. random variables with common distribution P^* where P^* minimizes $D(P \| Q)$ subject to $P \in \Pi$.

Problem: Generalize the above result for not necessarily i.i.d. $X_1, X_2, \ldots,$ and for constraints not necessarily on one-dimensional distributions only. More exactly, find possibly general conditions under which the following holds for a stationary ergodic process $X_1, X_2, \ldots$ and a given set Π of distributions on the kth Cartesian power of the common range of the X_i's. Let A_n be the event that the kth order empirical distribution of the sample $X_1, \ldots, X_{n+k-1}$ belongs to Π, and consider the conditional joint distribution of m consecutive random variables $X_{l_n}, X_{l_n+1}, \ldots, X_{l_n+m-S1}$ under the condition A_n. Then if $n \to \infty$ and $l_n \to \infty$, $n - l_n \to \infty$, this conditional joint distribution converges to the m-dimensional distribution of a stationary ergodic process $Y_1, Y_2, \ldots$ whose divergence rate from the given process $X_1, X_2, \ldots$ is minimum subject to the constraint that the k-dimensional distribution of the Y process belongs to Π.

If the X process is finite state Markov, a proposition of this kind was proved by Cover, Choi, and Csiszár [1]. It is conceivable that in statistical physics literature similar results may be available for Gibbs random fields.

REFERENCE

[1] T. Cover, B.S. Choi, and I. Csiszár, "Conditional Limit Theorems under Markov Conditioning," to appear *IEEE Trans. Inf. Theory.*

3.5 EIGHT PROBLEMS IN INFORMATION THEORY

R. Ahlswede

Universität Bielefeld
4800 Bielefeld 1
Germany

1. Multiuser Information Theory.

Problem 1: So far, the capacity regions of multiway channels have been characterized in only a few cases. The main difficulty consists of finding appropriate methods for *single-letterization.*

For complex channels this seems to be a hopeless task. We therefore suggest settling for somewhat less, that is, a description of the capacity region as the limit of information quantities depending on vector-valued random variables such that the speed of convergence in terms of the number of components can be bounded from above. There ought to be a way to do this.

Problem 2: There are nonprobabilistic channels that have never been considered in a multiuser situation. We suggest doing this for the permuting channels, which have been studied in [1].

Problem 3: One of the very challenging problems has been to determine the capacity region of the broadcast channel (Cover, 1972).

The following simpler problem encounters some of the typical difficulties. Suppose that V is a finite set, then a family $\{ E_{ij} : 1 \leq i \leq I , 1 \leq j \leq J \}$ of subsets of V is ε-good if for $A_i = \bigcup_j E_{ij}$ and $B_j = \bigcup_i E_{ij}$

(i) $| A_i \cap E_{i'j} | \leq \varepsilon | E_{i'j} |$ for all j and all $i' \neq i$;

(ii) $| B_j \cap E_{ij'} | \leq \varepsilon | E_{ij'} |$ for all i and all $j' \neq j$.

Derive bounds on I and J in terms of $| V |$ and ε .

Problem 4: Whereas there is an extensive literature on coding schemes for multiway channels with feedback, it seems that there is no theory for multisources in case of feedback. Such a theory should include various search problems such as group testing.

Problem 5: In [2], we studied several source coding problems involving decompositions of $n \times n$ arrays into as few as possible partial transversals such that each transversal has distinct symbols as entries. It is therefore of interest to know the possible lengths of such transversals. In particular we have the following:

Conjecture: Suppose that in an $n \times n$ array no symbol occurs more than n times as an entry. Then there exists a partial transversal of length $n-1$ with distinct symbols. The example $\left(\begin{smallmatrix} ab \\ ba \end{smallmatrix} \right)$ shows that one cannot always expect a transversal of length n .

2. Noiseless Coding for Multiple Purposes.

Consider a Bernoulli source $X^n = (X_1, \ldots, X_n)$. Suppose that there are n persons and that person t is interested in the outcome of X_t ($1 \le t \le n$) . A multiple purpose encoding (or program) shall be a sequence $f = (f_1(X^n), f_2(X^n), \ldots)$ of 0-1 valued functions f_i .

Person t requests sequentially the values of $f_1, f_2, \ldots,$ and stops as soon as he has identified the value of X_t . Let $l(f, t)$ denote the expected number of requests of person t for program f . We are interested in the quantity $L(n) = \min_{f} \max_{1 \le t \le n} l(f, t)$. The choice $f_i(X^n) = X_i$ $(1 \le i \le n)$ gives $l(f, t) = t$ for $1 \le t \le n$. Since $\frac{1}{n} \sum_{t=1}^{n} l(f, t) = \frac{n+1}{2}$ one should do better.

Problem 6: What is the asymptotic growth of $L(n)$? There are obvious generalizations of this problem.

3. Correlation Inequalities.

Correlation inequalities play a role in statistical physics, reliability theory, and so on. A systematic study was made in [3]. Instead of the Boolean operations $\vee$, $\wedge$ usually occurring in those inequalities, one can consider any two operations $\phi, \psi : S \times S \to S$, where S is a finite set. Further progress depends on the solution of the following.

Problem 7: For two maps $\phi_S : S \times S \to S$ and $\phi_T : T \times T \to T$, define the product

$$\phi_{ST} : (S \times T) \times (S \times T) \to S \times T$$

by

$$\phi_{ST}\ ((s_1, t_1), (s_2, t_2)) = (\phi_S(s_1, s_2), \phi_T(t_1, t_2))$$

$$\text{for all} \quad s_1, s_2 \in S, t_1, t_2 \in T\ .$$

Also ϕ associates to $A, B \subset S$ a new set in the Minkowski sense $\phi\ (A, B) \triangleq \{\ \phi\ (a, b) : a \in A, b \in B\ \}$. The pair $(\ \phi, \psi)$ is called *expansive*, if $|\ A\ |\ \ |\ B\ | \leq |\ \phi(A, B)\ |\ \ |\ \psi(A, B)\ |$ for all $A, B \subset S$.

Conjecture ([3]). If $(\ \phi_S, \psi_S)$ and (ϕ_T, ψ_T) are expansive, then the pair of products $(\ \phi_{ST}, \psi_{ST}\ )$ is also expansive.

4. Random Selection and Equidistribution.

Existence proofs by random selection are very popular in combinatorics, information theory, complexity theory and so on. We wonder whether they can be replaced by deterministic procedures, which have certain equidistribution properties. Our ideas are not yet precise. We came across the following number theoretical problem, which does not seem to fit into the classical theory of equidistribution.

Problem 8: Consider, for instance, the sets $A_n \triangleq \{\ \sum_{i=1}^{n} \varepsilon_i\, 5^i :$ $\varepsilon_i \in \{\ 0, 1\ \}\ \}$. Do the sets $A_n(m) \triangleq \{\ k \in A_n : k \equiv m \bmod 2^n\ \}$ satisfy for all $0 \leq m \leq 2^n - 1$ $|\ A_n(m)\ |\ 2^{-n} = O(1)$ (or at least $|\ A_n(m)\ |\ 2^{-n} = 2^{o(n)}$) ?

REFERENCES

[1] R. Ahlswede and A. Kaspi, ''Optimal Coding Strategies for Certain Permuting Channels,'' submitted to *IEEE Trans. Inf. Theory.*

[2] R. Ahlswede, ''Coloring Hypergraphs: A New Approach to Multiuser Source Coding,'' Part I, *J. Combinatorics, Inf. Syst. Sci.* 4, No. 1, pp. 76-115 (1979); Part II, *ibid.* 5, No. 3, pp. 220-268 (1980).

[3] R. Ahlswede and D.E. Daykin, ''Inequalities for a Pair of Maps $S \times S \rightarrow S$ with S a Finite Set,'' *Math. Z.* 165, pp. 267-289 (1979).

3.6 OPTIMUM SIGNAL SET FOR A POISSON TYPE OPTICAL CHANNEL

A.D. Wyner

AT&T Bell Laboratories
Murray Hill, NJ 07974

A simple model of an optical communication channel is the following. The *channel input* is a waveform $x(t)$ which satisfies

$$0 \le a \le x(t) \le b < \infty, \quad 0 \le t < \infty,$$

and the corresponding channel output is a Poisson jump process or counting process $\nu(t)$ with intensity function $x(t)$. Thus $\nu(t)$ is an integer-valued independent increments random process, and

$$\Pr\{\nu(t_1) - \nu(t_2) = k\} = \frac{e^{-\lambda}\lambda^k}{k!},$$

$$k = 0, 1, 2, \ldots, \text{ and } 0 \le t_1 \le t_2 < \infty$$

where

$$\lambda = \int_{t_1}^{t_2} x(t)\, dt.$$

Physically, $x(t)$ represents a photon intensity, and the parameter a (when $a > 0$) is the "dark current" which is always present. The jump process $\nu(t)$ represents photon arrivals at the receiver.

A *signal set* with parameters (M, T, S, P_e) consists of the following:

(a) A set of M waveforms $x_m(t)$, $0 \le t \le T$, $1 \le m \le M$, which satisfy

$$a \le x_m(t) \le b$$

and

$$\frac{1}{T} \int_0^1 x_m(t) = S.$$

(Physically, the parameter S represents average signal power).

(b) A "decoder" mapping D which maps jump processes on $[0,T]$ to $\{1, 2, \ldots, M\}$.

(c) Let ν_0^T be the received jump process $\nu(t), 0 \le t \le T$. Then the "error probability" is

$$P_e = \frac{1}{M} \sum_{m=1}^{M} \Pr \{D(\nu_0^T) \neq m \mid x_m(t) \text{ is the channel input}\}.$$

Our problem, for given $M \ge 2$, $a \le S \le b$, and $T > 0$, is to find the signal set that minimizes P_e .

I have a conjectured solution which will be discussed below.

This problem is reminiscent of that of finding optimal signal sets for the Gaussian channel with additive white noise and no bandwidth constraint. In fact, my conjecture is very close to the famous "simplex conjecture" for that channel but may be more tractable than the Gaussian problem. Here is my conjectured optimal signal set.

Since $a \le S \le b$, we can write $S = \theta a + (1 - \theta)b$. Suppose S, M are such that $\theta = k/M$, for some integer k. We construct our signal set as follows:

Let $N = \binom{M}{k}$, and let A be an $M \times N$ matrix, the columns of which are the N permutations of an M-vector with exactly k a's and $(M-k)$ b's. Thus, for example, for $k = 2$, $M = 4$ (so that $S = \frac{a+b}{2}$), A is the 4×6 matrix

$$A = \begin{bmatrix} b & b & b & a & a & a \\ b & a & a & b & b & a \\ a & b & a & b & a & b \\ a & b & b & a & b & b \end{bmatrix}.$$

Let $A = (a_{mn})$. The signal set is

$$x_m(t) = a_{mn}(t)\,, \qquad \frac{(n-1)T}{N} \le t < \frac{nT}{N}\,,$$

$$1 \le n \le N,\ \ 1 \le m \le M\,.$$

It is easy to check that $\int x_m(t)dt = S$.

Let us define $P_e^*(M,T,S)$ as the minimum P_e attainable for a signal set with parameters M,T,S. For $S = \left[\frac{k}{M}\right] a + \left[-\frac{k}{M}\right] b$, as above, it can be shown [1] that with M, S held fixed as $T \to \infty$

$$\frac{-1}{T} \log P_e^*(M,T,S) \to \left[\frac{k}{M}\right]\left[1 - \frac{k}{M}\right]\left[\sqrt{b} - \sqrt{a}\right]^2 \triangleq E_0. \qquad (1)$$

Thus, as $T \to \infty$, $P_e^*(M,T,S) = \exp\ \{ -E_0 T + o(T) \}$. A similar result holds for arbitrary S. Furthermore, the signal sets defined above satisfy (1).

REFERENCE

[1] A.D. Wyner, "Capacity and Error Exponent for the Direct Detection Optical Channel," submitted to *IEEE Trans. Inf. Theory,* 1987.

3.7 SPECTRA OF BOUNDED FUNCTIONS[†]

A.D. Wyner

AT&T Bell Laboratories
Murray Hill, NJ 07974

We are concerned here with waveforms $x(t)$, $-\infty < t < \infty$, which satisfy an amplitude-constraint, $|x(t)| \le A < \infty$, and their spectra. We pose two open problems. The first is the maximization of the energy of a filtered version of an amplitude-constrained pulse with finite support. The second is the question of how close the power spectral density of a stationary amplitude-constrained random process can be to a flat band-limited spectrum. These questions appear to be difficult, but answers to them will shed light on certain aspects of storage in magnetic media (disks, tapes, etc. which are inherently amplitude limited) and on communication over microwave radio links.

Problem 1: Consider the set of real-valued waveforms $x(t)$, $-\infty < t < \infty$, such that

$$|x(t)| \le 1 \tag{1}$$

and

$$x(t) = 0, \quad t < 0, \quad t > 1 \ . \tag{2}$$

The Fourier transform of $x(\cdot)$ is

$$X|f| = \int_{-\infty}^{\infty} x(t) e^{-i\,2\pi f t}\, dt = \int_0^1 x(t) e^{-i\,2\pi f t}\, dt \ . \tag{3}$$

Let $h(t)$ be the impulse response of an arbitrary linear filter, and let $H(f) = \int_{-\infty}^{\infty} h(t) e^{i 2\pi f t}\, dt$ be the filter transfer function. Then the energy of

[†] See the contribution of Boyd and Hajela in Chapter VI for more on this problem.

the filter output when $x(t)$ is the input is

$$E = \int_{-\infty}^{\infty} | H(f) |^2 | X(f) | \, df . \tag{4}$$

Our problem is to maximize E for fixed $H(f), T,$ over all $x(t)$ satisfying (1) and (2).

Comments. It is easy to show

(a) that if $x(t)$ satisfies (1) and (2) that, under very weak assumptions on $h(t)$, we can attain essentially the same value of E for $x(t)$ taking only the values ± 1 ;

(b)

$$E = \int_0^1 \int_0^1 x(\tau) \, x(s) \, R(\tau - s) \, d\tau ds , \tag{5a}$$

where

$$R(t) = \int_{-\infty}^{\infty} h(t - u) \, h(u) \, du . \tag{5b}$$

Thus when $R(t) \geq 0$, for $0 \leq t \leq 1$ (which happens when $h(t) \geq 0$) , E is maximized with $x(t) = 1$, $0 \leq t \leq 1$. For example, when

$$H(f) = \begin{cases} 1, & |f| < W, \\ 0, & |f| > W, \end{cases} \tag{6a}$$

and $W \leq 1/2$, then

$$R(t) = \frac{(2W)\sin(2\pi Wt)}{(2\pi Wt)} \geq 0, \; -1 \leq t \leq 1 . \tag{6b}$$

Problem 2: Let $x(t)$ be a real-valued stationary random process with $Ex(t) = 0$ and $| x(t) | \equiv A$. Let $R(t) = Ex(t) \, x(t + \tau)$, and let

$$S(f) = \int_{-\infty}^{\infty} R(t) e^{-i2\pi ft} \, dt \tag{7}$$

be the power spectral density of x. We are concerned with how "close" $S(f)$ can be to the "boxcar"

$$B(f) = \begin{cases} A^2/2\ , & |f| \le 1\ , \\ 0\ , & |f| > 1\ . \end{cases} \tag{8}$$

Note that $\int_{-\infty}^{\infty} B(f)df = A^2 = Ex^2(t) = \int_{-\infty}^{\infty} S(f)df$. Specifically, the problem is the maximization of

$$Q \triangleq \int_{-1}^{+1} \log(1 + S(f))\, df\ , \tag{9}$$

over all $S(f)$ realizable as the power spectral density of a random process $x(t)$ for which $|x(t)| = A$.

Comments.

(a) From the concavity of the logarithm,

$$Q \le 2 \log\left[1 + \frac{1}{2}\int_{-1}^{1} S(f)df\right] \le 2 \log\left\{1 + \frac{A^2}{2}\right\}. \tag{10}$$

Equality is achieved when $S(f) = B(f)$.

(b) Let $y(t)$ be a Gaussian random process with $Ey(t) = 0$ and with spectral density $\frac{B(f)}{A^2}$ so that $Ey^2(t) = 1$. Let $x(t) = A\ \mathrm{sgn}(y(t))$. Then $Ex(t) = 0$, and $|x(t)| = A$ (a.s.). It can be shown that the spectral density of $x(\cdot)$ is

$$S(f) \ge \frac{2}{\pi} B(f),\ -\infty < f < \infty\ , \tag{11a}$$

so that

$$Q \ge 2 \log\left\{1 + \frac{A^2}{\pi}\right\}. \tag{11b}$$

Inequalities (10) and (11b) yield estimates on sup Q. I conjecture that the upper bound (10) holds strictly and would sorely love to see a bound tighter than (10).

3.8 A STOCHASTIC DECISION PROBLEM

H.S. Witsenhausen

AT&T Bell Laboratories
Murray Hill, NJ 07974

1. Team Decision Problems.

In a team decision problem there are n agents. Agent i observes random variable Y_i and, as a function of this observation, takes decision u_i from a given set U_i of possible decisions. Denoting the decision function by γ_i, the problem is to choose $(\gamma_1, \ldots, \gamma_n)$ so as to optimize the expectation of a criterion $C(u_1, \ldots, u_n, Z)$, where Z is a random variable and the joint distribution of Z and the Y_i is given [1]. Note that by conditioning one can assume that Z is the n-tuple of all observations Y_i. Outside a few special cases, team problems are of high complexity [2].

If C depends *only* on the decisions, then trivially an optimum or ε-optimum can be achieved by constant decisions, so that the specification of the observations is irrelevant. However, if constraints are imposed on the probability distributions of the u_i, then meaningful and interesting problems result. Such problems come up naturally in diverse applications. The one discussed here originates from research in graph theory [3].

2. Problem Statement.

Let X_i $(i = 1, \ldots, n)$ be independent random variables with (not necessarily identical) nonatomic distributions. Of the n agents, agent i observes the variables *other* than X_i. Thus Y_i is the $(n-1)$-tuple $(X_1, \ldots, X_{i-1}, X_{i+1}, \ldots, X_n)$. The decisions are binary, with $U_i = \{0,1\}$ for all i. (Allowing decisions from the interval [0,1] reduces to the above case.) The constraints are that

$$E\{u_i\} = \alpha_i \quad (i = 1, \ldots, n), \tag{1}$$

where α_i are given constants in [0,1]. The objective is to minimize the expectation of

$$C(u_1, \ldots, u_n) = \sum_{1 \leq i < j \leq n} u_i \, u_j. \tag{2}$$

This is a problem with "lacunary" information pattern, as in [4]. It is trivial for $n < 3$.

For $n = 3$, a closed-form solution for general α_i is already too much to ask. We have, however, an interesting piece of qualitative information [5].

Theorem: When $n = 3$, there exists, for each triple $(\alpha_1, \alpha_2, \alpha_3)$ a quantization of each of the X_i into a three-letter alphabet, such that the agents can make their optimal decisions by using only the quantized form of the variables they observe.

Our questions is: Do similar statements hold for $n > 3$?

REFERENCES

[1] J. Marschak and R. Radner, *Economic Theory of Teams,* Yale University Press, New Haven, CT, 1972.

[2] J.N. Tsitsiklis and M. Athans, ''On the Complexity of Decentralized Decision Making and Detection Problems,'' *IEEE Trans. Automatic Control,* AC-30, pp. 440-446 (1985).

[3] F.R.K. Chung, private communication (1983).

[4] H.S. Witsenhausen, ''Team Guessing with Lacunary Information,'' *Math. Operations Res.,* 8, pp. 110-121 (1983).

[5] H.S. Witsenhausen, ''The Cyclic Minimum Correlation Problem,'' *J. Optimization Theory Appl.,* to appear.

3.9 UNSOLVED PROBLEMS RELATED TO THE COVERING RADIUS OF CODES

N.J.A. Sloane

AT&T Bell Laboratories
Murray Hill, NJ 07974

Some of the principal unsolved problems related to the covering radius of codes are described. For example, although it is almost 20 years since it was built, Elwyn Berlekamp's light-bulb game is still unsolved.

1. Introduction.

Codes with low covering radius have applications in source coding and data compression (see [6]). Although there has been considerable activity in recent years in studying these codes ([2]-[4], [6], [7], [9], [10], [12], [13]), many open questions remain. The following are some of the most important. Other problems may be found in [2] and [6].

2. What Is the Solution to Berlekamp's Light-Bulb Game?

In the Mathematics Department commons room at Bell Labs in Murray Hill there is a light-bulb game built by Elwyn Berlekamp nearly 20 years ago. There are 100 light bulbs, arranged in a 10×10 array. At the back of the box there are 100 individual switches, one for each bulb. On the front there are 20 switches, one for each row and column. Throwing one of the rear switches changes the state of a single bulb, while throwing one of the front switches changes the state of a whole row or column.

Suppose some subset S of the 100 bulbs are turned on using the rear switches. Let $f(S)$ be the minimum number of illuminated bulbs that can now be attained by throwing any sequence of row and column switches. The **problem** is to determine

$$R = \max_{S} f(S).$$

It is known [1] that $32 \leq R \leq 37$.

The preceding problem is in fact equivalent to finding the covering radius of a certain code. Let C be an $[n,k]$ binary, linear code. The *covering radius* R of C is the maximal distance of any vector $x \in F_2^n$ from C, that is,

$$R = \max_{x \in F_2^n} \min_{c \in C} \operatorname{dist}(x, c) . \tag{1}$$

Let us define a *light-bulb* code $L_{a,b}$ to be the $[n = ab,\ k = a + b - 1]$ linear code spanned by the rows and columns of an $a \times b$ rectangular array. Figure 1 shows some typical codewords of $L_{3,3}$ (which might also be called the tic-tac-toe code). Berlekamp's game asks for the covering radius of $L_{10,10}$. Since there are potentially 2^{100} choices for x in (1), a brute force attack will not succeed!

$$\boxed{\begin{matrix}1&1&1\\0&0&0\\0&0&0\end{matrix}} \longleftrightarrow (111\quad 000\quad 000)$$

$$\boxed{\begin{matrix}1&0&0\\1&0&0\\1&0&0\end{matrix}} \longleftrightarrow (100\quad 100\quad 100)$$

$$\boxed{\begin{matrix}0&1&1\\1&0&0\\1&0&0\end{matrix}} \longleftrightarrow (011\quad 100\quad 100)$$

Figure 1. Some codewords in the light-bulb code $L_{3,3}$.

More generally, one may ask for the covering radius $L_{a,b}$. Table 1 gives the known bounds on $L_{a,a}$. For large a it is known ([1], [6]) that

$$\frac{a^2}{2} - \frac{a^{3/2}}{2} + o(\, a^{3/2}\,) \leq R \leq \frac{a^2}{2} - \frac{a^{3/2}}{\sqrt{2\pi}} + o(\, a^{3/2}\,)\ .$$

See also [5] and [9].

Table 1. Covering Radius of Light-Bulb Code $L_{a,a}$, from [1] and [6] (n = length, k = dimension, R = covering radius, $t[\,n,k\,]$ = world record)

a	n	k	R	$t[n,k]$
1	1	1	0	0
2	4	3	1	1
3	9	5	2	2
4	16	7	4	3 or 4
5	25	9	7	5 or 6
6	36	11	?	8-10
7	49	13	≤ 16	12-15
8	64	15	22-23	
9	81	17	≤ 29	
10	100	19	32-37	

My reason for giving Berlekamp's game as the first problem is that it appears that light-bulb codes, and codes closely related to them, such as those in Equations (46) and (47) of [6], often have unusually low covering radii. It would therefore be valuable to have a better understanding of these codes.

A related question is to determine the exact covering radius of the codes obtained by the extended direct sum construction given in (79) and (81) of [6].

3. Is There a Code of Length 15, Dimension 6, and Covering Radius 3?

Two general questions in this subject are: (i) find the smallest possible covering radius $t[n,k]$ of any $[n,k]$ linear code, and (ii) exhibit explicit codes that attain or come reasonably close to this bound (see [6]). The value of $t[n,k]$ is known exactly if $k \leq 5$, or if $n \leq 14$, and a table of bounds on $t[n,k]$ for $n \leq 64$ is given in [6]. The first gap occurs when $n = 15$ and $k = 6$. A [15,6] code exists with $R = 4$, but the best bound only guarantees that $R \geq 3$. **Problem:** Is $t[15,6] = 3$ or 4?

4. Find an Abnormal Linear Code.

The "amalgamated direct sum" construction for constructing codes with low covering radius given in [6] works best when applied to *normal* codes (the definition is given below). It seems likely that almost all linear codes are abnormal, although at present (August 1986) not a single example of an abnormal linear code is known. Every code that has been studied so far has turned out to be normal! **Problem:** Find an abnormal linear code, or prove that all linear codes are normal. Abnormal *nonlinear* codes are known to exist (see [7]).

Definition. Let C be an $[n,k]$ code with covering radius R, and let $C_a^{(i)}$ denote the set of codewords $(c_1, \ldots, c_n) \in C$ with $c_i = a$ (for $i = 1, \ldots, n$ and $a = 0$ or 1). Then C is *normal* if, for some i,

$$\text{dist}\,(x, C_0^{(i)}) + \text{dist}\,(x, C_1^{(i)}) \leq 2R + 1$$

holds for all $x \in F_2^n$. Many classes of codes are known to be normal, including all codes of minimal distance $d \leq 5$, or with dimension $k \leq 5$, or with covering radius $R \leq 2$, or with length $n \leq 14$ (see [3],[7], and [13]).

5. What Is the Covering Radius of a First-Order Reed-Muller Code?

First-order Reed-Muller codes are among the simplest, most elegant, and most important of all codes [8, Chap. 14]. These codes have length $n = 2^m$, dimension $k = m + 1$, and minimal distance 2^{m-1}. For even m , Rothaus [12] showed that

$$R = \frac{n}{2} - \frac{\sqrt{n}}{2}.$$

But for odd m , it is only known in general that

$$\frac{n}{2} - \sqrt{\frac{n}{2}} \leq R < \frac{n}{2} - \frac{\sqrt{n}}{2}$$

(see [2] for references), and for odd $m \geq 15$ that

$$\frac{n}{2} - \frac{27}{32}\frac{\sqrt{n}}{\sqrt{2}} \leq R < \frac{n}{2} - \frac{\sqrt{n}}{2}$$

(Patterson and Wiedemann [10]). **Problem:** Determine R when m is odd.

This problem can be stated another way: Which boolean functions of m arguments are most difficult to approximate by linear functions?

For even m these codes are known to be normal [6]. **Problem:** Show that first-order Reed-Muller codes of length 2^m, m odd, are normal. (This would improve certain asymptotic estimates in [6].)

6. Find the Covering Radius of Cyclic Codes of Length 63.

In searching for codes with low covering radius, it was found that one of the cyclic codes of length 31, the [31,11] five-error-correcting BCH code, has an exceptionally low covering radius, namely, $R = 7$ (see the tables in [4] and [6]). It is likely that some cyclic codes of greater length will also have low R. **Problem:** Determine the covering radius of cyclic codes of lengths 33-63. (Tables of these codes may be found in [11].)

Postscript (November 25, 1986). Peter C. Fishburn and the author have recently solved Berlekamp's game and have determined all the values of R in Table 1.

REFERENCES

[1] T.A. Brown and J.H. Spencer, ''Minimization of ±1 Matrices Under Line Shifts,'' *Colloq. Math.* 23, pp. 165-171 (1971).

[2] G.D. Cohen, M.G. Karpovsky, H.F. Mattson, Jr., and J.R. Schatz, ''Covering Radius-Survey and Recent Results,'' *IEEE Trans. Inf. Theory,* IT-31, pp. 328-343 (1985).

[3] G.D. Cohen, A.C. Lobstein, and N.J.A. Sloane, ''Further Results on the Covering Radius of Codes,'' *IEEE Trans. Inf. Theory,* to appear.

[4] D.E. Downie and N.J.A Sloane, ''The Covering Radius of Cyclic Codes of Length up to 31,'' *IEEE Trans. Inf. Theory,* IT-31, pp. 446-447 (1985).

[5] Y. Gordon and H.S. Witsenhausen, ''On Extensions of the Gale-Berlekamp Switching Problem and Constant of l_p- Spaces,'' *Israel J. Math.,* 11, pp. 216-229 (1972).

[6] R.L. Graham and N.J.A. Sloane, ''On the Covering Radius of Codes,'' *IEEE Trans. Inf. Theory,* IT-31, pp. 385-401 (1985).

[7] K.E. Kilby and N.J.A. Sloane, ''On the Covering Radius Problem for Codes, I and II,'' submitted to *SIAM J. Algeb. Discrete Methods.*

[8] F.J. MacWilliams and N.J.A. Sloane, *The Theory of Error-Correcting Codes,* North-Holland, Amsterdam, 2nd printing, 1978.

[9] H.F. Mattson, Jr., ''An Improved Upper Bound on Covering Radius,'' preprint.

[10] N.J. Patterson and D.H. Wiedemann, ''The Covering Radius of the $(2^{15}, 16)$ Reed-Muller Code is at Least 16276,'' *IEEE Trans. Inf. Theory,* IT-29, pp. 354-356 (1983).

[11] W.W. Peterson and E.J. Weldon, Jr., *Error-Correcting Codes,* M.I.T. Press, Cambridge, MA, 2nd ed., 1972.

[12] O.S. Rothaus, ''On Bent Functions,'' *J. Combinatorial Theory,* 20A, pp. 300-305 (1976).

[13] N.J.A. Sloane, ''A New Approach to the Covering Radius of Codes,'' *J. Combinatorial Theory,* to appear.

3.10 A COMPLEXITY PROBLEM

R. Ahlswede

Universität Bielefeld
4800 Bielefeld 1
Germany

Combinatorial extremal problems involving more than one operation are usually very difficult. Complexity problems fall into this category. We propose here an approach to the construction of monotone Boolean functions of large formula size (and large combinational complexity) via the following extremal problem, which involves only one operation.

Denote by $M^{m,n}$ the set of (0, 1)-matrices with m rows and n columns and define for $A, B \in M^{m,n}$ the matrices $A \vee B$, $A \wedge B$ by

$$(A \vee B)(i, j) = \max\, (A(i, j), B(i, j)) ,$$

$$(A \wedge B)(i, j) = \min\, (A(i, j), B(i, j)), \quad 1 \le i \le m\ ;\ 1 \le j \le n\ . \qquad (1)$$

In terms of the matrices $X_k (1 \le k \le m)$ and $Y_l (1 \le l \le n)$, defined by

$$X_k(i, j) = \delta_{ki}\ ,\ \ Y_l(i, j) = \delta_{lj}\ \ \text{(Kronecker's } \delta\text{)}\ , \qquad (2)$$

one can obviously write for $A \in M^{m,n}$

$$A \ = \bigvee_{(i, j)\,:\,A(i, j) = 1} (X_i \wedge Y_j)\ . \qquad (3)$$

Define now for $A \in M^{m,n}$

$L(A) = 1 +$ minimal number of $\vee$-operations in a formula for A . (4)

Because of the distributive law, formula (3) is in general not best. We exclude this effect by two conditions.

Conjecture. If $A \in M^{m,n}$ satisfies the conditions

(a) There is no 2×2-minor with 1's only

(b) Every row and column has at least one 0

then $L(A) = \| A \|$, the number of 1's in A.

The conjecture says that for these matrices (3) is best. We conjecture the same also for combinational complexity restricted to $\vee$-operations. A positive answer (and its extensions to higher dimensional arrays) in conjunction with constructive results on Zarankiewic's problem would give functions $f : \{ 0, 1 \}^t \to \{ 0, 1 \}$ in NP of high monotone complexity.

3.11 CODES AS ORBITS

R. Ahlswede

Universität Bielefeld
4800 Bielefeld 1
Germany

For a finite set χ and natural n we call $U \subset \chi^n$ m-orbital, if there exist a $V \subset U$, $|V| = m$, and a subgroup G of the symmetric group Σ_n such that

$$V G = U .$$

1. Do there exist codes achieving capacity for the discrete memoryless channel whose code word set is 1-orbital?

This is the case for the list codes of exponentially small list size. Also, the Rate-Distortion function is achievable with 1-orbital codes ([1]). However, we tend to believe that question 1 has a negative answer and ask the following:

2. What is the minimal exponential growth of m such that capacity can be achieved with m-orbital codes?

Whereas the notion of linear codes is limited to very special symmetric channels, the proposed notion of orbital codes avoids these limitations and endows Shannon-sense information theory with a very helpful algebraic structure.

REFERENCE

[1] R. Ahlswede, ''On Orbital Codes,'' in preparation.

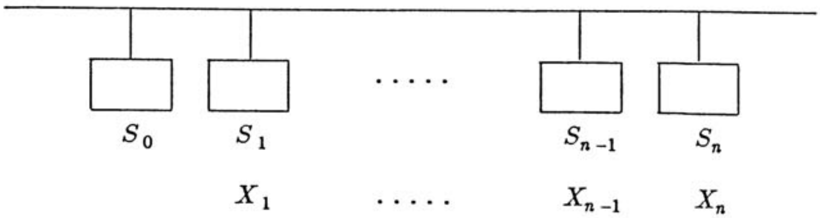
3.12 RELIABLE COMMUNICATION OF HIGHLY DISTRIBUTED INFORMATION[†]

Abbas El Gamal

Department of Electrical Engineering
Stanford University
Stanford, CA 94305

Shannon's theory of information [1] and subsequent generalizations to multiple users (for a survey see [2]) consider the situation of a small number of users each with an unlimited amount of information. The users communicate over a noisy channel with the goal of exchanging their information reliably. Here, we consider a complementary model. We assume a very large number of users, each with a small amount of information. We also assume that the communication takes place over a noisy channel but assume that the goal of the users is to compute a function reliably. This highly distributed information model is motivated by problems of decision making in a network. The users could be either a large number of processors, human beings, or simply the components of a logic circuit. In all cases, the noise is an inevitable physical limitation.

We introduce our model via the following example:



Broadcast Network

[†] See contribution by Gallager in Chapter VI for more on this.

Consider a broadcast network with $(n+1)$ users $S_0, S_1, \ldots, S_n$. User S_i, $1 \le i \le n$, is given the outcome of a Bernoulli(1/2) random variable X_i, that is $X_i \in \{0,1\}$, $P\{X_i = 1\} = 1/2$. The X_i's are all independent. Assume that the network is a binary discrete time broadcast channel and that only one user can send a "0" or a "1" at any time instant t.

Suppose user S_i sends $y \in \{0,1\}$ at time instant t (y naturally depends on X_i and all previously received bits). We consider two noise models:

1. **Transmitter Noise Model:** User S_j, $0 \le j \le n$, receives $y + Z_t$, where $\{Z_t, 1 \le t < \infty\}$ are independent identically distributed Bernoulli(ε) random variables and $+$ is the *mod* 2 addition operation.
2. **Receiver Noise Model:** User S_j, $0 \le j \le n$, receives $y + Z_{jt}$, where $\{Z_{jt}, 1 \le t < \infty, 0 \le j \le n\}$ are independent identically distributed Bernoulli(ε) random variables.

Let $f : \{0,1\}^n \to \{0,1\}$; the goal is to enable S_0 to compute f reliably with the least number of transmissions. More formally, we define a transmission sequence, or a protocol P, as a sequence $a_1, a_2, \ldots, a_M$, $a_i \in \{0, 1, \ldots, n\}$. Before communicating, the users must agree on a protocol to avoid collisions. A protocol is said to be an ε-protocol if at the end of the communication, the probability that S_0 can correctly compute f, P_c, is greater than $(1-\varepsilon)$. The complexity of the set of ε-protocols C_f^ε is the smallest M such that $P_c > 1 - \varepsilon$. The problem is to find C_f^ε and the optimal ε-protocol.

Naturally, C_f^ε will depend on the function f as well as on the noise model. Therefore, we propose the following questions:

Question 1. For each noise model, find the asymptotic growth rate in n of C_f^ε for a random f.

Question 2. Let $f = X_1 + X_2 + \cdots + X_n$, that is, f is the parity of $(X_1, X_2, \ldots, X_n)$. Find C_f^ε for both noise models.

Result. It can easily be shown that the complexity C_f^ε for the parity function under the transmitter noise model is $c(\varepsilon) \cdot n \log n$.

Conjecture 1. The asymptotic growth rate of C_f^ε for a random function f under the transmitter noise model is $n \log n$.

Conjecture 2. Gallager [3] proved an upper bound of $c \cdot n \log \log n$ for C_f^ε of the parity function under the receiver noise model. We conjecture that this bound is tight.

Related Problems.

1. Instead of requiring that S_0 computes f, assume that S_0 wishes to know the $(X_1, \ldots, X_n)$ sequence.
2. Instead of the users communicating over a broadcast network, consider communicating over other types of networks, for example, a ring or tree.
3. Assume that each user S_i, $0 \le i \le n$, is given a random integer $A_i \in \{0,N\}$, $\log N = (1 + \delta) \log n$. The objective is for all users to find the user with the largest integer. In the noiseless case, it can be shown [4] that the number of required transmissions need not exceed $2n$.

REFERENCES

[1] C.E. Shannon, "A Mathematical Theory of Communications," *Bell Syst. Tech. J.*, 27, pp. 379-423 and 623-656 (July and Oct. 1948).

[2] A. El Gamal and T. Cover, "Multiple User Information Theory," *Proc. IEEE*, 68, No. 12, pp. 1466-1483 (Dec. 1980).

[3] R. Gallager, "Computing Parity in a Broadcast Network," in this book.

[4] A. Orlitsky and A. El Gamal, "Broadcast Complexity," in preparation.

3.13 INSTABILITY IN A COMMUNICATION NETWORK

F.P. Kelly

Statistical Laboratory
Cambridge University
Cambridge CB 2ISB
Great Britain

1. Introduction.

The problems described here are concerned with a stochastic model of a communication network. The model represents the interactions between the random demands placed on a network, and the aim is to understand its stationary behavior. In particular, we are interested in any clues that the network may exhibit instabilities, with perhaps various distinct modes of behavior possible.

In Section 2, we describe the model when there is a finite set of channels; it can then be analyzed completely, and a challenge is to extend this analysis to various situations involving an infinite set of channels. In Section 3, we discuss a one-dimensional network which is partially understood and which is believed to be stable. In Section 4, we describe a tree network which is unstable -- it may have more than one stationary distribution. Finally, in Section 5, we describe a two-dimensional network for which there is a conjecture.

The motivation for the problems described here is twofold. First, the model arises naturally in connection with circuit-switching, concurrency control, and some forms of dynamic routing ([2], [3]). Second, the mathematical issues are similar to those that arise in the study of interacting particle systems. There has been enormous progress in this field concerning the relationship between macroscopic phenomena, such as the existence of a phase transition, and the microscopic dynamical description of a system ([4], [5]). This topic is related to the notion of stability in a communication network, and the methods developed may prove useful.

2. A Finite Network.

There is a finite set of channels, labeled $i = 1, 2, \ldots, I$. Channel i provides C_i circuits. Call attempts on route $r \in R$ arise as a Poisson process of rate ν_r, and as r varies, it indexes independent Poisson streams. A call attempt on route r requires A_{ir} circuits from channel i for $i = 1, 2, \ldots, I$. If for any $i \in \{1, 2, \ldots, I\}$ the number of free circuits on channel i is less than A_{ir}, then the call is lost. Otherwise, the call is accepted and occupies simultaneously A_{ir} circuits on channel i, for $i = 1, 2, \ldots, I$, for the holding period of the call. The call holding period is randomly distributed with unit mean and is independent of earlier arrival and holding times. Let $n_r(t)$ be the number of calls in progress at time t on route r, and let $n(t) = (n_r(t), r \in R)$. Then the stochastic process $\{n(t), t \geq 0\}$ has a unique stationary distribution and under this distribution $\pi(n) = P\{n(t) = n\}$ is given by

$$\pi(n) = B \prod_r \frac{\nu_r^{n_r}}{n_r!} \quad n \in S, \tag{1}$$

where

$$S = \{n : \sum_r A_{ir} n_r \leq C_i, \ i = 1, 2, \ldots, I\}$$

and B is a normalizing constant. Note that π does not depend on the distribution of call holding periods. If call holding periods are exponentially distributed, the stochastic process $\{n(t), t \geq 0\}$ is Markov.

3. A One-Dimensional Network.

Next we introduce some spatial structure. Imagine that users are arranged along an infinitely long cable and that a call between two points on the cable $s_1, s_2 \in IR$ involves just that section of cable between s_1 and s_2. Past any point along its length the cable has the capacity to carry simultaneously up to C calls: a call attempt between $s_1, s_2 \in IR$, $s_1 < s_2$, is lost if, past any point of the interval $[s_1, s_2]$, the cable is already carrying C calls. The statistics of call attempts are most easily defined using a space-time diagram (Figure 1). A rectangle $\{(s,t) : s_1 \le s \le s_2,\ t_1 \le t \le t_2\}$ represents a call attempt between points s_1 and s_2 made at time t_1. If accepted, this

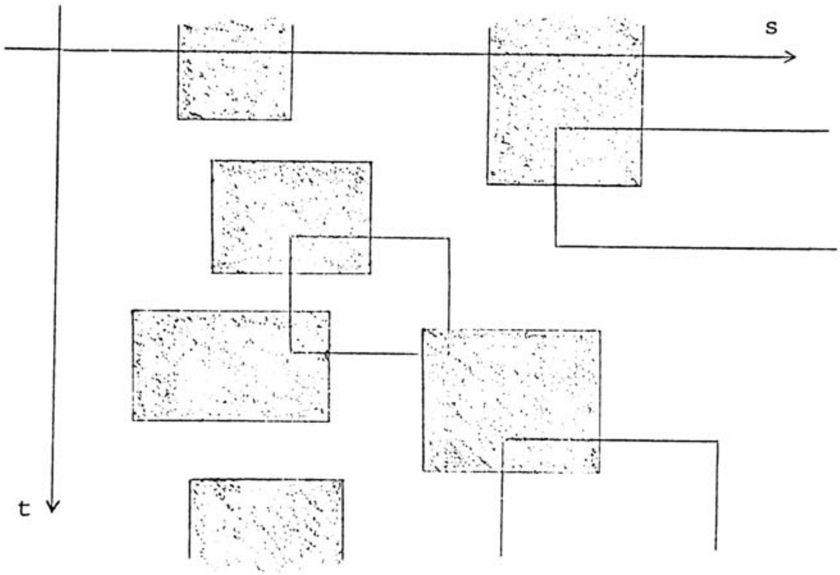


Figure 1. The space-time description of call attempts.

call will last until time t_2. Assume the north-east corners of rectangles are distributed as a Poisson process of rate λ (with respect to Lebesgue measure on IR^2). Assume that heights have unit mean, that widths have a distribution F with finite mean, and that heights and widths are independent of each other and of the positions of north-east corners. Informally, the probability that at time t a call attempt arises connecting a point s to a point $s + z$ is $\lambda\ dt\ ds\ dF(z)$. Let $X(s,t)$ be the number of calls in progress past point s on the cable at time t. It is possible to show that from an initial configuration of calls in progress at time $t = 0$, the space-time diagram defines the stochastic process $\{(X(s,t), s \in IR), t \ge 0\}$ with probability one. It is believed (but has not yet been rigorously proved) that this process has a unique stationary distribution. Some insight into the behavior of the system can be given by describing what is thought to be the unique stationary distribution of $(X(s,t),\ s \in I\!R)$ for a number of special cases. Suppose, for example, that the distribution of call distance F is exponential with parameter μ. Then it is believed that $(X(s,t),\ s \in I\!R)$ has the distribution of a certain Markov chain, stationary with respect to its parameter s, on the finite state space $\{0, 1, \ldots, C\}$. The structure of this Markov chain has been considered in detail by Ziedins [9]: roughly speaking, a Markov chain with transition rates $q(n, n+1) = \lambda$, $n = 0, 1, \ldots,$ $q(n, n-1) = n\,\mu$, $n = 1, 2, \ldots,$ is conditioned on its sample path lying within the set $\{0, 1, 2, \ldots, C\}$ for $s \in [-L, L]$, and then L is let tend to infinity. For a second example, suppose that F is general and that $C = 1$. Then it is believed that $(X(s,t),\ s \in I\!R)$ has the distribution of an alternating renewal process, with the lengths of successive intervals in state 1 (corresponding to calls in progress) having distribution function $\lambda\rho^{-1} \int_0^x e^{-\rho z}\, dF(z)$, and with the lengths of the intervening intervals in state 0 (corresponding to unoccupied stretches of cable) having an exponential distribution with parameter ρ; here ρ is the unique solution to the equation

$$\rho = \lambda \int_0^\infty e^{-\rho z}\, dF(z).$$

The acceptance probability for a call of length x is then

$$e^{-\rho x} \left[1 + \lambda \int_0^\infty z\, e^{-\rho z}\, dF(z) \right]^{-1} .$$

The network described in this section can be truncated and discretized so that it becomes a special case of the network of Section 2. From expression (1) the stationary distributions described above can be obtained as limits: further, the limits are not sensitive to the edge conditions imposed on the truncated network.

4. A Tree Network.

In this section, we describe an example which shows that with a countably infinite set of channels, the network of Section 2 may be unstable. Let V be the infinite tree with m (>2) edges emanating from each vertex. Regard the vertices as channels and suppose that each vertex has m circuits. Call attempts centered at vertex i arise as a Poisson process of rate ν. A call centered at vertex i requires m circuits from vertex i and one circuit from each of the m adjacent vertices. Let $X(i,t) = 1$ if a call centered at vertex i is in progress at time t, and let $X(i,t) = 0$ otherwise. Then the stochastic process $\{(X(i,t), i \in V), \ t \geq 0\}$ has more than one stationary distribution ([2], [4], [7]). Even when attention is restricted to stationary distributions which are invariant under graph isomorphisms, there may be more than one such distribution. For example, there is certainly more than one such distribution when

$$\nu > \frac{1}{m-1} \left[\frac{m-1}{m-2}\right]^m .$$

Variants can be constructed where the underlying graph is a two-dimensional lattice rather than a tree, the model then resembling the Ising model of an antiferromagnet.

5. A Two-Dimensional Network.

Consider now the two-dimensional lattice Z^2. Vertex $i = (i_1, i_2)$ never attempts to call vertex $j = (j_1, j_2)$ unless either $i_1 = j_1$ or $i_2 = j_2$. Call attempts between vertices (i_1, i_2) and (j_1, j_2) arise at rates

$$\frac{1}{2} \lambda (1-q) q^{j_1-i_1-1} \qquad \text{if} \quad i_1 < j_1, i_2 = j_2$$

and

$$\frac{1}{2} \lambda (1-q) q^{j_2-i_2-1} \qquad \text{if} \quad i_1 = j_1, i_2 < j_2.$$

A connected call between two vertices must use the direct (shortest) route between them, passing through each vertex on this route. However, a vertex cannot deal with more than one call terminating at or passing through it, and a call attempt is lost if the associated direct path includes a vertex already handling a call.

The calling rates correspond to a vertex initiating call attempts at rate λ : a call attempt traverses a distance that is geometrically distributed with parameter q in either the east-west or north-south direction. The rates are clearly very special but serve to focus attention on the question of interest. Using a space-time diagram and a percolation bound, it is possible to establish the existence of, and provide a construction for, the stochastic process representing calls in progress at time t. For small enough values of λ , the construction shows that the process has a unique stationary distribution. But what happens for larger values of λ?

Conjecture. There exist values of λ and q such that the process has more than one stationary distribution.

For certain values of λ and q , there may be a translation invariant stationary distribution under which connected calls lie predominantly in a north-south direction; by symmetry, there would then also exist a stationary distribution favoring east-west calls. The conjecture is related to that of Kelbert and Suhov ([1], [8]) who consider a packet-switched network with queueing. The model described here is simpler, possessing a relatively explicit stationary distribution for any finite truncation, and this may make it easier to study. Marbukh [6] has considered a circuit-switched network based on a complete graph and has shown that if blocked calls are redirected along alternative routes, then instabilities may occur. The intuition behind this result is that alternative routes will be longer, use more of the facilities of the network, and thus that above a certain threshold, alternative routing may lead to greater and greater congestion. The intuition for the conjecture here is geometrical: calls fit together more easily when they are aligned.

REFERENCES

[1] M.Ya. Kelbert and Yu.M. Suhov, "Conditions for Existence and Uniqueness of the Full Random Field Describing a State of a Switching Network," *Probl. Pered. Inform.*, 19, pp. 50-71 (1983).

[2] F.P. Kelly, "Stochastic Models of Computer Communication Systems," *J. Roy. Statist. Soc.*, B47, pp. 379-395 (1985).

[3] F.P. Kelly, "Blocking Probabilities in Large Circuit-Switched Networks," *Adv. Appl. Prob.*, 18, pp. 473-505 (1986).

[4] R. Kinderman and J.L. Snell, "Markov Random Fields and Their Applications," *Contemporary Mathematics,* Vol. I, American Mathematical Society, Providence, R.I., 1980.

[5] T.M. Liggett, *Interacting Particle Systems,* Springer-Verlag, New York, 1985.

[6] V.V. Marbukh, "Asymptotic Investigation of a Complete Communications Network with a Large Number of Points and Bypass Routes," *Probl. Pered. Inform.*, 17, pp. 89-95 (1981).

[7] F. Spitzer, "Markov Random Fields on an Infinite Tree," *Ann. Prob.*, 3, pp. 387-398 (1975).

[8] Yu.M. Suhov, "Full Random Field Describing States of a Switching Network," *Fundamentals of Teletraffic Theory,* Proceedings of the Third International Seminar on Teletraffic Theory, 1984. Institute for Problems of Information Transmission of the USSR Academy of Sciences, pp. 410-415.

[9] I. Ziedins, "Quasi-Stationary Distributions and One-Dimensional Circuit-Switched Networks," *J. Appl. Prob.*, 23 (1986).

3.14 CONJECTURE: FEEDBACK DOESN'T HELP MUCH

Thomas M. Cover

Departments of Electrical Engineering
and Statistics
Stanford University
Stanford, CA 94305

Consider the additive Gaussian noise channel with stationary time-dependent noise

$$Y(k) = X(k) + Z(k) \ ,$$

where $\{ Z(k) \}$ has power spectral density $N(f)$. A $(2^{nR}, n)$ feedback code for such a channel is given by a collection of functions

$$x_k^{(n)}(W, Y_1, Y_2, \ldots, Y_{k-1}) \ ,$$

$$k = 1, 2, \ldots, n \ , \quad W \in \{ 1, 2, \ldots, 2^{nR} \}$$

and a decoding function

$$g^{(n)} : \mathbf{R}^n \to \{ 1, 2, \ldots, 2^{nR} \} \ .$$

Throughout we have a power constraint

$$\underset{Y}{E} \frac{1}{n} \sum_{k=1}^{n} (x_k^{(n)} (W, \mathbf{Y}^{k-1}))^2 \leq P \ , \quad \text{for all } W \ .$$

Let

$$Y_k = x_k(W, Y^{k-1}) + Z_k \ ,$$

and let $W^{(n)}$ be uniformly distributed over $\{ 1, 2, \ldots, 2^{nR} \}$. We say that R is an *achievable rate* if there exists a sequence of $(2^{nR}, n)$ codes such that

$$P\{ g^{(n)}(\mathbf{Y}^n) \neq W^{(n)} \} \to 0 \ ,$$

as $n \to \infty$. The *feedback capacity* C_{FB} is defined to be the supremum of the achievable rates. The *nonfeedback capacity* C_{NFB} is defined to be the supremum of achievable rates over all codes $x_k^{(n)}(W)$ not depending on $\mathbf{Y}$.

Clearly, $C_{FB} \geq C_{NFB}$, with equality if $\{ Z_k \}$ is white noise. In general, I hope that a relation like

$$C_{FB}(P) \leq C_{NFB}(2P) \tag{1}$$

is true.

In particular, the above inequality would imply

$$C_{FB} \leq 2C_{NFB} \tag{2}$$

and

$$C_{FB} \leq C_{NFB} + 1/2 \ . \tag{3}$$

The first inequality is interesting at low powers; the last at high powers. Inequality (2) was stated by Pinsker and proved by Ebert [1], while (3) has been proved by Pombra and Cover [2]. But is (1) true?

The investigation hinges on maximization of

$$\frac{1}{n} I(W;\mathbf{Y}) = \frac{1}{n} (h(Y_1, \ldots, Y_n) - h(Z_1, \ldots, Z_n))$$

with and without feedback.

REFERENCES

1. P.M. Ebert, "The Capacity of the Gaussian Channel with Feedback," *BSTJ*, pp. 1705-1712 (Oct. 1970).

2. S. Pombra and T. Cover, "Gaussian Feedback Capacity," to be submitted to *IEEE Trans. Inf. Theory*.

3.15 THE CAPACITY OF THE RELAY CHANNEL

Thomas M. Cover

Departments of Electrical Engineering
and Statistics
Stanford University
Stanford, CA 94305

Consider the following seemingly simple discrete memoryless relay channel:

$$\begin{tikzcd} & Y_1 \arrow[dr, Rightarrow, "C_0"] & \\ X \arrow[ur] \arrow[rr] & & Y_2 \end{tikzcd}$$

Here Y_1, Y_2 are conditionally independent and conditionally identically distributed given X, that is, $p(y_1, y_2 \mid x) = p(y_1 \mid x)\, p(y_2 \mid x)$. Also, the channel from Y_1 to Y_2 does not interfere with Y_2. A $(2^{nR}, n)$ code for this channel is a map $x : 2^{nR} \rightarrow X^n$, a relay function $r : Y_1^n \rightarrow 2^{nC_0}$, and a decoding function $g : 2^{nC_0} \times Y_2^n \rightarrow 2^{nR}$. The probability of error is given by

$$P_e^{(n)} = P\{\, g(r(\mathbf{y}_1), \mathbf{y}_2) \neq W \,\} ,$$

where W is uniformly distributed over 2^{nR} and

$$p(w, \mathbf{y}_1, \mathbf{y}_2) = 2^{-nR} \prod_{i=1}^{n} p(y_{1i} \mid x_i(w)) \prod_{i=1}^{n} p(y_{2i} \mid x_i(w)) .$$

Let $C(C_0)$ be the supremum of the achievable rates R for a given C_0, that is, the supremum of the rates R for which $P_e^{(n)}$ can be made to tend to zero.

We note the following facts:

1. $C(0) = \sup_{p(x)} I(X; Y_2)$.

2. $C(\infty) = \sup_{p(x)} I(X; Y_1, Y_2)$.

3. $C(C_0)$ is a nondecreasing function of C_0 .

What is the critical value of C_0 such that $C(C_0)$ first equals $C(\infty)$?

REFERENCES

[1] T. Cover and A. El Gamal, ''Capacity Theorems for the Relay Channel,'' *IEEE Trans. Inf. Theory,* IT-25, No. 5, pp. 572-584 (Sept. 1979).

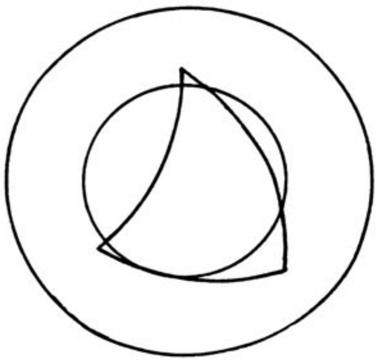
3.16 SIMPLEX CONJECTURE

Thomas M. Cover

Departments of Electrical Engineering
and Statistics
Stanford University
Stanford, CA 94305

It may not be known that the famous simplex conjecture in communication theory can be reduced to the following geometrical problem.

Prove that the spherical simplex in $\mathbf{R}^n$ of surface content Ω that maximizes the content of intersection with a given spherical cap is indeed the regular spherical simplex centered at the center of the cap.



Note: A spherical cap is the intersection of a (translated) half-space with the surface of the (unit) n-sphere. A spherical simplex is the intersection of n half-spaces with the surface of the unit n-sphere.

3.17 ESSENTIAL AVERAGE MUTUAL INFORMATION

Yaser S. Abu-Mostafa

California Institute of Technology
Pasadena, CA 91125

Consider two dependent random variables (S, C) and suppose that $\hat{\chi}$ is the optimal estimate of C when only S is known. $I(S;\, C)$ is a measure of how much S tells us about C, and $I(\hat{\chi}\,;\, C)$ is a measure of how much our optimal estimate $\hat{\chi}$ tells us about C. What can we say about $I(\hat{\chi}\,;\, C)$ if we know that $I(S;\, C) = 3$ bits, for example? The optimality of $\hat{\chi}$ suggests that $I(\hat{\chi}\,;\, C)$ should also be close to 3 bits. This is what we address in this problem. Let (S, C) be jointly distributed $\sim p(s,c)$, where $S = \{\, 0, \ldots, N-1 \,\}$ and $C = \{\, 0, \ldots, M-1 \,\}$. Let $\hat{\chi} : \{\, 0, \ldots, N-1 \,\} \rightarrow \{\, 0, \ldots, M-1 \,\}$ denote an arbitrary function of the outcomes of S. The problem is to estimate the numbers $\alpha(N, M)$ defined by

$$\alpha(N, M) = \inf_{p:I(S;C) > 0} \; \max_{\hat{\chi}=\hat{C}(S)} \left[\frac{I(\hat{\chi}\,;\, C)}{I(S;\, C)} \right]$$

Since $I(\hat{\chi}\,;\, C) \leq I(S;\, C)$ (data processing inequality), $\alpha(N, M) \leq 1$. In fact, $\alpha(N, M) < 1$ for N, M as shown in the following example for $\alpha(3, 2)$.

p(s,c)

C \ S	0	1	2
0	1/3	1/6	0
1	0	1/6	1/3

Either $\hat{\chi}(0) = \hat{\chi}(1)$, $\hat{\chi}(1) = \hat{\chi}(2)$, or $\hat{\chi}(2) = \hat{\chi}(0)$ will make $I(\hat{\chi}\,;\, C) < I(S;\, C)$.

Generalizations.

1. We can think of $\hat{\chi}$ in general as a compression of S. This generalizes $\alpha(N, M)$ to $\alpha(N, M, K)$, where $S = \{ 0, \ldots, N-1 \}$, $C = \{ 0, \ldots, M-1 \}$, and $\hat{\chi} : \{ 0, \ldots, N-1 \} \to \{ 0, \ldots, k-1 \}$.

2. To avoid the cases of very weak dependence between S and C, the minimization domain $(I(S; C) > 0)$ can be restricted to $I(S; C) \geq \delta$ or $I(S; C) \geq \varepsilon H(C)$.

3.18 POINTWISE UNIVERSALITY OF THE NORMAL FORM

Yaser S. Abu-Mostafa

California Institute of Technology
Pasadena, CA 91125

1. Motivation.

The problems posed here arise in the context of combinational complexity of Boolean functions whose truth tables cannot be concisely specified [2]. This class of functions arises in the study of computation and decision-making based on natural data, such as the case of pattern recognition in uncontrolled environments. The main feature of these functions is the lack of a structure that would allow an efficient systematic implementation. This leaves us with a large number of essentially unrelated cases to account for, which puts a lower bound on the complexity of these functions. However, an exhaustive solution is not necessary either, since the essential dimensionality of the data is typically far less than the actual dimensionality.

As an example, consider the problem of recognizing a tree in a visual scene. The input data is a matrix of binary pixels representing the scene, and the Boolean function decides the presence or absence of a tree. It is clear that a visual scene is not a totally random binary matrix; there are many correlations that reduce the entropy. On the other hand, the presence or absence of a tree cannot be formalized in a simple way; the visual object "tree," apart from being a fuzzy notion [12], is an assembly of a large number of loosely related observations. To define a tree is to capture these observations in a model, but the partial randomness due to the way natural objects are made precludes a concise model.

The formalization of these ideas involves defining and relating several quantitative measures on Boolean functions. These measures are the cost C of implementing a function, the entropy H of the data, the randomness

R of the function, and the complexity K which measures the relative complexity of the function as far as simple decomposition is concerned. The measures are based on combinational complexity [11] which is the actual cost of decision-making, Shannon's entropy [10] which measures the essential dimensionality of data, Kolmogorov-Chaitin complexity [4,7] which measures the randomness of strings, and compositional complexity [1] which is defined in terms of the standard pattern recognition system that makes a global decision based on local features. These notions are made precise in the next section.

2. Definitions.

Let N be a positive integer, and consider the set F_N of all Boolean functions f from $\{0,1\}^N$ to $\{0,1\}$. The cardinality of F_N is given by $|F_N| = 2^{2^N}$. The independent Boolean variables will be called $s_1, \ldots, s_N$. All logarithms and exponentials are to the base 2. The four measures, C, H, R, and K, assign to Boolean functions in F_N values ranging from 0 to N bits (approximately), with most of the functions assigned values close to N.

Let n be a non-negative integer. An n-input *universal gate* is a switching device with n input lines and 1 output line that can simulate any Boolean function of n variables, for example, a PROM with n address lines and 1 data line. The *cost* of this gate is defined as 2^n "cells." A combinational circuit Γ is a loop-free interconnection of universal gates where the variables $s_1, \ldots, s_N$ are supplied. The cost of Γ is the sum of the costs of its gates (wires are free, unlimited fan-out). Γ simulates f if f is the output of one of the gates in Γ.

Definition. The *(normalized) cost* C is a real-valued function defined on F_N by

$$C(f) = \log \min\{\text{ cost of } \Gamma : \Gamma \text{ simulates } f\ \} \quad \text{bits} .$$

$C(f)$ differs by at most a constant from the cost based on any other complete basis of switching devices such as 2-input NAND gates. It is clear that $C(f) \leq N$ bits, since an N-input PROM with cost 2^N cells can simulate any function in F_N.

Definition. Let $h(f) \leq 2^{N-1}$ be the number of 1's, or the number of 0's, in the Karnaugh map of f. The *(deterministic) entropy* H is a real-valued function defined on F_N by

$$H(f) = \log \left[1 + h(f)\right] \quad \text{bits.}$$

Clearly, $H(f) \leq N$ bits. The entropy of the constant functions is $\log(1 + 0) = 0$ bits, of the N-input AND function is $\log(1 + 1) = 1$ bit, and of the N-input XOR function is $\log(2^{N-1} + 1) \approx N$ bits. This entropy measure is related to Shannon's entropy (of the ensemble $\{0,1\}^N$ under some probability distribution) by considering only the typical blocks in the Karnaugh map of f.

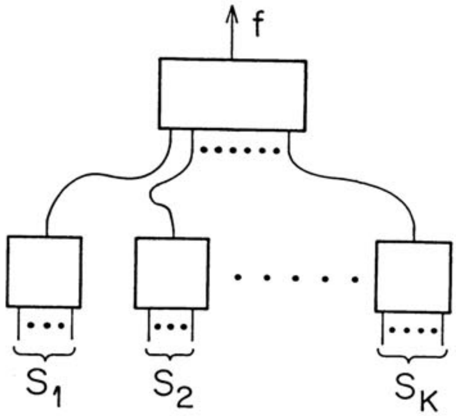
Let $\boldsymbol{\tau}(f)$ be a listing of the truth table of f, that is, $\boldsymbol{\tau}(f) = \tau_0, \tau_1, \ldots, \tau_{2^N-1}$ where τ_k is the value of f when the inputs are the N-bit binary representation of the number k. Let U be a universal Turing machine with input alphabet $\{0,1\}$, and let $\mathbf{p}$ denote the binary program supplied to the tape of U. If, given $\mathbf{p}$, U halts and leaves the binary string $\mathbf{w}$ on the tape, we say that $\mathbf{w} = U(\mathbf{p})$. $|\mathbf{p}|$ denotes the length of $\mathbf{P}$.

Definition. The *randomness* R is a real-valued function defined on F_N by

$$R(f) = \log \min \{ \ |\mathbf{p}| : U(\mathbf{p}) = \boldsymbol{\tau}(f) \ \} \quad \text{bits.}$$

A legal program $\mathbf{p}$ for U consists of an encoding of a Turing machine followed by an input string, hence $|\mathbf{p}|$ is positive and the logarithm is valid. Also, since any string $\boldsymbol{\tau}(f)$ can be generated by a program whose length is a constant (the code of a trivial Turing machine) + the length of the string (namely, 2^N), $R(f)$ is at most $\approx N$ bits. In contrast with the other measures, $R(f)$ is an uncomputable function.

A normal form is a simple decomposition of the Boolean function $f(s_1, \ldots, s_N)$ into $f = g(h_1, \ldots, h_K)$, where the h_k's are Boolean functions depending only on variables within subsets $S_1, \ldots, S_K$ of $\{s_1, \ldots, s_N\}$. A normal form is characterized by the (not-necessarily-distinct) subsets $S_1, \ldots, S_K$ and said to admit a function f if f can be decomposed as above with the h_k's depending on the variables within the S_k's, respectively. The number of functions in F_N admitted by a normal form is denoted by $N(S_1 \cdots S_K)$. For example, if $K = N$ and $S_K = \{s_k\}$, then $N(S_1 \cdots S_N) = 2^{2^N}$. In general, $N(S_1 \cdots S_K)$ expresses the power of the normal form $S_1 \cdots S_K$.



The Normal Form

Definition. The *(normal-form) complexity* K is a real-valued function defined on F_N by

$$K(f) = \log \log \min \{N(S_1 \cdots S_K) : S_1 \cdots S_K \text{ admits } f\} \quad \text{bits.}$$

Since any normal form admits the two constant functions, taking the logarithm twice is valid. Also, since $|F_N| = 2^{2^N}$, $K(f) \leq N$ bits. Having a large value of $K(f)$ means that f cannot be expressed as a function of few arguments each of which depends on few variables. A circuit simulation of the normal form $S_1 \cdots S_K$ consists of K primary universal gates with $|S_1|, \ldots, |S_K|$ inputs, followed by a secondary universal gate with K inputs (see figure). The cost of this circuit is directly related to

$\log N(S_1 \cdots S_K)$ [2], since a universal gate of n inputs costs 2^n cells and simulates 2^{2^n} functions. Therefore, $K(f)$ can be thought of as the (normalized) cost of normal-form simulation of f.

3. Known Relations.

In this section, we state the known pairwise relations between the four measures $C, H, R,$ and K. We shall say that "$A(f) \leq B(f) + o(N)$ for all f" means: Given $\varepsilon > 0$ there is a positive integer N_o such that $N \geq N_o$ and $f \in F_N$ implies that $A(f) \leq B(f) + \varepsilon N$. We shall also say that "$A(f) \leq B(f) + o(N)$ for *almost* all f" means: Given $\varepsilon > 0$ there is a positive integer N_o such that $N \geq 0$ and $0 < \alpha \leq 1$ implies that the ratio between $|\{ f \in F_N : A(f) > B(f) + \varepsilon N \text{ and } (\alpha - \varepsilon) N \leq A(f) < (\alpha + \varepsilon) N\}|$ and $|\{ f \in F_N : (\alpha - \varepsilon) N \leq A(f) \leq (\alpha + \varepsilon) N\}|$ is less than ε. The following relations are proved [2,3] by simulation, enumeration, and construction.

R1: $C(f) \leq H(f) + o(N)$ for all f.
R2: $C(f) \leq R(f) + o(N)$ for *almost* all f.
R3: $C(f) \leq K(f) + o(N)$ for all f.

R4: $H(f) \leq C(f) + o(N)$ for *almost* all, but not all, f.
R5: $H(f) \leq R(f) + o(N)$ for *almost* all, but not all, f.
R6: $H(f) \leq K(f) + o(N)$ for *almost* all, but not all, f.

R7: $R(f) \leq C(f) + o(N)$ for all f.
R8: $R(f) \leq H(f) + o(N)$ for all f.
R9: $R(f) \leq K(f) + o(N)$ for all f.

R10: $K(f) \leq C(f) + o(N)$ for *almost* all f.
R11: $K(f) \leq H(f) + o(N)$ for *almost* all f.
R12: $K(f) \leq R(f) + o(N)$ for *almost* all f.

4. Problems.

Relations R1-R12 of the previous section raise a number of questions about how strongly C, H, R, and K are related. The following questions address stronger versions of relations R2, R10, R11, and R12:

Q1: Is $C(f) \leq R(f) + o(N)$ for all f ?
Q2: Is $K(f) \leq C(f) + o(N)$ for all f ?
Q3: Is $K(f) \leq H(f) + o(N)$ for all f ?
Q4: Is $K(f) \leq R(f) + o(N)$ for all f ?

The answers to these questions, combined with relations R1-R12, determine the exact asymptotic relations between C, H, R, and K. For example, is $|C(f) - K(f)| = o(N)$ for all f ? In other words, is the difference between the minimum cost of an unrestricted simulation and the minimum cost of a normal-form simulation of *any* function f asymptotically negligible w.r.t. N ? Relations R3 and R10 give an affirmative answer to the question in an "almost always" sense. An affirmative answer in an "always" sense would mean that the normal form is a *pointwise universal* (asymptotically optimal for *every* function) structure for simulation of Boolean functions. If the answer is affirmative, more specific questions about the size of the error term $o(N)$ can be addressed. For example, it is easy to see that $|C(f) - K(f)| = \Omega(\sqrt{N})$ for some simple functions such as the N-input XOR. Is $|C(f) - K_M(f)| = 0(N^{1/M})$ for all f, where $K_M(f)$ is based on an M-stage normal form instead of a two-stage normal form?

The answers to Q1-Q4 also yield the answers to other questions of interest. Is $|C(f) - R(f)| = o(N)$ for all f ? An affirmative answer to Q3 bounds the cost of normal-form simulation of a function by the essential dimensionality (entropy) of the function. This would mean that the standard pattern recognition system is asymptotically optimal for the typical pattern recognition problem. Other questions related to the size of the error term $o(N)$ (which is $O(\log N)$ for some, and $O(\sqrt{N})$ for other, of the relations R1-R12) are also of theoretical and practical interest.

REFERENCES

[1] H. Abelson et al., "Compositional Complexity of Boolean Functions," *Discrete Appl. Math.*, 4, pp. 1-10 (1982).

[2] Y. Abu-Mostafa, *Complexity of Information Extraction*, Ph.D. Thesis, Caltech, 1983.

[3] Y. Abu-Mostafa, "Complexity of Random Problems," invited paper, *IEEE International Symposium on Information Theory*, 1985.

[4] G. Chaitin, "A Theory of Program Size Formally Identical to Information Theory," *J. Assoc. Comput. Mach., 22, pp. 329-340 (1975).*

[5] R. Duda and P. Hart, *Pattern Classification and Scene Analysis*, Wiley-Interscience, New York, 1973.

[6] Z. Kohavi, *Switching and Finite Automata Theory*, 2nd ed., McGraw-Hill, New York, 1978.

[7] A. Kolmogorov, "Three Approaches for Defining the Concept of Information Quantity," *Inf. Transmission*, 1, pp. 3-11 (1965).

[8] P. Martin-Lof, "The Definition of Random Sequences," *Inf. Control*, 9, pp. 602-619 (1966).

[9] R. McEliece, *The Theory of Information and Coding*, Addison-Wesley, Reading, MA, 1977.

[10] C. Shannon, "A Mathematical Theory of Communication," *Bell Syst. Tech. J.*, 28, pp. 59-98 (1949).

[11] C. Shannon, "The Synthesis of Two-Terminal Switching Circuits", *Bell Syst. Tech. J.*, 28, pp. 59-98 (1949).

[12] L. Zadeh, "Fuzzy Sets," *Inf. Control*, 8, pp. 338-353 (1965).

3.19 ON CLASSIFICATION WITH PARTIAL STATISTICS AND UNIVERSAL DATA COMPRESSION

Jacob Ziv

Technion
Haifa, Israel

Classification of finite alphabet sources with partial statistics is studied. Efficient universal discriminant functions are introduced and are shown to be closely related to universal data compression.

It is demonstrated that if the probability measure of one of the two sources is not known, it is still possible to find a discriminant function that performs as well as the optimal (likelihood-ratio) discriminant functions (which is computable only if the two measures are fully known). When both measures are not known but training vectors are available from at least one of the two sources, it is shown that no discriminant function can perform efficiently, as long as the length of the training sequence does not grow at least linearly with the length of the classified vector.

Furthermore, a universal discriminant function is introduced and shown to perform efficiently when the length of the training sequence grows linearly with the length of the classified vector.

3.20 ARE BAYES RULES CONSISTENT IN INFORMATION?

Andrew R. Barron

Department of Statistics
University of Illinois
Champaign, IL 61820

Bayes' rule provides a method for constructing estimators of probability density functions in both parametric and nonparametric cases. Let $X_1, X_2, \ldots, X_n$ be a random sample from an unknown probability measure P_0 with density function $p_0(x)$ with respect to a dominating measure $\lambda(dx)$. Let μ be a prior probability measure on the space of all probability measures P which have densities $p(x) = dP/d\lambda$. Then the mean of the posterior yields the following estimator of the density function

$$\hat{p}_n(x) = \hat{p}(x; X_1, X_2, \ldots, X_n) = \frac{\int p(x)(\prod_{i=1}^{n} p(X_i))d\mu}{\int(\prod_{i=1}^{n} p(X_i))d\mu}.$$

To obtain a consistency result, it is natural to require that the prior assigns positive probability to neighborhoods of the true distribution. In particular, we suppose

$$\mu\{ P : D(P_0 \,\|\, P) < \varepsilon \} > 0, \text{ for all } \varepsilon > 0 . \tag{1}$$

Here $D(P_0 \,\|\, P) = \int p_0(x) \log (p_0(x)/p(x)) \,\lambda(dx)$ is the informational divergence (also called relative entropy or Kullback-Leibler number).

1. The Problem.

Determine whether the sequence of Bayes estimators $\hat{p}_n$ converges to the true density p_0 in the sense that

$$\lim_{n\to\infty} E\, D(P_0 \,\|\, \hat{P}_n) = 0.$$

Here the expectation is with respect to P_0. It is also of interest to know whether

$$\lim_{n\to\infty} D(P_0 \,\|\, \hat{P}_n) = 0\ , \quad P_0 \text{ almost surely.}$$

Either result would imply that the sequence of random variables $D(P_0 \,\|\, \hat{P}_n)$ converges to zero in probability.

Remark: An inequality between the information and the L^1 distance $(D(P_0 \,\|\, \hat{P}_n) \geq (1/2)(\int |p_0 - \hat{p}_n|)^2$; see [1]) shows that convergence in information implies convergence of the density estimator in the L^1 sense

$$\lim_{n\to\infty} E \int | p_0(x) - \hat{p}_n(x) | \lambda(dx) = 0.$$

2. Evidence for Consistency.

Does $E\, D(P_0 \,\|\, \hat{P}_n)$ tend to zero? We argue that the answer is yes along a subsequence, yes in the Cesaro sense, and yes if the posterior mean is replaced by a sample average of posterior means.

Lemma 1: *If condition (1) is satisfied then*

$$\liminf_{n\to\infty} E\, D(P_0 \,\|\, \hat{P}_n) = 0\ ;$$

also

$$\liminf_{n\to\infty} D(P_0 \,\|\, \hat{P}_n) = 0\ , \quad P_0 \quad \text{almost surely.}$$

Moreover,

$$\lim_{n\to\infty} \frac{1}{n} \sum_{k=1}^{n} E\, D(P_0 \,\|\, \hat{P}_k) = 0.$$

Lemma 2: *Let $\tilde{p}_n$ be an average of posterior means, that is,*

$$\tilde{p}_n(x; X^n) = \frac{1}{n} \sum_{k=1}^{n} \hat{p}_k(x; X^k)$$

where $X^k = (X_1, \ldots, X_k)$. If condition (1) is satisfied then

$$\lim_{n\to\infty} E\, D(P_0 \,\|\, \tilde{P}_n) = 0.$$

Thus the average $\tilde{p}_n = (1/n)\, \Sigma_{k=1}^{n} \hat{p}_k$ smooths out any humps of large D

that might lead to inconsistency. It is interesting to note that convergence still holds if the kth term in the definition of $\tilde{p}_n$ is replaced by $\hat{p}_k(\cdot\ ; X^{n,k})$, where $X^{n,k}$ is any subset of the n observations of size k.

We note that the posterior mean density is the best possible estimator from the point of view of the Bayes risk (with loss function given by the informational divergence). Thus if any estimator exists which is Bayes risk consistent, then the posterior mean is Bayes risk consistent.

Lemma 3: *Among all probability density estimators based on the data X^n, the posterior mean density estimator $\hat{p}_n(x; X^n)$ minimizes the Bayes risk*

$$R_n = \int E_P\, D(P \,\|\, \hat{P}_n)\, d\mu.$$

Moreover, the Bayes risk R_n is a decreasing sequence. Thus

$$\lim_{n\to\infty} R_n \text{ exists.}$$

It is not known if this limit is zero. Although the average risk is decreasing, the risk $E_P\, D(P \,\|\, \hat{P}_n)$ might *increase* for some P and some n. If we could ensure that $E_{P_0}\, D(P_0 \,\|\, \hat{P}_n)$ were decreasing, then by Lemma 1 we would have $\lim E_{P_0}\, D(P_0 \,\|\, \hat{P}_n) = 0$.

Doob [2] used martingale arguments to establish Bayes consistency results. The drawback is that the results only show convergence for distributions in a set of prior measure one, and there is no known method for determining whether a given distribution is in this set. Nevertheless, the following result is readily obtained.

Lemma 4: *Except for a set of distributions P which has μ measure zero, if condition (1) is satisfied for P then*

$$\lim_{n\to\infty} D(P \,\|\, \hat{P}_n) = 0\ , \quad P \text{ almost surely.}$$

The following result is proved in Barron [3] using the technique of Schwartz [4]. It was first obtained by Freedman [5] in the discrete case (under the extra condition of finite entropy $H(P_0)$).

Lemma 5: *If condition (1) is satisfied then the posterior distribution $\mu_n(\cdot \mid X^n)$ asymptotically concentrates on open neighborhoods of the true distribution P_0, that is,*

$$\lim_n \mu_n(\{P \in N\} \mid X^n) = 1, \ P_0 \ \text{ almost surely.}$$

This result assumes that the neighborhoods N are open with respect to the topology of setwise convergence of probability measures. (For instance, N could be $\{P: \sum_A \mid P_0(A) - P(A) \mid < \varepsilon\}$, where the sum is for A in a countable partition of the sample space.)

Finally, we mention that for parametric problems, Strasser [6] has shown under condition (1) and other mild assumptions that if the maximum likelihood estimator is consistent, then Bayes rules are also consistent. Although consistency in the information sense is not usually addressed in the parametric setting, the usual conditions for the consistency of the MLE are sufficiently restrictive that convergence of the parameter estimators $\hat{\theta} \to \theta$ implies $D(P_\theta \,\|\, P_{\hat{\theta}}) \to 0$.

3. Evidence Against Consistency.

In Barron [7] it will be shown that there exist priors which satisfy (1),

$$\mu\{P: D(P_0 \,\|\, P) < \varepsilon\} > 0 \ \text{ for all } \varepsilon > 0,$$

yet the posterior distribution given X^n asymptotically concentrates outside D neighborhoods of the true P_0, that is, for some $\varepsilon > 0$,

$$\lim_n \mu_n(\{P: D(P_0 \,\|\, P) < \varepsilon\} \mid X^n) = 0, \ P_0 \ \text{ almost surely.}$$

Proof of Lemma 1 and Lemma 2. Let P^n denote the product measure with joint probability density function $p(x^n) = \prod_{i=1}^n p(x_i)$ and let M^n denote the mixture of these distributions obtained using the prior μ. This mixture has joint density function

$$m(x^n) = \int p(x^n)\, d\mu.$$

We first show that condition (1) implies that the informational divergence between P_0^n and M^n has a rate tending to zero; that is,

$$\lim_{n\to\infty} \frac{1}{n} D(P_0^n \,\|\, M^n) = 0.$$

Given $\varepsilon > 0$, let $N = \{ P : D(P_0 \,\|\, P) < \varepsilon \}$. Now the divergence rate is

$$\frac{1}{n} D(P_0^n \,\|\, M^n) = \frac{1}{n} E \log \frac{p_0(X^n)}{\int p(X^n) d\mu} \le \frac{1}{n} E \log \frac{p_0(X^n)}{\int_N p(X^n) d\mu}$$

$$= \frac{1}{n} E \log \frac{p_0(X^n)}{\int_N p(X^n) d\mu / \mu(N)} + \frac{1}{n} \log \frac{1}{\mu(N)}.$$

Here all the expectations are with respect to P_0^n. By the convexity of the informational divergence this is

$$\le \int_N \frac{1}{n} D(P_0^n \,\|\, P^n)\, d\mu/\mu(N) + \frac{1}{n} \log \frac{1}{\mu(N)}$$

$$= \int_N D(P_0 \,\|\, P)\, d\mu/\mu(N) \;+ \frac{1}{n} \log \frac{1}{\mu(N)}.$$

By the definition of N this is

$$\le \;\; \varepsilon \quad + \quad \frac{1}{n} \log \frac{1}{\mu(N)}.$$

Letting $n \to \infty$ then $\varepsilon \to 0$ shows that indeed

$$\lim_{n\to\infty} \frac{1}{n} D(P_0^n \,\|\, M^n) = 0.$$

Now we need to relate this to the convergence of density estimators.

Let $\hat{p}_n(x_{n+1})$ be our density estimate at the point x_{n+1} based on the data $X^n = x^n$. We can write this as

$$\hat{p}_n(x_{n+1}) = \frac{\int p(x_{n+1}, x^n) d\mu}{\int p(x^n) d\mu} = \frac{m(x_{n+1}, x^n)}{m(x^n)} = m(x_{n+1} \mid x^n).$$

The last expression is sometimes called the predictive density. It is the conditional density function for X_{n+1} given X^n. Note that with respect to M^n the data $X_1, X_2, \ldots, X_n$ are no longer independent (but they are exchangeable).

Now by the chain rule

$$\frac{1}{n} D(P_0^n \| M^n) = \frac{1}{n} \sum_{k=1}^{n} E \log \frac{p_0(X_k)}{m(X_k \mid X^{k-1})}.$$

The terms in the sum are just $E\, D(P_0 \| \hat{P}_k)$. Thus

$$\frac{1}{n} D(P_0^n \| M^n) = \frac{1}{n} \sum_{k=1}^{n} E\, D(P_0 \| \hat{P}_k).$$

But we have shown that condition (1) implies that this tends to zero. Thus the $E\, D(P_0 \| \hat{P}_n)$ tends to zero in the Cesaro sense. Since the terms are positive this implies that we have convergence to zero along a subsequence. This implies convergence in probability along a subsequence and hence almost sure convergence along a further subsequence. This completes the proof of Lemma 1.

For Lemma 2, use the convexity of divergence once more to obtain

$$E\, D(P_0 \| \tilde{P}_n) = E\, D(P_0 \| \frac{1}{n} \sum \hat{P}_k) \leq \frac{1}{n} \sum_{k=1}^{n} E\, D(P_0 \| \hat{P}_k)$$

which tends to zero. This completes the proof.

REFERENCES

[1] I. Csiszár, ''Information-type Measures of Difference of Probability Distributions and Indirect Observations,'' *Studia Sci. Math. Hungar.* 2, pp. 299-318 (1967).

[2] J.L. Doob, ''Application of the Theory of Martingales,'' *Colloq. Int. CNRS*, pp. 22-28 (1949).

[3] A.R. Barron, ''Discussion on the Consistency of Bayes Estimates,'' *Ann. Statistics*, 14, pp. 26-30 (1986).

[4] L. Schwartz, ''On Bayes' Procedures,'' *Z. Wahrsch. verw. Gebiete*, 4, pp. 10-26 (1965).

[5] D. Freedman, ''On the Asymptotic Behavior of Bayes Estimates in the Discrete Case,'' *Ann. Math. Statistics*, 34, pp. 1386-1403 (1963).

[6] H. Strasser, ''Consistency of Maximum Likelihood and Bayes Estimates,'' *Ann. Statistics*, 9, pp. 1107-1113 (1981).

[7] A.R. Barron, ''On Uniformly Powerful Tests and Bayes Consistency,'' in preparation.

3.21 ON FINDING MAXIMALLY SEPARATED SIGNALS FOR DIGITAL COMMUNICATIONS

D.J. Hajela and Michael L. Honig

Bell Communications Research
Morristown, NJ 07960

1. Notation.

The L_p norm of a function $f : [0,\infty) \to \mathbf{R}$ (real numbers) is given by

$$\| f \|_p \equiv \left[\int_0^\infty | f(t) |^p \, dt \right]^{1/p} .$$

Similarly, the L_p norm over an interval $[0,T]$ is defined as

$$\| f \|_{p,T} \equiv \left[\int_0^T | f(t) |^p \, dt \right]^{1/p} .$$

The cases $p = \infty$ and $p = 2$ are of primary interest. The L_∞ norm of a continuous function f over an interval $[0,T]$ is defined as

$$\| f \|_{\infty,T} \equiv \lim_{p \to \infty} \| f(t) \|_{p,T} = \sup_{0 \le t \le T} | f(t) | .$$

If h and f are functions from $[0,\infty)$ into $\mathbf{R}$ such that $\| h \|_{\infty,T}$ and $\| f \|_{\infty,T}$ are finite for all T then $h*f$ is given by

$$(h*f)(t) \equiv \int_0^t h(s) \, f(t-s) ds .$$

2. Problem Statements.

(P1) Given a function $h(t)$ (assume $\| h \|_\infty < \infty$), some time interval $[0,T]$, and some small constant $d > 0$, find input functions

$u_1(t), \ldots, u_N(t)$, where $\| u_i \|_{p'} \leq 1$, $i = 1, \ldots, N$, such that $\min_{i \neq j} \| h^*u_j - h^*u_i \|_{p,T} \geq d$, with N as large as possible. In general, $p' \neq p$, however, we will assume that either $p' = p = \infty$ or $p' = p = 2$. Let $N_{\max}(T)$ denote the largest possible N. A related question is how fast does $N_{\max}(T)$ increase with T; that is, what is $\lim_{T \to \infty} \left[\log N_{\max}(T)/T \right]$?

The following two problems are alternate versions of (P1). In all cases the inputs must satisfy $\| u_i \|_{p'} \leq 1$.

(P2) Given the number of inputs N and a small constant d, find inputs $u_1(t), \ldots, u_N(t)$ which minimize the time T such that $\min_{i \neq j} \| h^*u_j - h^*u_i \|_{p,T} \geq d$. Let $T_{\min}(N)$ denote the minimum time.

(P3) Given the interval $[0,T]$ and the number of inputs N, find inputs $u_1(t), \ldots, u_N(t)$ which maximize $d = \min_{i \neq j} \| h^*u_j - h^*u_i \|_{p,T}$.

It is apparent that

$$T_{\min}(N) = \inf \left\{ T \mid N_{\max}(T) \geq N \right\}$$

and

$$N_{\max}(T) = \max \left\{ N \mid T_{\min}(N) \leq T \right\} .$$

3. Motivation.

Consider an information source that must transmit one of N messages through a channel characterized by the transfer function $H(s)$ (impulse response $h(t)$). The receiver can sample the channel output an arbitrary, but finite, number of times and can compare the samples with a set of threshholds to decide which of the N possible messages were transmitted. The analog to digital converter at the receiver can measure the channel output only to within a given finite precision, that is, to within

$\pm\, d$. In addition, a maximum amplitude constraint is imposed on the inputs to the channel. It is assumed that any random disturbance, which the channel may introduce, is masked by the finite precision with which the receiver measures the channel output. A solution to (P1)-(P3) for the case $p = p' = \infty$ would reveal the maximum number of messages that can be reliably transmitted in a given time interval $[0,T]$.

The case $p = 2$ is relevant if the channel is modeled as a linear transfer function followed by a white Gaussian noise source, and it is assumed that the receiver computes a maximum likelihood estimate of the input message given the received signal over the time interval $[0,T]$. In this case the inputs $u_1(t), \ldots, u_N(t)$ should be selected to maximize the minimum distance defined as

$$d_{\min} = \min_{i \neq j} \| g * u_i - g * u_j \|_{2,T} , \tag{1}$$

where g is the impulse response of the combined channel and receive filter. An average power constraint on the inputs corresponds to the case $p' = 2$. The only reference of which the authors are aware that states problem (P1) precisely for the case $p = p' = 2$ is a paper by Root [1] in which upper and lower bounds are given for the parameter $\log N_{\max}(T)$, which is referred to as "ε capacity." Of course, variations of (P1)-(P3) can be considered. For example, it may be desirable to impose both a maximum amplitude (L_∞) and average power (L_2) constraint on the inputs and insist that the L_2 (or L_∞) distance between outputs be maximized.

4. Some Results.

Some results pertaining to (P1)-(P3) for the case $p = p' = \infty$ are given by the following two theorems [2].

Theorem 1: There exists a solution to (P2) such that $| u_i(t) | = 1$ for $i = 1, \ldots, N$ and $0 \le t \le T$, and each $u_i(t)$ changes sign a finite number of times.

If, in particular, $h(t) = \sum_{i=0}^{n} A_i e^{-\alpha_i t}$, where A_i and $\alpha_i > 0$ are constants, then there exists a solution to (P2) such that each $u_i(t)$ switches between 1 and -1 at most $(N-1)(n-1)$ times.

Theorem 2: Suppose that $h(t) = Ae^{-\alpha t}$, where A and $\alpha > 0$ are constants, and that the message to be transmitted contains K bits, that is, $N = 2^K$. There exists a solution to (P2) such that

$$u_j(t) = b_{jk}, \qquad (k-1)\Delta \le t < k\Delta, \ 1 \le k \le K,$$

where b_{jk} is either 1 or -1, corresponding to the kth bit of the jth message, and

$$\Delta = -\frac{1}{\alpha} \ln \left[1 - \frac{d}{2A} \right].$$

The solution to (P1)-(P3) for the case $h(t) = Ae^{-\alpha t}$ therefore consists of standard "bit by bit" signaling in which ± 1 is sent corresponding to each incoming bit for the fixed duration Δ. It is conjectured that these signals are also optimal if the impulse response has the form

$$h(t) = \sum_{i=0}^{n} A_i \, e^{-\alpha_i t},$$

where the A_i and α_i are positive constants.

5. Some Related Problems.

In this section it is shown how problems (P1)-(P3) for the case $p' = p = 2$ are related to some problems which have been addressed in the literature (i.e., see [3]-[6]).

Optimum Pulse Shaping.

Suppose that the message to be transmitted is a sequence of bits and the inputs $u_i(t)$, $i = 1, \ldots, N$, are constrained to be pulse amplitude modulated (PAM) signals; that is,

$$u_i(t) = \sum_k a_{i,k} \, p(t - kt_0), \tag{2}$$

where $p(t)$ is the pulse shape and the $a_{i,k}$'s can assume one of 2^L

values, L being the number of bits transmitted per symbol interval t_0. It is easily shown that for this case the minimum distance, given by (1), can be written

$$d_{\min}^2 = \inf_{\varepsilon_k \in S, K} \frac{1}{2\pi} \int_{-\infty}^{\infty} | H(\omega)\, P(\omega) \sum_{k=1}^{K} \varepsilon_k\, e^{-i\omega k t_0} |^2 \, d\omega \,, \tag{3}$$

where the set S contains all possible values of the difference of two symbols $a_{i,k} - a_{i,k}'$, K is any integer greater than zero, $\varepsilon_1 \neq 0$, and $H(\omega)$ and $P(\omega)$ are the respective Fourier transforms of $h(t)$ and $p(t)$; that is,

$$H(\omega) = \int_{-\infty}^{\infty} h(t) e^{-i\omega t}\, dt \,.$$

Here we assume that the message length (N) is arbitrarily large and that the average transmitted power is constant; that is, $\| p(t) \|_2 = \| P(\omega) \|_2 = 1$. According to the previous constraints, (P3) can be restated as:

(P4) For a given t_0 and set S, find $P(\omega)$ that maximizes $d_{\min}$.

A discrete version of this problem in which the impulse response $p(t)$ becomes a vector is considered in [3]-[5]. In [3] it is shown that this problem is a linear programming (LP) problem; however, the number of constraints is typically too large for an LP algorithm to be useful by itself. A solution to (P4) for a discrete impulse response of length 26 is obtained in [5] by combining an LP algorithm with a tree search algorithm.

Optimum Signaling Rate.

Suppose now that the input signals $u_i(t)$ are constrained to be of the form (2), where the pulse shape, determined by the product $P(\omega)\, H(\omega)$, is specified and the set of transmitted levels is $A = \{ \pm \alpha, \pm 3\alpha, \ldots, \pm M\alpha \}$, where $M = 2^L - 1$ and α is chosen to satisfy an average power constraint. In this case, $d_{\min}$ given by (3) will be a function of the signaling rate $1/t_0$ and the number of levels 2^L. The information rate is $R \equiv L/t_0$ bits/sec and the average power is

$E \equiv \alpha^2(4^L - 1)/(3t_0)$ where $\alpha^2(4^L - 1)/3$ is the average energy per pulse assuming that the transmitted symbols are uniformly distributed. Under these constraints (P3) is roughly equivalent to:

(P5) Given a rate R and $P(\omega)\,H(\omega)$, find the number of levels M that maximize $d_{\min}$ subject to $E = 1$.

Suppose that

$$H(\omega)\,P(\omega) = \begin{cases} 1 & |\,\omega\,| \le W \\ 0 & |\,\omega\,| > W \end{cases} \tag{4}$$

and the set of levels $A = \{1, -1\}$ in which case from (3) $d_{\min}$ can be written

$$\frac{d_{\min}^2(\delta)}{4} = \inf_{\varepsilon_k \in \{0, \pm 1\},\, K} \frac{1}{2\delta} \int_{-\delta}^{\delta} \left|\, 1 + \sum_{k=1}^{K} \varepsilon_k\, e^{-i2\pi\theta k} \right|^2 d\theta\,, \tag{5}$$

where $\delta = t_0 W$ and $0 < \delta \le 1/2$. If the rate $1/t_0 = 2W$, then $\delta = 1/2$ and $d_{\min}^2/4 = 1$. Also, $d_{\min}^2(\delta)/4 \le 1$ for $\delta < 1/2$ (obtained by setting $\varepsilon_k = 0,\ k > 0$). The rate $2W$ is called the *Nyquist rate*. The behavior of $d_{\min}$ when the symbol rate $1/t_0$ is greater than the Nyquist rate ($\delta < 1/2$) is studied in [5] and [6].

The following question is posed in [5]. Suppose we wish to compare multilevel signaling at the Nyquist rate, that is, $L = L_1 > 1$, and $1/t_0 = 2W$, with binary signaling at faster than the Nyquist rate, that is, $L = 1$, $A = \{1, -1\}$, and $T_{BIN} \equiv t_0$, where $t_0 \le 1/(2W)$. The information rate and average transmitted power for both schemes are assumed to be the same,

$$R \equiv 2WL_1 = \frac{1}{T_{BIN}} = \frac{W}{\delta} \tag{6a}$$

and

$$2W\alpha^2\,\frac{4^{L_1} - 1}{3} = \frac{1}{T_{BIN}}\,. \tag{6b}$$

Given R, for which scheme is $d_{\min}$ greater? The *gain* G of faster binary signaling (FBS) relative to multilevel Nyquist signaling (MNS) is defined as the ratio of $d_{\min}^2$ for FBS to $d_{\min}^2$ for MNS. For MNS, $d_{\min} = 2\alpha$. Using (6), the gain can be written [5]

$$G \equiv \left[\frac{d_{\min}^2(\delta)}{4} \right] \frac{2}{3} \, \delta(4^{1/(2\delta)} - 1) \, ,$$

where $d_{\min}(\delta)$ is given by (5). It is shown in [7] that $d_{\min}(\delta)/4$ is lower bounded by a computable expression, which is greater than zero, and goes to one as δ goes to one. This bound improves upon the previous lower bound in [6], which states only that $d_{\min}(\delta)$ is strictly greater than zero for $\delta > 0$. It is also shown in [7] that there exists a $\delta_0 < 1/2$ such that $\delta > \delta_0$ implies that $d_{\min}(\delta)/4 = 1$ (which implies that $G > 1$). This suggests the following problem.

(P6) Find δ which maximizes G.

REFERENCES

[1] W.L. Root, ''Estimates of ε Capacity for Certain Linear Communication Channels,'' *IEEE Trans. Inf. Theory,* IT-14, No. 3, pp. 361-369 (May 1968).

[2] M.L. Honig, S. Boyd, and B. Gopinath, ''On Optimum Signal Sets for Digital Communications With Finite Precision and Amplitude Constraints,'' in preparation.

[3] R.R. Anderson and G.J. Foschini, ''The Minimum Distance for MLSE Digital Data Systems of Limited Complexity,'' *IEEE Trans. Inf. Theory,* IT-21, No. 5, pp. 544-551 (Sept. 1975).

[4] S.A. Fredriccson, ''Optimum Transmitting Filter in Digital PAM Systems with a Viterbi Detector,'' *IEEE Trans. Inf. Theory,* IT-20, pp. 479-489 (July 1974).

[5] G.J. Foschini, ''Contrasting the Performance of Faster Binary Signalling with QAM,'' *Bell Syst. Tech. J.*, 63, No. 8, pp. 1419-1445 (Oct. 1984).

[6] J.E. Mazo, ''Faster Than Nyquist Signalling,'' *Bell Syst. Tech. J.*, 54, No. 8, pp. 1451-1462 (Oct. 1976).

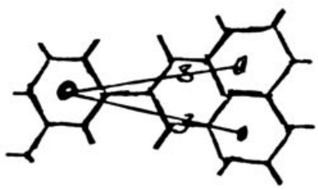
[7] D.J. Hajela, ''On Faster Than Nyquist Signalling, Parts I-III,'' in preparation.

3.22 FREQUENCY ASSIGNMENT IN CELLULAR RADIO

Edward C. Posner

Department of Electrical Engineering
and Jet Propulsion Laboratory
Caltech
Pasadena, CA 91125

Cellular radio uses a number of channels or frequencies (e.g., $7 \times 44 = 308$) divided into local cells (hexagons here) such that the same frequency can be reused in cells at graph distance 3 or greater:



Here the whole plane is tiled. If we allow "call rearrangement," we can think of assigning channels after we see the list of all call requests. Any number ≥ 0 of calls can be requested from any cell. The calls are being made to stationary, not to mobile, phones so one call corresponds to one channel. Suppose we have a bound on demand of the form "total number of calls requested in *every* 1-sphere is at most M."

Let there be f frequencies, a constraint of the problem. What is $M(f)$, the largest demand bound M that still allows all calls to be serviced by the f channels, so that no channel is used in two cells closer than graph distance 3? (f divisible by 7 is probably of most interest.)

Partial Results: Pierre Baldi (now at UCSD) in his 1986 Caltech thesis showed

$$\lfloor \frac{f}{2} \rfloor \le M(f) \le \lceil \frac{2f}{3} \rceil .$$

Problem: Improve this. In particular, find $M(7)$ and $M(14)$.

Note: $7 \le M(14) \le 10$ by Baldi's result.
Note: $M(7) = 3$ or 4. For $M(7) \ge 3$ by above, Maria Klawe of IBM Almaden, San Jose, found a configuration at SPOC'86 showing $M(7) \le 4$. Also at SPOC'86, George Soules of IDA-Princeton, using linear programming and Klawe's configuration, showed

$$M(f) \le \lceil \frac{2f}{3} \rceil - 1 \quad \text{for} \quad f \equiv 1(3) .$$

CHAPTER IV.

PROBLEMS IN COMPUTATION

Computational and algorithmic complexity are wide open areas. What is the quickest computation and what is the shortest program for a computation? Computational and algorithmic complexity clearly trade off. Nonetheless, these two fields don't seem to feed on each other. The contributions in this section fall in both areas.

The chapter on communication and this chapter on computation should have a very close relationship in the future. Clearly, communication is computation limited and computation is communication limited. At the bottom, both computation and communication must call on physical processes to achieve their goals. When we get down to using tweezers on atoms, who is to say whether we will think as communication theorists, computer scientists, physicists, or mathematicians?

Contents

4.1 IN SEARCH OF A ONE-WAY FUNCTION

Jacob Ziv

Technion
Haifa, Israel

Consider straight-line (SL) algorithms over a finite field with q elements.

The ε-SL complexity $C_\varepsilon(\phi)$ of a function ϕ is defined as the length of the shortest SL algorithm which computes a function f, such that $f(x) = (x)$ is satisfied for at least $(1 - \varepsilon)q$ elements of F. The function f is called an " ε-approximation of ϕ."

A function ϕ is SL-"one way" of range δ, $0 \leq \delta \leq 1$, if ϕ satisfies the following three properties:

1. There exists an infinite set S of finite fields such the ϕ is defined in every $F \in S$ and ε is one-to-one (i.e., ϕ^{-1} exists) in every $F \in S$.
2. For every ε such that $0 \leq \varepsilon \leq \delta$, $C_\varepsilon(\phi^{-1})$ tends to infinity as the cardinality q of F approaches infinity.
3. For every ε such that $0 \leq \varepsilon \leq \delta$,

$$\eta = \liminf_{q \to \infty} \eta \triangleq \liminf_{q \to \infty} \frac{\log C\, \varepsilon(\phi^{-1}) - \log C\, \varepsilon(\phi)}{\log C\, \varepsilon(\phi)} > 1 ;$$

   η is called the work-factor.

Example: $\phi(x) = x^3$ is one-way in the range $\delta \geq 1/3 - 1/q$, where q is the cardinality of the field.

$$C_\varepsilon(\phi) = 2$$

$$C_\varepsilon(\phi) = o(\log q)$$

Hence,

$$\eta = o(\log q)$$

It has been shown [1] that a lower bound of n^3 on the complexity of a function f over $GF(2^n)$ is also a lower bound on the product of run-time and program size Turing machines.

Open Problem: Is there a one-way function with work factor $\eta > (\log q)^3$ (thus making it a one-way function in terms of Turing complexity)?

REFERENCE

[1] A. Lempel, G. Serussi, and J. Ziv, ''On the Power of Straight-Line Computations in Finite Fields,'' *IEEE Trans. Inf. Theory,* IT-28, No. 6, pp. 875-879 (Nov. 1982).

4.2 AVERAGE CASE COMPLETE PROBLEMS[†]

Leonid A. Levin

CS/CLA
Boston University
and MIT
Boston, MA 02215

Many interesting combinatorial problems were found to be *NP*-complete. Since there is little hope to solve them fast in the worst case, researchers look for algorithms which are fast just "on average." This matter is sensitive to the choice of a particular *NP*-complete problem and a probability distribution of its instances. Some of these tasks are easy and some not. But one needs a way to distinguish the "difficult on average" problems. Such negative results could not only save "positive" efforts but may also be used in areas (like cryptography) where hardness of some problems is a frequent assumption. It is shown in [1] that the Tiling problem with uniform distribution of instances has no polynominal "on average" algorithm, unless every *NP*-problem with every simple probability distribution has it.

It is interesting to try to prove similar statements for other *NP*-problems which have resisted "average case" attacks.

REFERENCE

[1] L. Levin, "Average Case Complete Problems," *SIAM J. Comput.*, No. 1, pp. 285-286 (1986).

---

† Supported by NSF Grants # MCS-8104211,8304498.

4.3 DOES A SINGLE BIT ACCUMULATE THE HARDNESS OF THE INVERTING PROBLEM?

Leonid A. Levin

Computer Science Department
Boston University
Boston, MA 02215

It is demonstrated by Yao [1] what a crucial role information theory can play in the theory of computation. These matters deserve more consideration.

Let $|x|$ be the length of $x \in S = \{0, 1\}^*$ and $x \circ y$ be the concatenation of x, y. Let $(x \cdot y)$ be the inner product of $x, y \in \mathbf{Z}_2^n$ and $f(x)$ be an easily computable function over S preserving $|x|$. Assume that on a constant fraction of instances of each length any fast algorithm fails to invert $f(x)$. Prove then that even a single bit $B(x, y) = (x \cdot y)$ will be computed incorrectly, on a constant fraction of instances, by any fast algorithm $A(x, f(y))$. This would be true for $B'(i, y)$, equal to the ith bit of the Justesen code of y. Another conjecture is that the correlation between $B(x, y)$ (or its modification) and $A(x, f(y))$ divided by A's running time is at most a constant power of the average of the reciprocal running time needed to invert f on strings of a given length.

REFERENCE

[1] A.C. Yao, "Theory and Applications of Trapdoor Functions," in Proceedings of the 23rd IEEE Symposium on Foundations of Computer Science, 1982, pp. 80-91.

4.4 COMPUTING THE BUSY BEAVER FUNCTION

Gregory J. Chaitin

IBM Research Division
Yorktown Heights, NY 10598

Efforts to calculate values of the noncomputable Busy Beaver function are discussed in the light of algorithmic information theory.

I would like to talk about some impossible problems that arise when one combines information theory with recursive function or computability theory. That is, I would like to look at some unsolvable problems which arise when one examines computation unlimited by any practical bound on running time, from the point of view of information theory. The result is what I like to call "algorithmic information theory" [1].

In the Computer Recreations department of *Scientific American* [2], A.K. Dewdney discusses efforts to calculate the Busy Beaver function Σ . This is a very interesting endeavor for a number of reasons.

First of all, the Busy Beaver function is of interest to information theorists, because it measures the capability of computer programs as a function of their size, that is, as a function of the amount of information which they contain. $\Sigma(n)$ is defined to be the largest number that can be computed by an n-state Turing machine; to information theorists it is clear that the correct measure is bits, not states. Thus it is more correct to define $\Sigma(n)$ as the largest natural number whose program-size complexity or algorithmic information content is less than or equal to n. Of course, the use of states has made it easier and a definite and fun problem to calculate values of Σ (number of states); to deal with Σ (number of bits) one would need a model of a binary computer as simple and compelling as the Turing machine model, and no obvious natural choice is at hand.

Perhaps the most fascinating aspect of Dewdney's discussion is that it describes successful attempts to calculate the initial values $\Sigma(1), \Sigma(2), \Sigma(3), \ldots$ of an uncomputable function Σ. Not only is Σ

uncomputable, but it grows faster than any computable function can. In fact, it is not difficult to see that $\Sigma(n)$ is greater than the computable function $f(n)$ as soon as n is greater than (the program-size complexity or algorithmic information content of f) + $O(1)$. Indeed, to compute $f(n) + 1$, it is sufficient to know (a minimum-size program for f) and the value of the integer (n – the program-size complexity of f). Thus the program-size complexity of $f(n) + 1$ is $\leq$ (the program-size complexity of f) + $O(\log \mid n -$ the program-size complexity of $f \mid)$, which is $< n$ if n is greater than $O(1)$ + the program-size complexity of f. Hence, $f(n) + 1$ is included in $\Sigma(n)$, that is, $\Sigma(n) \geq f(n) + 1$, if n is greater than $O(1)$ + the program-size complexity of f.

Yet another reason for interest in the Busy Beaver function is that, when properly defined in terms of bits, it immediately provides an information-theoretic proof of an extremely fundamental fact of recursive function theory, namely, Turing's theorem that the halting problem is unsolvable [3]. Turing's original proof involves the notion of a computable real number and the observation that it cannot be decided whether or not the nth computer program ever outputs an nth digit, because otherwise one could carry out Cantor's diagonal construction and calculate a paradoxical real number whose nth digit is chosen to differ from the nth digit output by the nth program, and which therefore cannot actually be a computable real number after all. To use the noncomputability of Σ to demonstrate the unsolvability of the halting problem, it suffices to note that, in principle, if one were very patient, one could calculate $\Sigma(n)$ by checking each program of size less than or equal to n to determine whether or not it halts, and then running each program that halts to determine what its output is, and then taking the largest output. Contrariwise, if Σ were computable, it would then provide a solution to the halting problem, for an n-bit program either halts in time less than $\Sigma(n + O(1))$, or else it never halts.

The Busy Beaver function is also of considerable metamathematical interest; in principle, it would be extremely useful to know larger values of $\Sigma(n)$. For example, this would enable one to settle the Goldbach conjecture and the Riemann hypothesis, and in fact any conjecture such as

Fermat's which can be refuted by a numerical counterexample. Let P be a computable predicate of a natural number, so that for any specific natural number n it is possible to compute in a mechanical fashion whether or not $P(n)$, P of n, is true or false, that is, to determine whether or not the natural number n has property P. How could one use the Busy Beaver function to decide if the conjecture that P is true for all natural numbers is correct? An experimental approach is to use a fast computer to check whether or not P is true, say for the first billion natural numbers. To convert this empirical approach into a proof, it would suffice to have a bound on how far it is necessary to test P before settling the conjecture in the affirmative if no counterexample has been found, and of course rejecting it if one was discovered. Σ provides this bound, for if P has program-size complexity or algorithmic information content k, then it suffices to examine the first $\Sigma\ (k + O(1))$ natural numbers to decide whether or not P is always true. Note that the program-size complexity or algorithmic information content of a famous conjecture P is usually quite small; it is hard to get excited about a conjecture that takes a hundred pages to state.

For all these reasons, it is really quite fascinating to contemplate the successful efforts which have been made to calculate some of the initial values of $\Sigma(n)$. In a sense these efforts simultaneously penetrate to "mathematical bedrock" and are "storming the heavens," to use images of E. T. Bell. They amount to a systematic effort to settle all finitely refutable mathematical conjectures, that is, to determine all constructive mathematical truth. And these efforts fly in the face of fundamental information-theoretic limitations on the axiomatic method [3-5], which amount to an information-theoretic version of Gödel's famous incompleteness theorem [6].

Here is the Busy Beaver version of Gödel's incompleteness theorem: n bits of axioms and rules of inference cannot enable one to prove what is the value of $\Sigma(k)$ for any k greater than $n + O(1)$. The proof of this fact is along the lines of the Berry paradox. Contrariwise, there is an n-bit axiom which does enable one to demonstrate what is the value of $\Sigma(k)$ for any k less than $n - O(1)$. To get such an axiom, one either asks God for the number of programs less than n bits in size which halt, or one asks God for a specific n-bit program which halts and has the maximum possible running time or the maximum possible output before halting. Equivalently, the divine revelation is a conjecture $\forall k\, P(k)$ (with P of program-size complexity or algorithmic information content $\leq n$) which is false and for which (the smallest counterexample i with $\neg P(i)$) is as large as possible. Such an axiom would pack quite a wallop, but only in principle, because it would take about $\Sigma(n)$ steps to deduce from it whether or not a specific program halts and whether or not a specific mathematical conjecture is true for all natural numbers.

These considerations involving the Busy Beaver function are closely related to another fascinating noncomputable object, the halting probability of a universal Turing machine on random input, which I like to call Ω , and which is the subject of an essay by my colleague Charles Bennett that was published in the Mathematical Games department of *Scientific American* some years ago [7].

REFERENCES

[1] G.J. Chaitin, "Algorithmic Information Theory," in *Encyclopedia of Statistical Sciences*, Vol. 1, Wiley, New York, 1982, pp. 38-41.

[2] A.K. Dewdney, "A Computer Trap for the Busy Beaver, the Hardest-Working Turing Machine," Computer Recreations Dept., *Sci. Am.*, 251, No. 2, pp. 19-23 (Aug. 1984).

[3] M. Davis, "What Is a Computation?" in *Mathematics Today: Twelve Informal Essays*, L. A. Steen (ed.), Springer-Verlag, New York, 1978, pp. 241-267.

[4] G.J. Chaitin, "Randomness and Mathematical Proof," *Sci. Am.*, 232, No. 5, pp. 47-52 (May 1975).

[5] G.J. Chaitin, "Gödel's Theorem and Information," *Int. J. Theor. Phys.*, 22, pp. 941-954 (1982).

[6] D.R. Hofstadter, *Gödel, Escher, Bach: An Eternal Golden Braid*, Basic Books, New York, 1979.

[7] M. Gardner, "The Random Number Ω Bids Fair to Hold the Mysteries of the Universe," Mathematical Games Dept., *Sci. Am.*, 241, No. 5, pp. 20-34 (Nov. 1979).

4.5 THE COMPLEXITY OF COMPUTING DISCRETE LOGARITHMS AND FACTORING INTEGERS

A. M. Odlyzko

AT&T Bell Laboratories
Murray Hill, NJ 07974

Practically all knapsack public key cryptosystems have been broken in the last few years, and so essentially the only public key cryptosystems that still have some credibility and are widely known are those whose security depends on the difficulty of factoring integers (the RSA scheme and its variants) and those whose security depends on the difficulty of computing discrete logarithms in finite fields. Therefore, the computational complexity of these two problems is of great interest.

At the time of the workshop, one aspect of the then-current state of knowledge on these two fundamental problems seemed to be highly unsatisfactory. This was the fact that all the fast algorithms for discrete logarithms and all but one of the fast algorithms for factoring integers had running-time estimates that depended on the efficiency with which matrices could be inverted. These algorithms require the solution of a system of linear equations of the form

$$Ax = y \,, \tag{1}$$

where A is a matrix of size $m \times n$, x and y are column vectors of lengths m and n, respectively, and m is close to n. The interesting ranges of values for n are between 10^3 and 10^7. Ordinary Gaussian elimination requires about n^3 steps for the solution of (1). Strassen's algorithm, which might be practical for large n, takes about $n^{\log_2 7} = n^{2.807\ldots}$ steps. The best general-purpose algorithm that is known, due to Coppersmith and Winograd [1], takes about $n^{2.495\ldots}$ steps, but is almost certainly impractical. No algorithm can solve the system (1) in fewer than about n^2 steps (there are that many entries in the matrix, after all!).

Depending on how fast the system (1) can be solved, various algorithms have different asymptotic running-time estimates. If we let $L = L(p)$ denote any quantity that satisfies

$$L = \exp\{ [1 + o(1)] [(\log_e p)(\log_e \log_e p)]^{1/2} \} \text{ as } p \to \infty , \quad (2)$$

and suppose that the system (1) can be solved in time about n^r for various values of r, then Table 1 summarizes the state of knowledge at the time of the workshop about the efficiency of the best factoring algorithms for factoring integers around p in size. A similar table can be prepared for the running times of various discrete logarithm algorithms.

The question that was raised at the workshop was whether the estimates for the running times of these algorithms that are obtained by assuming $r > 2$ are really appropriate. Even if we cannot solve general systems of the form (1) in time $O(n^{2+\varepsilon})$ for every $\varepsilon > 0$, we can take advantage of the fact that the systems that arise in factorization and discrete logarithm algorithms are very sparse. Some methods to take advantage of that sparseness were presented, and their effectiveness was supported both by results of large-scale simulations and heuristic arguments. (See [2] for a brief description.) The conclusion was drawn that, at least in the foreseeable future, these methods are likely to make the system (1) easy to solve. Still, a question remained about the asymptotic performance.

As a result of that presentation, several methods were developed that can solve sparse systems of the form (1) in not much more than n^2 steps. The first such methods were developed by D. Coppersmith and the author, following a suggestion of N. Karmarkar. These methods consist of adaptations of the conjugate gradient [3] and the Lanczos [4] algorithms to solve linear equations over finite fields. They have been tested successfully on quite large systems. Brief accounts of these adaptions are given in [2] and [5].

Soon afterwards, D. Wiedemann [6] found a more elegant and probably even faster method, based on the use of the Berkelamp-Massey algorithm and the Cayley-Hamilton theorem. A brief account of it can also be found in [2].

Now that the main question, whether systems of the form (1) that arise in factorization and discrete logarithm algorithms can be solved in about time n^2, has been answered in the affirmative, we are faced with a more important and basic question.

Table 1. Asymptotic Running Times for Factoring Integers

Algorithm	$r = 3$	$r = 2.807...$	$r = 2.495...$	$r = 2$
Schnorr-Lenstra [7]	L	L	L	L
Continued fraction [8]	$L^{1.13...}$	$L^{1.12...}$	$L^{1.11...}$	$L^{1.11...}$
Schroeppel linear sieve [8]	$L^{1.22...}$	$L^{1.18...}$	$L^{1.11...}$	L
Pomerance quadratic sieve [8]	$L^{1.06...}$	$L^{1.04...}$	$L^{1.02...}$	L
Coppersmith, Odlyzko, and Schroeppel [5]	$L^{1.16...}$	$L^{1.13...}$	$L^{1.081...}$	L

There are now several algorithms known that can factor an integer around p in time $L(p)$ (see Table 1 and [9], which presents a new algorithm based on elliptic curves), as well as several algorithms that can compute discrete logarithms in fields $GF(p)$ for p a prime in time $L(p)$. (For fields $GF(2^n)$, discrete logarithms can be computed much faster [10], and the new sparse matrix methods are also useful in speeding this algorithm [2].) Does this mean that $L(p)$ is the natural lower bound for the computational complexity of factoring and finding discrete logarithms? It is the author's guess that this is not the case and that we are missing some insight that will let us break below the $L(p)$ barrier.

REFERENCES

[1] D. Coppersmith and S. Winograd, "On the Asymptotic Complexity of Matrix Multiplication," *SIAM J. Comp.,* 11, pp. 472-492 (1982).

[2] A.M. Odlyzko, "Discrete Logarithms in Finite Fields and their Cryptographic Significance," in *Advances in Cryptology: Proceedings of Eurocrypt 84* (T. Beth, N. Cot, and I. Ingemarsson, eds.), LNCS #209, Springer, New York, 1985, pp. 224-314.

[3] M.R. Hestenes and E. Stiefel, "Methods of Conjugate Gradients for Solving Linear Systems," *J. Res. Natl. Bur. Stand.,* 49, pp. 409-436 (1952).

[4] C. Lanczos, "Solution of Systems of Linear Equations by Minimized Iterations," *J. Res. Natl. Bur. Stand.,* 49, pp. 33-53 (1952).

[5] D. Coppersmith, A.M. Odlyzko, and R. Schroeppel, "Discrete Logarithms in $GF(p)$," *Algorithmica,* 1, pp. 1-15 (1986).

[6] D. Wiedemann, "Solving Sparse Linear Equations Over Finite Fields," *IEEE Trans. Inf. Th.,* IT-32, pp. 54-62 (1986).

[7] C.P. Schnorr and H.W. Lenstra, Jr., "A Monte Carlo Factoring Algorithm with Linear Storage," *Math. Comp.,* 43, pp. 289-311 (1984).

[8] C. Pomerance, "Analysis and Comparison of Some Integer Factoring Algorithms," in *Computational Number Theory: Part 1* (H.W. Lenstra, Jr., and R. Tijdeman, eds.), Mathematics Centre Tract 154, Mathematics Centre, Amsterdam, 1982, pp. 89-139.

[9] H.W. Lenstra, Jr., "Factoring Integers with Elliptic Curves," to appear.

[10] D. Coppersmith, "Fast Evaluation of Logarithms in Fields of Characteristic Two," *IEEE Trans. Info. Theory,* IT-30, pp. 587-594 (1984).

4.6 KNAPSACK USED IN FACTORING

Don Coppersmith

IBM Research
Yorktown Heights, NY 10598

Suppose we are given l integers $x_1, x_2, \ldots, x_l$, in the range from $-l^{1.5}$ to $+l^{1.5}$. These integers may be thought of as being random and uniformly distributed in their range.

Consider the event that three of the integers add to zero:

$$x_i + x_j + x_k = 0 . \tag{1}$$

If the x_i's are truly random, we will have about $cl^{1.5}$ ordered triples (i, j, k) of indices satisfying (1), for some constant c.

The problem is to discover these triples as quickly as possible. Specifically, in time $l^{1.5+\varepsilon}$, can you write down $l^{1.5-\varepsilon}$ triples satisfying (1)?

One can do so in time l^2: sort the x_i's then for each fixed x_i run forward through the x_j and backward through the x_k, trying to keep $x_j + x_k$ near $-x_i$, to discover all pairs (j, k) such that (i, j, k) satisfies (1).

Another approach is to use a fast Fourier transform; by setting up a vector of length $2l^{1.5}$, with 1 denoting the position of each x_i, then taking a convolution of this vector with itself, we can compute the *number* of triples involving each index i in time $l^{1.5+\varepsilon}$. However, we do not compute the triples themselves, so this does not solve the problem.

Motivation. The problem was originally motivated by an algorithm for factoring integers near perfect cubes. Suppose we are trying to factor $N = M^3 + O(M)$. We can first find integers y_i near M which are *smooth,* that is, the product of small primes. With an appropriate choice of l, and an appropriate definition of "small" primes, there will be l such y_i with $| y_i - M | < l^{1.5}$. Now set $x_i = y_i - M$. Whenever (1) is satisfied, we will have

$$y_i\, y_j\, y_k - N = (x_i + M)\,(x_j + M)\,(x_k + M) - N$$

$$= (x_i\, x_j\, x_k) + M\,(x_i\, x_j + x_i\, x_k + x_j\, x_k) + M^2\,(x_i + x_j + x_k) + M^3 - N$$

$$= (x_i\, x_j\, x_k) + M\,(x_i\, x_j + x_i\, x_k + x_j\, x_k) + 0 + O(M)$$

$$= O(Ml^3)$$

Thus $y_i\, y_j\, y_k - N$, being relatively small, will itself have a reasonable chance of being "smooth." If it is, we have related some small primes multiplicatively mod N. This gives us one of the l equations needed by the Morrison-Brillhart method of factorization. This technique could be viewed as an attempt to speed up the equation-gathering phase of the Morrison-Brillhart algorithms [1].

This application is supplanted, however, by the Reyneri cubic sieve [2,3]. In that algorithm, the y_i are replaced by the set of *all* integers y_i' in the range $[M - l, M + l\,]$. Then one ends up recovering equations relating the y_i with the small primes. One has to gather more equations then (as many equations as both the small primes and the y_i') but they are somewhat easier to find (the residues $y_i'\, y_j'\, y_k' - N$ turn out to be smaller, $O(Ml^2)$ rather than $O(Ml^3)$, and thus more likely to be smooth), and in addition the knapsack problem disappears.

The knapsack problem remains as an intellectual challenge, however, even after its motivation is removed.

REFERENCES

[1] C. Pomerance, ''Analysis and Comparison of Some Integer Factoring Algorithms,'' in *Computational Methods in Number Theory: Part I* (H.W. Lenstra, Jr., and R. Tijdeman, eds.), Mathematics Centre Tract 154, Mathematics Centre Amsterdam, 1982, pp. 89-139.

[2] J.M. Reyneri, unpublished manuscript.

[3] Don Coppersmith, Andrew M. Odlyzko, and Richard Schroeppel, "Discrete Logarithms in *GF*(p)," Research Report RC 10985, IBM T.J. Watson Research Center, Yorktown Heights, NY, 10598, Feb. 14, 1985; *Algorithmica,* 1, pp. 1-15 (1986).

4.7 RELIABLE COMPUTATION WITH ASYNCHRONOUS CELLULAR ARRAYS

Peter Gacs

Deptartment of Computer Science
Boston University
Boston, MA 02215

1. The homogeneous construction and local connectivity of cellular arrays makes them the natural domain for the formulation of certain general questions concerning reliable computation. We have addressed the problem of reliable computation in discrete time in two works. Gacs [1] constructs a (fairly complex) one-dimensional array while Gacs and Reif [2], based on Toom's work, construct a very simple three-dimensional array. Even if built of unreliable components, these arrays can simulate any one-dimensional cellular array reliably.

2. Continuous-time (asynchronous) models are in many respects more natural to consider than the discrete ones, especially as physical systems. Very simple methods are known to convert a discrete-time system into one that will work correctly even if the state transition of each component happens at arbitrary times, provided whenever it happens its result is predictable.

3. The one-dimensional model of Gacs [1] can probably be extended to also deal with asynchrony. But encouraged by the simplicity of the Gacs-Reif model [2] and the simplicity of the model mentioned in 2 above, we expect a simple solution, at least in three (or four?) dimensions also for the case when both asynchrony and errors are present. The simplest ideas were already discarded experimentally by Charles Bennett using the Cellular Automata Machine simulator.

   However, he is currently investigating a three-dimensional scheme based on the recognition that synchronization faults in three dimensions form rings of vortices.

4. Three-dimensional cellular arrays are not physically realizable. Our newest results, obtained at Bellcore in the summer of 1985, show that a real complexity-tradeoff is possible in a two-dimensional reliable array. In this scheme, "information" errors are corrected by a hierarchical coding and repetition scheme, while "structure" errors are corrected using Toom's rule (instead of the complex procedures used in [1]). The bottom level of the new scheme is fairly simple but it is still a challenging problem to simplify it down to physical plausibility.

REFERENCES

[1] P. Gacs, ''Reliable Computation with Cellular Automata,'' *J. Comput. Syst. Sci.,* to appear. Final version: Boston University Technical Report, 1985.

[2] P. Gacs and J. Reif, ''A Simple Three-Dimensional Real-Time Reliable Cellular Array,'' Proceedings of the ACM Symposium on the Theory of Computing, Spring 1985. Final version: Boston University Technical Report, 1986.

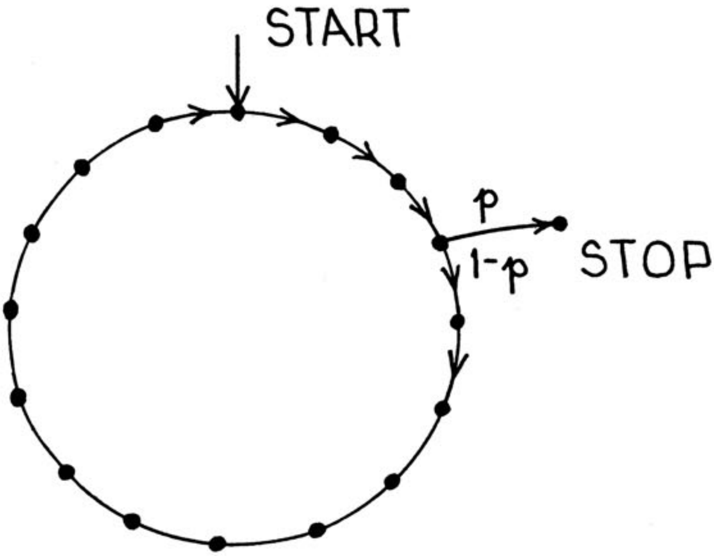
4.8 FINITE MEMORY CLOCKS

Thomas M. Cover

Departments of Electrical Engineering
and Statistics
Stanford University
Stanford, CA 94305

How does one tell time when the number of states in the clock is insufficient to count the elapsed time? For that matter, how good are humans at estimating the passage of time?

Let P_n be the probability that a given m-state Markov chain first enters its clock state at time n. We can design a clock such that $P_n \approx (m-1)/ne$, for $n \gg m$. Can one do better?



4.9 DISTRIBUTED SHORTEST PATH ALGORITHMS

R.G. Gallager

Department of Electrical Engineering
and Computer Science
M.I.T.
Cambridge, MA 02139

Consider a graph $G(V,E)$ with a distinguished node called the root and with some positive weight associated with each direction on each edge. The length of a path in the graph is the sum of the weights in the direction of the path over the edges of the path. The shortest path problem is to find a minimum weight path from each node to the root. In the special case where each edge has unit weight, we call the shortest path problem the minimum hop problem.

A distributed shortest path algorithm is an algorithm for a communication network to solve the shortest path problem for the graph corresponding to the network. Each node of the network has a processor and the facility to send messages over the edges adjacent to the node. Each node is initially unaware of the topology and knows only the weights of the adjacent edges and whether or not it is the root. Each node has a copy of the algorithm, which is a set of rules for reading messages, processing, and sending other messages over the outgoing edges. The communication is asynchronous but error free and messages travel in first come first serve order over any given edge in any given direction. A message consists of a small (i.e., bounded) number of parameters such as path weights or node identities.

The communication complexity of a distributed shortest path algorithm, as a function of $|N|$ and $|E|$, is the worst case total number of messages, over all edges, required to solve the shortest path problem. We view the problem as solved when each node knows the first edge on a shortest path from itself to the root. The worst case is taken over all graphs and weights of given $|N|$ and $|E|$ and over all delays for individual messages. The time complexity is the worst case time to solve the problem under the assumption that processing time is negligible and each communication takes at most one unit of time (but this time unit is unknown to the algorithm).

The problem is to find distributed algorithms that minimize communication complexity or time complexity or some tradeoff between the two. As an important special case, find such algorithms for the minimum hop problem. It is easy to see that the communication complexity must be at least $|E|$ and the time complexity must be at least $|N|$. It is also easy to see that simply flooding all the topology information through the network solves the problem with communication complexity $|E|^2$. Some progress has been made on the problem for the minimum hop case. Frederickson [1] has developed an algorithm with a communication complexity and time complexity of $O(|N| \sqrt{|E|})$. Also, Awerbuch and Gallager [2,3] have developed algorithms, one of which has a communication complexity of $O(|N|^{1.6} + |E|)$ and time complexity $O(|N|^{1.6})$ and the other of which has a communicaiton complexity of $O(|E|^{1+\varepsilon})$ and a time complexity of $O(|N|^{1+\varepsilon})$, where ε approaches 0 as $\sqrt{2 \log_2 \log_2 |N| / \log_2 |N|}$.

REFERENCES

[1] G. Frederickson, "A Single Source Shortest Path Algorithm for a Planar Distributed Network," in Proceedings of the 2nd Symposium on Theoretical Aspects of Computer Science, Jan. 1985.

[2] B. Awerbuch and R.G. Gallager, "Communication Complexity of Distributed Shortest Path Algorithms," MIT Technical Report LIDS-P-1473, June 1985.

[3] B. Awerbuch and R.G. Gallager, "Distributed BFS Algorithms," in IEEE Symposium on the Foundations of Computer Science, Oct. 1985.

4.10 THE SCOPE PROBLEM

H.S. Witsenhausen

AT&T Bell Laboratories
Murray Hill, NJ 07974

1. Definitions.

By a *system* we will mean a finite sequence $S_1, \ldots, S_m$ of finite sets of positive integers. Denote by (a, i) the occurrence of integer a in set S_i. The *scope* of (a, i) is the union of the sets S_α with $j \le \alpha \le k$, where $1 \le j \le i \le k \le m$ and j is as low and k is as high as possible subject to the condition that for all β satisfying $j < \beta < k$, one has $a \in S_\beta$. This means that the scope consists of the sets in the run of a's to which (a, i) belongs, extended at each end of the run by one additional set, unless that end of the run is one end of the system.

A system is valid if it satisfies the *scope condition:* for any occurrence (a, i) of any integer a, the scope of (a, i) contains $\{1, 2, \ldots, a\}$. Let $\psi(k)$ be the largest integer that can occur in a valid system with sets of maximum cardinality k, and let $\psi_1(k)$ be the largest integer that can occur in set S_1, or equivalently S_m, under the same assumption.

2. Conjectures.

From the constructions for the equivalent "saturation problem" in [1], it follows that $\psi(k) \ge 4k - 1$ and that $\psi_1(k) \ge 4k - 2$. This motivates the following conjectures:

Conjecture 1: $\psi(k) = 4k - 1$.
Conjecture 2: $\psi_1(k) = 4k - 2$.

Conjecture 1 implies Conjecture 2 because the system that gives $\psi_1(k) > 4k - 2$ and its mirror image can be put together, with an obvious adjustment, to yield a valid system contradicting Conjecture 1.

Some Examples. Systems that achieve $\psi(k) = 4k - 1$ are the following.

For $k = 2$:
$\{1\},\{2,3\},\{4,5\},\{1,7\},\{3,7\},\{2,7\},\{1,6\},\{2,6\},\{3,6\},\{1,6\},\{4,5\},\{2,3\},\{1\}$.

For $k = 3$:
$\{1\},\{2,3,4\},\{5,6,7\},\{1,8,9\},\{2,8,9\},\{3,8,9\},\{1,4,10\},\{2,3,10\},\{4,5,10\},$
$\{1,6,10\},\{2,6,10\},\{3,7,11\},\{1,7,11\},\{4,5,11\},\{2,3,11\},\{1,4,11\},$
$\{3,8,9\},\{2,8,9\},\{1,8,9\},\{5,6,7\},\{2,3,4\},\{1\}$.

In general, valid systems achieving the conjectured values can be constructed recursively. What remains to be settled is whether this can be improved upon or not.

REFERENCES

[1] H.S. Witsenhausen, "On Woodall's Interval Problem," *J. Combinatorial Theory, Ser. A,* 21, pp. 222-229 (1976).

[2] D.R. Woodall, "Problem No. 4," *Combinatorics,* London Mathematics Society Lecture Note Series, No. 13, Cambridge Universitiy Press, Cambridge, 1974, p. 202.

4.11 A CONJECTURED GENERALIZED PERMANENT INEQUALITY AND A MULTIACCESS PROBLEM†

Bruce Hajek

Department of Electrical Engineering
University of Illinois
Urbana, IL 61801

1. The Conjecture.

Let k and n be positive integers, and let I denote the set of k-tuples, $I = \{1, 2, \ldots, n\}^k$. For $1 \leq j \leq k$, let S_j denote the collection of subsets L of I such that L has cardinality n and no two elements of L have the same jth coordinate. Let $S = \bigcup_j S_j$. Finally, let $F_{n,k}$ be the multinomial in variables $\mathbf{x} = (\, \mathbf{x_i} : \mathbf{i} \in I \,)$ defined by

$$F_{n,k}(\mathbf{x}) = \sum_{L \in S} \prod_{\mathbf{i} \in L} \mathbf{x_i} \, .$$

Conjecture 1. Under the constraints

$$\mathbf{x} \geq 0 \quad \text{and} \quad \sum_{\mathbf{i}} x_{\mathbf{i}} = 1 \, , \tag{1}$$

$F_{n,k}$ attains its maximum at $\mathbf{x}$ if and only if $x_{\mathbf{i}} = n^{-k}$ for all $\mathbf{i}$.

2. Permanent Inequality as Special Case.

We consider the case $k = 2$ in this section. Then $\mathbf{x} = (\, x_{ij} : 1 \leq i, j \leq n \,)$ can be viewed as an $n \times n$ matrix. Now

† Editorial note added in proof: The two equivalent conjectures 1 and 1′ have been shown to be false in the recent preprint, J. Körner and K. Marton, "Random Access Communication and Graph Entropy," *IEEE Trans. Inf. Theory,* under review. The problem of finding the optimizing partitions $A_1, A_2, \ldots, A_k$ in Conjecture 1′ remains open, however. It is intimately connected to the perfect hashing problem, also treated in this volume (J. Körner, "The Information Theory of Perfect Hashing," this volume.)

$$F(\mathbf{x}) = \sum_{L \in S_1} \prod_{i \in L} x_i + \sum_{L \in S_2} \prod_{i \in L} x_i - \sum_{L \in S_1 \cap S_2} \prod_{i \in L} x_i .$$

The last sum on the right-hand side is by definition the permanent of the matrix $\mathbf{x}$, and the other sums can be rewritten to yield

$$F(\mathbf{x}) = \prod_i \left(\sum_j x_{ij} \right) + \prod_j \left(\sum_i x_{ij} \right) - \mathrm{perm}(\mathbf{x}).$$

If Conjecture 1 is true, then it is still true under the additional constraint

$$\sum_j x_{ij} = \sum_j x_{ji} = \frac{1}{n} \text{ for all } i . \tag{2}$$

Under (2) we get $F(\mathbf{x}) = (2/n^n) - \mathrm{perm}(\mathbf{x})$. Thus, the conjecture implies the fact that the permanent of $\mathbf{x}$ is minimized subject to the constraints (1) and (2) if and only if $x_{ij} = 1/n^2$ for all i, j. This fact was conjectured in 1926 by B. L. van der Waerden and was proved in 1980 by G. P. Egorychev (see [1]).

3. Application to Random Access Strategies [2].

Let $U^1, \ldots, U^n$ be independent random variables, each uniformly distributed over the unit interval [0, 1]. We say that a partition A of the interval into n disjoint sets (called the atoms of A) *separates* (the points $U^1, \ldots, U^n$) if each one of the atoms contains exactly one of the U^i. We call A an equipartition if each of its n atoms has Lebesgue measure $1/n$.

Now, let $A_1, \ldots, A_k$ each partition the interval [0, 1] into n atoms. Upon setting

$$x_{i_1 i_2 \cdots i_k} = \mathrm{meas}\left(A_1^{i_1} \cap A_2^{i_2} \cap \cdots \cap A_k^{i_k} \right), \tag{3}$$

we see that Conjecture 1 is equivalent to the following conjecture.

Conjecture 1′. Partitions $A_1, \ldots, A_k$ maximize the probability

$$P\,[\text{at least one of the } A_k \text{ separates}]$$

if and only if the partitions are equipartitions and are independent of each other, that is, if and only if the right-hand side of (3) is n^{-k} for each $i_1, \ldots, i_k$.

Could the conjecture be established, a number of corollaries would follow. For example, suppose $A_1, A_2, \ldots$ is an infinite sequence of independent equipartitions and that B is the random partition defined by $B = A_K$, where K is the random variable defined by

$$K = \min \{ k : A_k \text{ separates } U^1, \ldots, U^n \} .$$

Then B is a random partition. Conjecture 1′ and Fuch's inequality [3] can be used to show that B has minimum entropy over all random partitions which separate U .

Acknowledgement: I am grateful to Eli Gafni and Pierre Humblet for discussions on this problem.

REFERENCES

[1] D.E. Knuth, "A Permanent Inequality," *Am. Math. Monthly,* pp. 731-740 (Dec. 1981).

[2] T. Berger, "The Poisson Multiple-Access Conflict Resolution Problem," in *Multi-User Communications (G. Longo, ed.),* CISM Courses and Lecture Series, No. 265, Springer-Verlag, New York, 1981.

[3] L. Fuchs, "A New Proof of an Inequality of Hardy-Littlewood-Polya," *Math. Tidsskrift B,* pp. 53-54 (1947).

4.12 ROTATION DISTANCE

Daniel D. Sleator

Carnegie-Mellon University
Pittsburgh, PA 15213

Robert E. Tarjan

Computer Science Department
Princeton University
Princeton, NJ 08544

William P. Thurston

Mathematics Department
Princeton University
Princeton, NJ 08544

In this note we summarize our recent results on *rotation distance,* a distance measure on binary trees with computer science applications. Our main result is that the maximum rotation distance between any two n-node binary trees is at most $2n-6$ for $n \geq 11$, and this bound is tight for infinitely many n.

Rotation Distance.

A *rotation* is a local transformation on a binary tree that changes the depths of certain nodes but preserves the symmetric order of the nodes (see Figure 1). A rotation takes $O(1)$ time on any standard representation of a binary tree. Rotations are the operations used to rebalance binary search trees [1,2]; thus they play a fundamental role in data structures.

Rotations also impose a mathematical structure on the set of all n-node binary trees. Let R_n, the *rotation graph,* be the undirected graph whose vertices are the n-node binary trees such that two trees are adjacent if and only if one can be obtained from the other by a single rotation. Let $d(T_1, T_2,)$, the *rotation distance* between trees T_1 and T_2, be the distance between T_1 and T_2 in R_n, that is, the minimum number of rotations needed to transform T_1 into T_2 or vice versa. This note summarizes our recent work on rotation distance. Further details and proofs will appear in [3].

We formulate two fundamental questions about rotation distance:

Problem 1. Let d_n be the diameter of R_n, that is, the minimum number of rotations that suffice to transform any n-node binary tree into any other. What is d_n ?

Problem 2. Devise a polynomial-time algorithm that, given any two n-node binary trees T_1 and T_2, computes $d(T_1, T_2)$.

Our results provide an almost-complete solution to Problem 1 and an approximate solution to Problem 2. Concerning Problem 1, we prove:

Theorem 1. $d_n \leq 2n - 6$ for all $n \geq 11$.

Theorem 2. $d_n = 2n - 6$ for infinitely many n .

We conjecture, but cannot yet prove, that $d = 2n - 6$ for all $n \geq 11$. However, we believe that an extension of our methods will establish this. We have computed the exact value of d_n for $n \leq 16$ (see Figure 2). These results show that $d_n = 2n - 6$ for $11 \leq n \leq 16$.

Concerning Problem 2, we exhibit a linear-time algorithm that will estimate $d(T_1, T_2)$ to within a factor of 2. Coming closer than a factor of 2 in general seems hard; however, our methods allow the exact computation of $d(T_1, T_2)$ in various special cases.

There has been very little previous work on rotation distance. To our knowledge the only published work is by Culik and Wood [4], who defined the concept and showed that $d_n \leq 2n - 2$ for all n . Leighton (private communication) showed that $d_n \geq 7n/4 - O(1)$ for infinitely many n .

The original definition of rotation distance is not so easy to study. Thus it is advantageous to transform it into something more amenable. The binary trees are counted by the Catalan numbers [5] as are many other mathematical objects, including the triangulations of a polygon. It is these with which we shall work. The n-vertex binary trees are in one-to-one correspondence with the triangulations of an $(n + 2)$-gon if rotationally equivalent triangulations are regarded as distinct. Furthermore, rotation on binary trees corresponds to the *diagonal flip* operation on triangulations, in which we remove a diagonal (causing two triangles to merge into a quadrilateral) and replace it with the other diagonal of the quadrilateral (see Figure 3). Rotation distance on binary trees corresponds to flip distance on triangulations; the *flip distance* $f(T_1, T_2)$ between two triangulations T_1 and T_2 (or vice versa). In the triangulation setting, Problems 1 and 2 become:

Problem 1′. Determine $f_n = \max \{ f(T_1, T_2) \mid T_1$ and T_2 are triangulations of an n-gon$\}$.

Problem 2′. Devise a polynomial-time algorithm to compute $f(T_1, T_2)$ for any triangulations T_1 and T_2.

We summarize our results on triangulations.

Theorem 1. $f_n \le 2n - 10$ for all $n \ge 13$.

Proof. Any triangulation of an n-gon has $n - 3$ diagonals. Given any vertex x of initial degree $d(x) < n - 3$, we can increase $d(x)$ by a suitable diagonal flip. Thus in $n - 3 - d(x)$ flips, we can produce the triangulation all of whose diagonals have one end at x. It follows that, given any two triangulations T_1 and T_2, we can convert T_1 into T_2 in $2n - 6 - d_1(x) - d_2(x)$ flips, where x is any vertex of degree $d_1(x)$ in T_1 and degree $d_2(x)$ in T_2. A little algebra shows that if $n \ge 13$, there is a vertex x such that $d_1(x) + d_2(x) \ge 4$. The theorem follows. □

Theorem 2′. $f_n = 2n - 10$ for infinitely many n.

The proof of Theorem 2′ is our most interesting and complicated result. It uses a second transformation of the problem, to triangulating a polyhedron (dissecting it into tetrahedra), and relies on volumetric arguments in hyperbolic space.

Lemma 1. If T_1 and T_2 are any two triangulations having a common diagonal e, then any minimum-length sequence of flips from T_1 to T_2 leaves e alone; indeed any flip sequence from T_1 to T_2 that flips e uses at least two more flips than the minimum number.

Lemma 2. If T_1 and T_2 are any two triangulations with no common diagonals but some diagonal e of T_1 can be converted into a diagonal e' of T_2 in one flip, then there is a shortest flip sequence from T_1 to T_2 that first flips e to e'.

A further result along the lines of Lemmas 1 and 2 concerning diagonals fixable in two flips can be proved. However, such results seem to be of no help in solving Problem 2′, because there are pairs of triangulations T_1 and T_2 such that fixing even a single diagonal requires $\Omega(n)$ flips. On the other hand, Lemma 1 allows us to estimate $f(T_1, T_2)$ to within a constant factor:

Theorem 3. Let $g(T_1, T_2)$ be the number of diagonals in T_1 that are not in T_2. Then $g(T_1, T_2) \le f(T_1, T_2)$

We close by mentioning another problem, having to do with rotations, that arises in the study of self-adjusting search trees [6,7]. A *turn* is a pair of rotations as illustrated in Figure 4.

Problem 3. Starting from an arbitrary n-node binary tree T, what is the maximum number of right turns that can be made before no more are possible?

We conjecture that the maximum number of right turns is $O(n)$, but can only prove $O(n \log n)$. Note that, starting from an arbitrary tree, the maximum number of right rotations that can be made is exactly $\binom{n}{2}$.

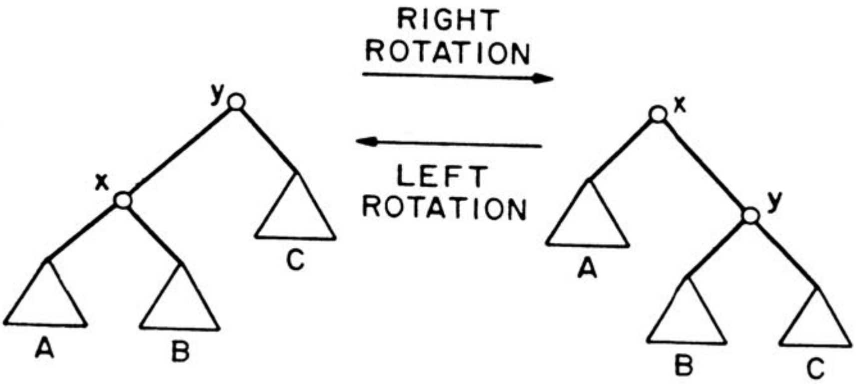


Figure 1. A rotation in a binary tree. Triangles denote subtrees. The tree shown could be part of a larger tree.

n	d_n
1	0
2	1
3	2
4	4
5	5
6	7
7	9
8	11
9	12
10	15
11	16
12	18
13	20
14	22
15	24
16	26

Figure 2. Values of d_n for small n .

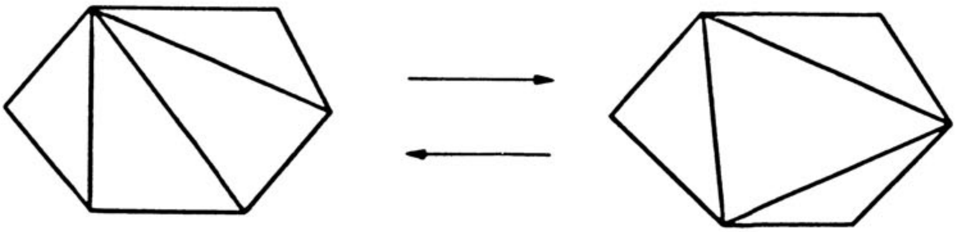


Figure 3. A diagonal flip in a triangulation.

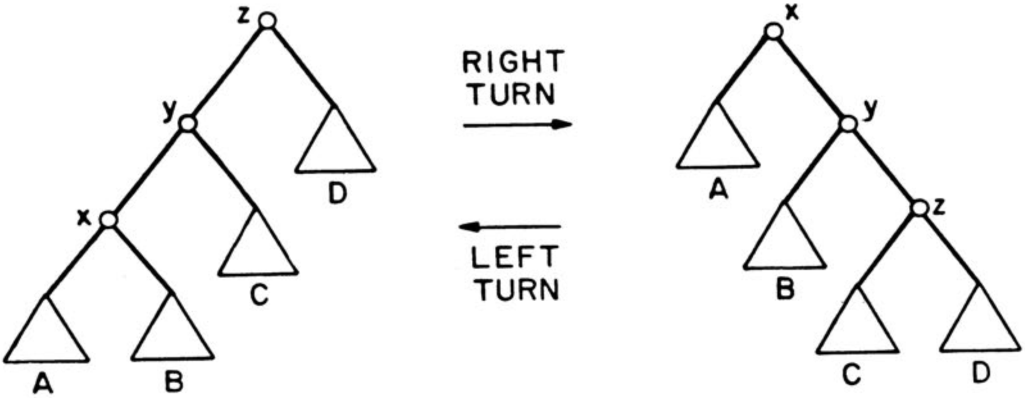


Figure 4. A turn on a binary tree.

REFERENCES

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

[2] R.E. Tarjan, *Data Structures and Network Algorithms,* Society for Industrial and Applied Mathematics, Philadelphia, PA, 1983.

[3] D.D. Sleator, R.E. Tarjan, and W.P. Thurston, ''Rotation Distance, Triangulations, and Hyperbolic Geometry,'' *Proceedings of the 18th Annual ACM Symposium on Theory of Computation,* pp. 122-135 (1986).

[4] K. Culik II and D. Wood, ''A Note on Some Tree Similarity Measures,'' *Info. Process. Lett.,* 15, pp. 39-42 (1982).

[5] D.E. Knuth, *The Art of Computer Programming,* Vol. 1: *Fundamental Algorithms,* 2nd ed., Addison-Wesley, Reading, MA, 1973.

[6] D.D. Sleator and R.E. Tarjan, ''Self-Adjusting Binary Search Trees,'' *J. Assoc. Comput. Mach.,* 32, pp. 652-686 (1985).

[7] R.E. Tarjan, ''Sequential Access in Splay Trees Takes Linear Time,'' *Combinatorica,* 5, pp. 367-378 (1985).

4.13 EFFICIENT DIGITAL SIGNATURE SCHEMES BASED ON MULTIVARIATE POLYNOMIAL EQUATIONS

Adi Shamir

Applied Mathematics
The Weizmann Institute
Rehovot, Israel

In 1983, Ong Schnorr and Shamir proposed a new type of digital signature scheme, based on multivariate polynomial equations modulo composite numbers. The scheme had some unique features (such as a constant arithmetic complexity and a universal modulus capability), which made it an attractive alternative to the RSA signature scheme. Unfortunately, the first two incarnations of this scheme (based on binary quadratic equations and ternary cubic equations) were shown to be breakable by J. M. Pollard. The major open problem concerning this scheme is whether there exists a safe incarnation which is still attractive from a practical point of view.

4.14 SOME RESULTS FOR THE PROBLEM "WAITING FOR GODOT"

Michael L. Honig

Bell Communications Research
Morristown, NJ 07960

Problem Statement: Consider an $M/D/1$ queueing system (Poisson arrival process, deterministic service times) and a *test customer*. The test customer is waiting for a friend whose arrival time is an exponentially distributed random variable. The test customer can either join the queue, if one exists, or wait outside the queue. Once the test customer joins the queue, he must stay in the queue until he reaches the server. If the test customer reaches the server after his friend arrives, he is served. Otherwise, he can either join the back of the queue, or wait outside the queue. What policy should the test customer follow to minimize the mean delay until service?

Let λ be the arrival rate of customers to the queue, let μ, the service rate, be normalized to one, and let α be the rate at which the test customer's friend arrives. At any given time t, let v denote the total service time (virtual work) of customers in front of the test customer, j denote the number of customers in back of the test customer, and k be a variable indicating whether or not the test customer's friend has arrived. Define the "move-along" policy as the policy whereby the test customer always stays in the queue. Under the move-along policy, the test customer immediately moves to the back of the queue if he reaches the server before his friend arrives. To prove that the move-along policy is optimal for given λ and α, a new class of policies is defined by insisting that the test customer *always* joins the queue, but he is allowed to move to the back of the queue at any time. Any policy allowed in the problem statement can be duplicated by a policy in this new class. If the move-along policy is the optimal policy in this new class of policies, then it must be the optimal policy in the original set of policies.

Define the state space for the problem as

$$\mathbf{S} \equiv \left\{ (v, j, k) \mid v \in R^+, j \in I^+, k \in \{0,1\} \right\},$$

where R^+ and I^+ are the set of non-negative reals and integers, respectively. Where unspecified, k is assumed to indicate that the test customer's friend has not arrived. The *state trajectory* from time $t = 0$ to $t = T$ is defined as the continuum of states visited from time $t = 0$ to time $t = T$, and is denoted as $\mathrm{s}[0, T]$. A general policy A is defined, which maps state trajectories to actions. For any policy A, the only actions allowed are either to stay in the current position or jump to the back of the queue (i.e., move from state (v, j) to state $(v + j, 0)$). Suppose the state trajectory from time $t = 0$ to $t = T$ is known to be $\mathrm{s}[0, T]$. The mean delay until the test customer is served starting at time T under policy A is defined as $d^A_{\mathrm{s}[0,T]}$. The mean delay until the test customer is served assuming the move-along policy is adhered to is denoted as $d_{v,j}$, where (v, j) is the current state. For the move-along policy the state trajectory previous to time T is irrelevant.

Theorem 1: Let $\mathrm{s}[0, T]$ be any state trajectory which reaches state (v, j) at time T. Then $d_{v,j} = \inf_A d^A_{\mathrm{s}[0,T]}$ if and only if $d_{v,j} \le d_{v+j,0}$, for all v and j.

This theorem holds for all A in the new class of policies defined above.

The move-along mean delay, $d_{v,j}$, satisfies the recursion

$$d_{v,j} = v + e^{-(\lambda+\alpha)v} \sum_{k=0}^{\infty} \frac{(\lambda v)^k}{k!} d_{j+k,0}$$

with boundary condition

$$d_{0,0} = \frac{1}{\lambda + \alpha} + \frac{\lambda}{\lambda + \alpha} d_{1,0} .$$

The solution can be written

$$d_{v,j} = v + e^{-x_\infty(v+j)}\, d_{0,0} + \sum_{k=0}^{\infty} \left[\lambda^k (j + \lambda v e^{-x_k}) \exp \left[-jx_k - \sum_{i=0}^{k-1} x_i - v x_{k+1} \right] \right],$$

where

$$x_{k+1} = \lambda(1 - e^{-x_k}) + \alpha, \;\; x_0 = 0 ,$$

and

$$x_\infty = \lim_{k\to\infty} x_k .$$

This expression can be used to prove the next two theorems.

Theorem 2: If $\lambda \le \alpha / (1 - e^{-\alpha})$, then $d_{v,j} < d_{v+j,0}$ for all positive v and j.

Theorems 1 and 2 therefore imply that the move-along policy is optimal if $\lambda \le \alpha / (1 - e^{-\alpha})$.

Theorem 3: Given any α, there exists a λ_0 such that if $\lambda \ge \lambda_0$, the move-along policy is not optimal.

Theorem 3 applies to the original problem statement, as well as to the modified problem in which the test customer may leave the queue at any time.

Acknowledgment: The author thanks T.J. Ott for completing the proof of Theorem 2.

4.15 PROBLEMS ON TILING, INDEPENDENT SETS, AND TRIGONOMETRIC POLYNOMIALS

D. Hajela

Bell Communications Research
Morristown, NJ 07960

Problem 1: Given $S \subseteq \mathbf{Z}^n, x \in \mathbf{Z}^n$, a translate of S by x is $S + x = \{s + x \mid s \in S\}$.

Question: Given $S \subseteq \mathbf{Z}^n$ with $|S| = m$:

(a) Do disjoint translates of S cover all of $\mathbf{Z}^n$?

(b) If so, how quickly can you decide this? Is there an algorithm polynomial in m to do this?

The answer is *yes* for S being a *periodic tile*. This means there exist $p_1, \ldots, p_n \in \mathbf{Z}^n$ such that

1. $\bigcup_{\substack{k_i \in \mathbf{Z} \\ 1 \le i \le n}} S + k_1 p_1 + k_2 p_2 + \cdots + k_n p_n = \mathbf{Z}^n$.

2. $(S + k_1 p_1 + \cdots + k_n p_n) \cap (S + j_1 p_1 + \cdots + j_n p_n) = \emptyset$ if $(k_1, \ldots, k_n) \ne (j_1, \ldots, j_n)$.

Problem 2: $A \subseteq \mathbf{Z}$ is called *independent* if $\sum_{1 \le i \le n} \varepsilon_i a_i = 0$ with $a_i \in A$. $\varepsilon_i = \pm 1, 0$ implies $\varepsilon_i = 0$ for all $1 \le i \le n$.

Question: (Pisier, 1981) For every *finite* $B \subseteq A$, say with $|B| = n$, *assume* there is a $C \subseteq B, |C| \ge n/2$ and C is independent. Prove or Disprove: A is a finite union of independent sets.

Problem 3: Note that for any $n_1, \ldots, n_k \in \mathbf{Z}$,

$$\sqrt{\pi}\,\sqrt{k} \le \max_{\theta \in [0,2\pi]} |\sin n_1 \theta + \cdots + \sin n_k \theta| \le k,$$

since

$$\int_0^{2\pi} | \sin n\theta + \cdots + \sin n_k \theta |^2 = \pi k .$$

Easy: There are $n_1, \ldots, n_k \in \mathbf{Z} / \{0\}$ such that

$$\max_{\theta \in [0,2\pi]} | \sin n_1\theta + \cdots + \sin n_k \theta | \le c \sqrt{k}$$

for c a fixed constant (e.g., Rudin-Shapiro polynomials).

Question: (H. Bohr, early 1950s, 1952?) Are there $0 < n_1 \le \cdots \le n_k$ with $n_i \in \mathbf{Z}$ for all i, such that

$$\max_{\theta \in [0, 2\pi]} | \sin n_1 \theta + \cdots + \sin n_k \theta | \le c \sqrt{k}$$

for some constant c ?

Known: There are $0 < n_1 \cdots \le n_k$ such that

$$\max_{\theta \in [0,2\pi]} | \sin n_1\theta + \cdots + \sin n_k\theta | \le ck^{2/3} .$$

4.16 COMMUNICATION COMPLEXITY OF SHIFTS

Thomas M. Cover

Departments of Electrical Engineering
and Statistics
Stanford University
Stanford, CA 94305

Let $\mathbf{X} = (X_1, X_2, \ldots, X_n)$, where $X_i \sim$ Bernoulli (1/2). Let $\mathbf{Y} = (X_{T+1}, X_{T+2}, \ldots, X_T)$, where T is uniformly distributed over $\{0, 1, 2, \ldots, n-1\}$. Thus $\mathbf{y}$ is a cyclic T-shift of $\mathbf{x}$. Here $T + k$ is modulo n.

How many bits must $\mathbf{y}$ communicate to $\mathbf{x}$ in order that $\mathbf{x}$ can determine the shift T? We claim that $\log(n + 1)$ bits are sufficient. Simply cycle $\mathbf{y}$ until $\sum_{i=1}^{n} y_{i+k} 2^i$ is largest, then transmit k. This works whenever $\mathbf{x},\mathbf{y}$ determine k.

The problem is much harder if $\mathbf{y}' = \mathbf{y} \oplus \mathbf{e}$, where $\mathbf{e} \sim$ Bernoulli (p). The noise in $\mathbf{y}'$ ruins the above approach. Now how many bits are required?

4.17 A CODING PROBLEM CONCERNING SIMULTANEOUS THRESHOLD DETECTION

Michael L. Fredman

Department of Electrical Engineering
and Computer Science
University of California at San Diego
La Jolla, CA 92093

We define a threshold detection system (TDS) of order N to be a collection of N binary codewords, $V_{1,} V_2, \ldots, V_N$, and N binary decision trees, $T_{1,} T_2, \ldots, T_N$, such that the tree T_i on input V_j reports "no" if $j < i$, and "yes" otherwise.

(A binary decision tree T is a binary tree each of whose internal nodes is labeled with a positive integer, and whose leaves are labelled "yes" or "no". When provided with a binary vector V as input, V defines a path through T by invoking the rule that upon reaching a node labeled j, branch left if the jth bit of V is 0, otherwise branch right. The "yes/no" label of the leaf reached is the output generated by T on input V.)

We define the read complexity of a TDS to be the maximum height of any of its N trees (the worst case decision time) and we define its write complexity to be the maximum Hamming weight of any of its N binary vectors (a measure perhaps of the power required to store one of these vectors - worst case). Our interest centers on the inherent trade-offs of the read/write complexities associated with a TDS. For example, if the read complexity of a TDS is 1, then its write complexity must be at least $(N-1)/2$, which is optimal; and if the write complexity of a TDS is 1, then its read complexity must be at least $(N-1)/2$, which is optimal. Our first problem is to estimate or evaluate the intermediate range of possible trade-offs. (The solution to this problem has implications regarding the complexity of certain data structure algorithms [1].)

If we try to minimize simultaneously both the read and write complexities, we can easily obtain an upper bound of 1 g(N) (the binary logarithm of N) by using the N binary vectors of dimension 1 g(N) for the V_i's, and simply having each T_i read these 1 g(N) bits. However, we can do better, obtaining an upper bound of roughly 1 g(N)/2.54 [1]. We can demonstrate [1] a lower bound of c lg(N)/lglg(N) (where c is a positive constant), but we suspect that the truth is asymptotic to c lg(N) .

Another variant of this problem is obtained by redefining the write complexity of a TDS to be the diameter of the set $\{ V_1, \ldots, V_N \}$.

REFERENCE

[1] M.L. Fredman, "The Complexity of Maintaining an Array and Computing its Partial Sums," *J. Assoc. Comput. Mach.*, pp. 250-260 (1982).

4.18 COOLING SCHEDULES FOR OPTIMAL ANNEALING

Bruce Hajek

Department of Electrical Engineering
University of Illinois
Urbana, IL 61801

We study a technique inspired by statistical mechanics, called simulated annealing [2] or stochastic relaxation [1], when applied to the maximum matching problem. The technique appears useful [2] for solving large, difficult (e.g., NP-hard) problems. Our motivation for studying the relatively simple maximum matching problem is to obtain sharp results concerning sufficient convergence rates. Numerous extensions can be readily conjectured.

Let G be an undirected graph. A matching is a set of edges, no two of which have a common vertex. Let M denote the set of all matchings for G. Let M^* denote the set of matchings M with maximum cardinality. The maximum matching problem is to find a matching in M^*. We will discuss a probabilistic method for doing this.

Definition. Given $\rho > 0, \Pi^\rho$ is the probability distribution on M defined by

$$\Pi^\rho(M) = \rho^{|M|}/Z \quad \text{where} \quad Z = \sum_{M \in M} \rho^{|M|}$$

and $|A|$ denotes the cardinality of a set A. Note that if we set Π^∞ to be the limit of Π^ρ as ρ tends to infinity, then

$$\Pi^\infty(M) = \begin{cases} \dfrac{1}{|M^*|} & \text{if } M \in M^* \\ 0 & \text{otherwise.} \end{cases}$$

Thus, if we could sample a random variable with distribution Π^ρ for large ρ then it would be a maximum cardinality matching with high probability.

A possible method of constructing a random variable with distribution Π^{ρ} for some large ρ is to simulate a Markov process whose steady-state distribution is Π^{ρ}. In practice, such simulations could be performed in discrete time. For theoretical purposes, we study a continuous-time Markov process with stationary distribution Π^{ρ}. The process can readily be simulated in discrete time, however.

Consider a Markov chain with state space M and transition rate matrix $Q^{\lambda,\,\mu}$ defined by

$$Q^{\lambda,\,\mu}(M, M') = \begin{cases} \lambda & \text{if } M' = M \cup \{e\},\ e \notin M \\ \mu & \text{if } M' = M/e,\ e \in M \\ 0 & \text{for other } M,\ M' \text{ with } M \neq M'. \end{cases}$$

In words, links disappear at rate μ and a link appears at a given site at rate λ, as long as the site is eligible. It is easy to show that the chain has equilibrium measure Π^{ρ}, where $\rho = \lambda/\mu$. In fact, a stronger condition is easily checked:

$$\Pi^{\rho}(M)\, Q^{\lambda,\,\mu}(M, M') = \Pi^{\rho}(M')\, Q(M', M) \text{ all } M, M'.$$

We now replace λ and μ by deterministic functions of time, (λ_t) and (μ_t). We call (λ_t, μ_t) a schedule since it determines the transition rates as a function of time, and we set $\rho_t = \lambda_t / \mu_t$. More formally, we consider the time-inhomogeneous Markov chain with transition rate matrix (Q_t) defined by $Q_t = Q^{\lambda_t,\,\mu_t}$. For convenience, we let $\lambda_t = 1$ for all t so that $\rho_t = 1/\mu_t$. We let α_t denote the probability distribution of the chain at time t. It satisfies the Kolmogorov forward equation

$$\alpha_t = \alpha_t\, Q_t\,.$$

If (μ_t) is "slowly varying," then we should have $\alpha_t \approx \Pi^{\rho_t}$ for large t. If, in addition, μ_t tends to zero (so ρ_t tends to infinity) as t tends to infinity, then Π^{ρ_t} converges to Π^{∞}. Thus, if μ_t converges to zero slowly enough, it should be true that α_t converges to Π^{∞}. This implies that the

Markov chain converges in probability to the set of maximal matchings, if μ_t varies slowly enough. (In fact, a little more is expected; α_t converges to a *uniform* distribution on M^*.)

A proof of convergence based on this reasoning was given in [1] for a different optimization problem. Our goal is to obtain sharp estimates on how fast we can let μ tend to zero.

In the following two theorems we implicitly make these assumptions on μ:

$$\mu_0 < +\infty, \ \mu_t \text{ is nonincreasing },$$

and

$$\lim_{t \to \infty} \mu_t = 0$$

Theorem 1: Fix a graph G.

(i) If all maximal matchings of G have maximum cardinality, then

$$\lim_{t \to \infty} \sum_{M \in M^*} \alpha_t (M) = 1 . \tag{1}$$

(ii) Otherwise, (1) is true if and only if

$$\int_0^\infty \mu_t \, dt = +\infty. \tag{2}$$

Theorem 2: The following conditions are equivalent:

$$\lim_{t \to \infty} \alpha_t = \Pi^\infty \text{ for all graphs } G ,$$

$$\int_0^\infty \mu_t^2 \, dt = +\infty. \tag{3}$$

Remarks.

1. For the sake of analogy with statistical mechanics, we note that Π^ρ can be reexpressed as

$$\Pi^\rho (M) = \exp(-V(M)/T)/Z ,$$

where $T = 1/\ln(\rho)$ and $V(M) = -|M|$. We call $V(M)$ the potential energy of a state M and T the temperature of the system. As T tends to zero, Π^ρ converges to the uniform distribution on the set M^* of minimum potential-energy states.

2. If for large t, μ_t has the form $\mu_t = t^{-1/c}$, equivalently if $T_t = c/\ln t$, then by Theorem 1, the chain converges in probability to the set of maximal matchings if and only if $c \geq 1$, and it converges to a uniform dist$^{\underline{n}}$ on such matchings if and only if $c \geq 2$.

The fact that condition (2) is strictly weaker than the condition (3) implies that a proof of Theorem 1 based purely on the motivating discussion we gave cannot be given.

REFERENCES

[1] S. Geman and D. Geman, "Stochastic Relaxation, Gibbs Distributions, and the Bayesian Restoration of Images," preprint, September 1983.

[2] S. Kirkpatrick, C.D. Gelatt, Jr., and M.P. Vecchi, "Optimization by Simulated Annealing," *Science*, 220, pp. 671-680 (1983).

CHAPTER V.

PROBLEMS IN THE CRACKS

Here we see the authors indulging themselves in a wider range of inquiry. Two of the problems, Ergodic Process Selection by T. Cover and Gambler's Ruin: A Random Walk on the Simplex by T. Cover, have been partially solved by Hajek (see Chapter VI).

Contents

5.1. PICK THE LARGEST NUMBER

Thomas M. Cover

Departments of Electrical Engineering
and Statistics
Stanford University
Stanford, CA 94305

Player 1 writes down any two distinct numbers on separate slips of paper. Player 2 randomly chooses one of these slips of paper and looks at the number. Player 2 must decide whether the number in his hand is the larger of the two numbers. He can be right with probability one-half. It seems absurd that he can do better.

We argue that Player 2 has a strategy by which he can correctly state whether or not the other number is larger or smaller than the number in his hand with probability *strictly greater than one-half.*

Solution: The idea is to pick a random *splitting number* T according to a density $f(t)$, $f(t) > 0$, for $t \in (-\infty, \infty)$. If the number in hand is less than T , decide that it is the smaller; if greater than T , decide that it is the larger.

Problem: Does this result generalize? Does it apply to the secretary problem?

5.2. ERGODIC PROCESS SELECTION[†]

Thomas M. Cover

Departments of Electrical Engineering
and Statistics
Stanford University
Stanford, CA 94305

Let $\{ (X_i, Y_i) \}_{i=1}^{\infty}$ be a jointly ergodic stationary stochastic process. Define a selection function $\delta_n : \mathbf{X}^{n-1} \times \mathbf{Y}^{n-1} \to \{ 0, 1 \}$, $n = 1, 2, \ldots$. We wish to maximize

$$\lim_{n \to \infty} \frac{1}{n} \sum_{i=1}^{n} (\delta_i(X_1, \ldots, X_{i-1}, Y_1, Y_2, \ldots, Y_{i-1}) X_i$$

$$+ (1 - \delta_i(X_1, \ldots, X_{i-1}, Y_1, \ldots, Y_{i-1})) Y_i)$$

over all selection functions. Thus δ_i chooses either X_i or Y_i to add to the running average.

It is intuitively clear that

$$\delta_i = \begin{cases} 1 , & E\{ X_i \mid \text{Past} \} > E\{ Y_i \mid \text{Past} \} \\ 0 , & \qquad\qquad\qquad < \\ \text{arb.}, & \qquad\qquad\qquad = \end{cases}$$

will maximize the above limit of the average return. The proof may be tricky.

[†] See Hajek's solution to this problem under moment constraints in Chapter VI.

5.3 FINDING THE OLDEST PERSON [†]

Pravin Varaiya

Department of Electrical Engineering
University of California
Berkeley, CA 94720

There are N people. Each person's age is independently and uniformly distributed over $[0, 1]$. You want to find who the oldest person is (not the person's age) with the minimum expected number of questions when the questions are structured as follows.

You pick a number $x(1)$ and ask, "Who is older than $x(1)$?" Depending on the response, you pick $x(2)$ and ask, "Who is older than $x(2)$?" Suppose at the end of K questions you determine who the oldest person is. Let $K^* := \min E\, K$, where the minimum is over all policies $x(1), x(2)$, and so on. The value of K^* can readily be determined via Dynamic Programming. (See, K. J. Arrow, L. Pesotchinsky, and M. Sobel, "On Partitioning of a Sample with Binary-Type Questions in Lieu of Collection Observations," Stanford University, September 1978.)

Suppose now we allow more general questions. You pick a subset $A(1)$ of $[0, 1]$ and ask "Whose age belongs to $A(1)$?" Then you select $A(2)$ and ask "Whose age belongs to $A(2)$?" Suppose you determine the oldest person after K questions. Let $K\# : \min E\, K$.

Conjecture: $K\# = K^*$.

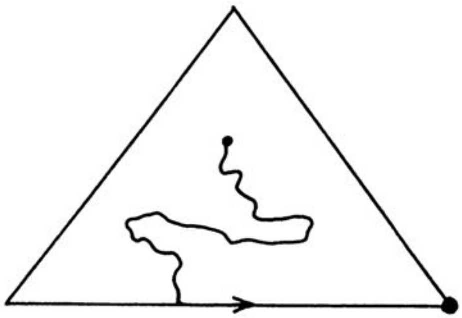
[†] See Chapter VI, Section 6.5 for solution.

5.4 GAMBLER'S RUIN: A RANDOM WALK ON THE SIMPLEX†

Thomas M. Cover

Departments of Electrical Engineering
and Statistics
Stanford University
Stanford, CA 94305

It is known that if two gamblers with capitals p and $1-p$, respectively, engage in a fair game (we can model it by Brownian motion on the unit interval starting at p) until one of the gamblers goes broke, then the gambler with initial capital p will win the game with probability p. Now suppose that there are m gamblers with capitals corresponding to a point $\mathbf{p}$ in the simplex $p_i \geq 0$, $\sum p_i = 1$. A random walk in the simplex occurs, and the gamblers go broke one by one. Once a gambler goes broke, he stays broke. What is the induced probability distribution on the order in which the gamblers go broke?



† Hajek has exhibited a solution to this problem for $m = 3$ gamblers. See Chapter VI.

5.5 LINEAR SEPARABILITY

Thomas M. Cover

Departments of Electrical Engineering
and Statistics
Stanford University
Stanford, CA 94305

Let $(\mathbf{X}_i, \theta_i)$, $i = 1, 2, \ldots, n$, be i.i.d. random pairs, where $\{\theta_i\}$ is Bernoulli with parameter 1/2, and $\mathbf{X}_i \sim f_{\theta_i}(\mathbf{x})$, $\mathbf{x}_i \in \mathbf{R}^d$. We say $\{(\mathbf{X}_i, \theta_i)\}_{i=1}^n$ is *linearly separable* if there exits a vector $\mathbf{w} \in \mathbf{R}^d$ and a real number T such that

$$\begin{aligned} \mathbf{w}^t \mathbf{x}_i &\geq T, \quad \theta_i = 1 \\ &< T, \quad \theta_i = 0, \qquad \text{for} \quad i = 1, 2, \ldots, n. \end{aligned}$$

Let $P(n, d, f_0, f_1)$ be the associated probability that $\{(X_i, \theta_i)\}_{i=1}^n$ is linearly separable.

The following results are known.

Theorem 1: Identical distributions [1,2].

$$P(n, d, f, f) = 2^{-(n-1)} \sum_{i=0}^{d} \begin{bmatrix} n-1 \\ i \end{bmatrix},$$

for any density $f(\mathbf{x})$.

Theorem 2: Distributions differing by translation [3].

Let $f_2(\mathbf{x}) = f_1(\mathbf{x} + t\,\mathbf{v})$. Then $P(n, d, f_1, f_2)$ is monotonically increasing in $t \geq 0$. When $t = 0$, $P(n, d, f_1, f_2) = P(n, d, f, f)$, and $P(n, d, f_1, f_2) \to 1$, as $t \to \infty$.

Theorem 3:. Distributions differing by scale (Krueger, unpublished).

Let $f_2(\mathbf{x}) = \frac{1}{a} f_1(a\mathbf{x})$, $a > 0$. Then $P(n, d, f_1, f_2)$ is monotonically nondecreasing in a , for $a \geq 1$.

All this seems to suggest that different densities lead to an increase in the probability of separability. Hence the following:

Conjecture.

$$P(n, d, f_1, f_2) \geq \left(\frac{1}{2} \right)^{n-1} \sum_{i=0}^{d} \binom{n-1}{i} ,$$

for all densities $f_1(x), f_2(x)$.

REFERENCES

[1] T. Cover, "Geometrical and Statistical Properties of Systems of Linear Inequalities with Applications in Pattern Recognition," *IEEE Trans. Electronic Comput.*, EC-14, No. 3, pp. 326-334 (June 1965).

[2] R.O. Winder, "Single State Threshold Logic," *Switching Circuit Theory and Logical Design,* AIEE Special Publications S-134, pp. 321-332, September 1961.

[3] F. Bruckstein and T. Cover, "Monotonicity of Linear Separability under Translation," *IEEE Trans. Pattern Anal. Machine Intelligence,* PAMI-7, No. 3, pp. 355-358 (May 1985).

5.6 THE GENERIC RANK OF A^2

John N. Tsitsiklis

Laboratory for
Information and Decision Systems
M.I.T.
Cambridge, MA 02139

We define a *structured matrix* $\mathbf{A}$ to be the set of all matrices (of a given dimension $n \times n$) in which certain entries are constrained to be zero. We then define the *generic rank* of $\mathbf{A}$ to be the maximum of the ranks of any $A \in \mathbf{A}$. It turns out that the generic rank of $\mathbf{A}$ may be computed easily. Form a bipartite graph $G = (V, E)$, where the set of vertices is $V = \{1, 2, \ldots, n; 1', \ldots, n'\}$. For any $(i, j) \in \{1, \ldots, n\}^2$, the edge (i, j') belongs to E if and only if the ijth entry of matrices in $\mathbf{A}$ is not constrained to be zero. Then, the generic rank of $\mathbf{A}$ equals the maximum number of edges in any bipartite matching of that graph.

Suppose that we are given two structured matrices $\mathbf{A}, \mathbf{B}$ of dimensions $m \times n$, $n \times m$, respectively. We define the generic rank of $\mathbf{A}\,\mathbf{B}$ as the maximum of the ranks of AB over all $A \in \mathbf{A}$, $B \in \mathbf{B}$. This problem is related to the problem of finding the "structurally" fixed modes of a controlled linear system and has been studied under various guises [1-7]. It was shown in [2] that this problem is equivalent to a simple network flow problem and can therefore be solved in polynomial time, as follows. Construct a graph for each one of the two structured matrices $\mathbf{A}, \mathbf{B}$, as in the previous paragraph, and join the two graphs by identifying the nodes corresponding to columns of $\mathbf{A}$ with the nodes corresponding to rows of $\mathbf{B}$ (see Figure 1). Let each node in this graph have unit capacity. Then, the generic rank of $\mathbf{A}\,\mathbf{B}$ is equal to the maximum flow that may be transferred through this graph.

Suppose now that $m = n$ and that $\mathbf{A} = \mathbf{B}$, so that the A and B matrices have to obey the same constraints. (Still, this does not require that

$A = B$.) If we impose the additional requirement that $A = B$, does the generic rank change? More formally, is it true that

$$\max_{\substack{A \in \mathbf{A} \\ B \in \mathbf{B}}} \operatorname{rank}(AB) = \max_{A \in \mathbf{A}} \operatorname{rank} A^2 \; ?$$

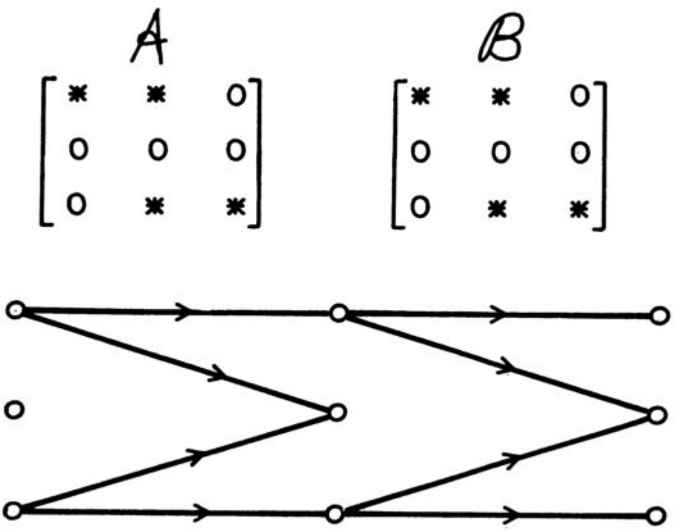


Figure 1. Example of the redirection to a network flow problem.

REFERENCES

[1] C.T. Lin, "Structural Controllability," *IEEE Trans. Aut. Control,* 19, pp. 201-208 (1974).

[2] C.H. Papadimitriou and J.N. Tsitsiklis, "A Simple Criterion for Structurally Fixed Modes," *Syst. Control Lett.,* 4, pp. 333-337 (1984).

[3] V. Pichai, M.E. Sezer and D.D. Siljak, "A Graphical Test for Structurally Fixed Modes," *Math. Modeling,* 4, pp. 339-348 (1983).

[4] V. Pichai, M.E. Sezer, and D.D. Siljak, "A Graph-Theoretic Characterization for Structurally Fixed Modes," *Automatica,* 20, pp. 247-250 (1984).

[5] K. Reinschke, "Graph-Theoretic Characterization of Fixed Modes in Centralized and Decentralized Control," *Int. J. Control* 39, pp. 715-729.

[6] M.E. Sezer and D.D. Siljak, "Structurally Fixed Modes," *Syst. Control Lett.,* 1, pp. 60-64 (1981).

[7] R.W. Shields and J.B. Pearson, "Structural Controllability of Multi-input Linear Systems," *IEEE Trans. Aut. Control,* 21, pp. 203-212 (1976).

5.7 THE STABILITY OF THE PRODUCTS OF A FINITE SET OF MATRICES

John N. Tsitsiklis

Laboratory for
Information and Decision Systems
M.I.T.
Cambridge, MA 02139

Let $F = \{A_1, \ldots, A_N\}$ be a set of $n \times n$ matrices. Given a sequence $S = \{ A_{i_k}\}_{k=1}^{\infty}$, with $A_{i_{ki}} \in F$, we consider products of the form $B_{M,S} = \prod_{k=1}^{M} A_{i_k}$. We are interested in questions of the following type:

1. Is the set $\{B_{M,S} : M = 1, 2, \ldots \}$ bounded for all sequences S? (We will then say that F is stable.) Does $B_{M,S}$ converge to zero, as $M \to \infty$ for all S?
2. What happens if we impose some restrictions on the set of allowed sequences S?
3. What are some simple classes of matrices for which the answers to 1 and 2 become simpler?

Motivation. Such problems arise in at least two different contexts:

(a) *Lyapunov stability of time-varying linear systems [1,2].* Given a system of the form $x(t+1) = A(t)\,x(t)$, suppose that it is known that $A(t) \in F$, for each t, but that the exact value of $A(t)$ is not a priori known, because of exogenous conditions or changes in the operating point of a nonlinear system. Questions 1-3 refer to the stability of such a system.

(b) *Asynchronous computation.* A serial iterative algorithm may be visualized as a process whereby a fixed sequence of operations is applied to the initial data. Accordingly, in an "asynchronous" algorithm, a sequence of operations is again applied to the input data, except that the exact order at which different operations are applied is unknown and possibly chaotic. This leads naturally to the question whether the end result is asymptotically independent of the actual order. In this context, questions 1-3 are relevant to convergence conditions for asynchronous (and typically distributed) algorithms for the solution of linear equations or certain classes of optimization problems [3-5].

The main available result states that F is stable if and only if there exists a convex neighborhood V of the origin such that $A_k V \subset V, \ \forall A_k \in F$ [1,2].

We now pose some more specific questions.

1. We restrict to sequences S such that each matrix $A_k \in F$ appears infinitely many times in that sequence. Are there any simple necessary and sufficient conditions (referring to the existence of convex neighborhoods with certain properties) for $B_{M,S}$ to converge to zero as $M \to \infty$, for all such S?
2. We may also pose the above question under a more stringent requirement on the sequences S. Namely, we require that, for a given integer K, each matrix $A_k \in F$ appears at least once every K times in the sequence.
3. Assuming that some simple conditions have been found for problems 1 and 2 above, are there any effective algorithmic tests for them?
4. A class of algorithms has been suggested in [1,2] to test whether there exists a convex neighborhood V such that $A_k V \subset V, \ \forall A_k \in F$. However, these algorithms do not necessarily terminate in a finite number of steps (although they almost always do). Is there a finite algorithm for this problem?
5. Suppose that we alter slightly the original problem to the following: Does there exist a rectangular V such that $A_k V \subset V, \ \forall A_k \in F$? If

the orientation of the rectangle V is also fixed, this problem reduces to a simple linear programming problem. Is there a simple solution if the orientation of V is left free?

REFERENCES

[1] R.K. Brayton and C.H. Tong, "Stability of Dynamical Systems: a Constructive Approach," *IEEE Trans. Circuits Syst.,* 26, pp. 224-234 (1980).

[2] R.K. Brayton and C.H. Tong, "Constructive Stability and Asymptotic Stability of Dynamical Systems," *IEEE Trans. Circuits Syst.,* 27, pp. 1121-1130 (1980).

[3] D. Chazan and W. Miranker, "Chaotic Relaxation," *Linear Algebra Appl.,* 2, pp. 199-222 (1969).

[4] D.P. Bertsekas, "Distributed Asynchronous Computation of Fixed Points," *Math. Programming,* 27, pp. 107-120 (1983).

[5] J.N. Tsitsiklis, "Problems in Decentralized Decision Making and Computation," Ph.D. thesis, Department of EECS, M.I.T, Cambridge, MA, 1984.

5.8 ELECTRICAL TOMOGRAPHY

E.N. Gilbert and L.A. Shepp

AT&T Bell Laboratories
Murray Hill, NJ 07974

1. Introduction.

Tomography deduces a physical function $\sigma(P)$ (say a density), at points P inside a living organ, from measurements made on the outside. With suitable interpretation, $\sigma(P)$ may reveal tumors or other abnormalities. In X-ray tomography, $\sigma(P)$ is an attenuation coefficient, external measurements supply integrals

$$\alpha(L) = \int_L \sigma(P)\, ds \tag{1}$$

along straight line rays L through the organ, and the integral equation (1) is solved for $\sigma(P)$ (see [1]). In another kind of tomography, using nuclear magnetic resonance measurements, $\sigma(P)$ is deduced from integrals over planes instead of lines (see [2]).

Here we give a very preliminary feasibility study of electrical tomography. Each measurement will pass a small current through the organ between two external electrodes; the voltage between another pair of electrodes is then recorded. The function to be determined is the electrical conductivity $\sigma(P)$. If $\sigma(P)$ could be deduced easily from these measurements, electrical tomography would have the advantages of simple measuring equipment offering no health hazards. Unfortunately, there is still no simple solution to the problem of obtaining $\sigma(P)$ from the measurements. The difficulty in finding $\sigma(P)$ seems to be related to the fact that each measurement involves the whole organ, not just points on a line or plane. Without actually solving for $\sigma(P)$ in general, one can still produce examples showing that certain large changes in $\sigma(P)$ have only small effects on external measurements. Then, to give meaningful results, electrical tomography seems to require high-accuracy measurements.

2. Measurements.

The current density vector J (in amperes per square meter) is derivable from a potential function u (in volts) by $J = -\sigma \text{ grad } u$, where u satisfies a partial differential equation

$$\operatorname{div}(\sigma \nabla u) = 0 . \tag{2}$$

If only one could measure u internally, (2) might be solved as a first-order partial differential equation for the unknown $\sigma = \sigma(P)$. The characteristics of this equation are precisely the current lines (having everywhere the direction of grad u). Along a current line, one finds

$$\frac{d}{du} \log \sigma = - \frac{\Delta u}{|\nabla u|^2},$$

but even this only determines $\sigma(P)$ within a constant of integration that can differ for different lines. Potentials for several different flow patterns will be needed before $\sigma(P)$ becomes well-determined. Of course the real problem, with u available only externally, may require many more flows.

A finite number of measurements, each using two current probes and two voltage probes, can use only a finite number n of probe locations. Viewed externally, the organ is an unknown electrical network with n accessible terminals. One may imagine these terminals interconnected by a discrete network N of unknown resistors. It is unreasonable to expect external measurements to determine the configuration, or graph, of N. For example, with $n = 3$, external measurements cannot distinguish between Y and Δ configurations (see [3]). Instead, one must assume N to have some convenient graph, say a lattice, and try to determine the resistance values.

Simple examples of problems of this type are instructive. Suppose first that N contains resistors $r_1, \ldots, r_n$ connected in a ring, with r_i between terminals i and $i+1$. Suppose there are n measurements, the ith using terminals i and $i+1$ for both the current probes and voltage probes. Each measurement then determines the resistance p_i seen across the terminals of r_i, and one requires $r_1, \ldots, r_n$ satisfying

$$\frac{1}{p_i} = \frac{1}{r_i} + \frac{1}{R - r_i}\ , \tag{3}$$

where

$$R = r_1 + \ldots + r_n\ . \tag{4}$$

One can solve (3) for r_i, treating R as an unknown parameter to be determined from (4). Although each equation (3) has two roots, only solutions with real positive r_i are admissible. It turns out that only one of the 2^n choices of roots produces a solution (see [4]). C. L. Mallows has also shown that $\binom{n}{2}$ resistances r_{ij}, arranged in a complete graph, are uniquely determined from the resistances p_{ij} that can be measured externally. Of course, simple resistance measurements with point probes are not apt to be reliable in tomography because the measured resistances will depend on the probe pressure used.

Care is needed to choose a graph such that external measurements determine unique resistances. For example, in Figure 1, N has 8 resistors and $n = 4$ terminals. Since voltage probe pairs can have $\binom{4}{2} = 6$ locations, and the current probes likewise, 36 measurements might seem ample to determine the resistances. However, the three sets of resistance values in Table 1 give like results in all 36 measurements. With n terminals, there are only $n - 1$ independent ways of injecting current and only $n - 1$ independent voltage measurements. Further dependencies, that follow from the reciprocity theorem, reduce the number of independent measurements to $\binom{n}{2}$. Figure 1 should be replaced by a network with only 6 resistors.

The graph should also be chosen so that its resistances (or conductances) provide a discrete approximation of $\sigma(P)$ in continuous tissue. The complete graph, for example, is inappropriate. Instead, resistors might be arranged in a cubic lattice. If the array fills a large cube, b resistors on each edge, there are $n = 6b^2 + 2$ accessible terminals and only $3b(b+1)^2 < \binom{n}{2}$ resistors. Since there are more possible independent external measurements than resistors, there will be problems of either avoiding redundant measurements or using them deliberately to counteract measurement errors.

3. Accuracy.

It seems that electrical tomography will require extremely accurate measurements. This can be shown by a pair of examples having potentials, u, u', differing only slightly externally, but which are solutions of (1) with radically different conductances $\sigma(P)$, $\sigma'(P)$. In one such pair, the organ is taken as the unit sphere and current I is injected between north and south poles. For the first solution, $\sigma(P)$ is taken to be a constant σ_0. For the second solution, $\sigma'(P)$ is the same constant σ_0 outside a smaller concentric sphere of radius a and $\sigma'(P) = \sigma_i$, another constant, inside the smaller sphere. Since equation (1) reduces to Laplace's equation in regions of constant $\sigma(P)$, the potentials u, u' can be found using spherical harmonics. On the unit sphere, the two potentials are found to differ by an amount given by a series, in which the most important contribution is a dipole term

$$\frac{2\pi\sigma_0(u' - u)}{I} = \frac{9(1 - \delta)\, a^3 \cos\theta}{1 + 2\delta + 2(1 - \delta)\, a^3} + O(a^7).$$

Here $\delta = \sigma_i / \sigma_0$, θ is the colatitude angle measured away from the north pole, and potentials have been made equal on the equator. In any measurement, the two voltage readings can then differ by at most

$$\frac{9I\,(1 - \delta)\, a^3}{\pi\sigma_0\,(1 + 2\delta + 2(1 - \delta)\, a^3)} + O(a^7).$$

If a is not large, this difference is uniformly small or order $O(a^3)$ whether the inner sphere represents a hole ($\delta = 0$) or a lump of metal ($\delta = \infty$). Injecting current between electrodes not diametrically opposite produces even smaller differences in voltage readings.

By contrast, in X-ray tomography, changing $\sigma(P)$ within a sphere of radius a has a bigger effect $O(a)$ on some of the line integrals $\alpha(L)$ in (1).

REFERENCES

[1] L.A. Shepp and J.B. Kruskal, ''Computerized Tomography: The New Medical X-Ray Technology,'' *Am. Math. Monthly,* 85, pp. 420-439 (1972).

[2] L.A. Shepp, ''Computerized Tomography and Nuclear Magnetic Resonance, *J. Comp. Asst. Tomo.,* 4, pp. 94-107 (1980).

[3] A.E. Kennelly, ''The Equivalence of Triangles and Three-Pointed Stars in Conducting Networks,'' *Electrical World and Engineer,* 34, No. 12, p. 413 (1899). Most textbooks on electrical circuits also discuss this theorem.

[4] E.N. Gilbert and L.A. Shepp, ''A Resistance Problem,'' *SIAM Rev.,* 26, p. 429 (1984).

Table 1. Resistance Values for Three Networks (Figure 1), Indistinguishable by External Measurement

	Network		
Resistance	1	2	3
a	54	∞	∞
b	54	54	45
c	54	45	45
d	54	54	∞
e	54	18	6
f	54	18	30
g	54	90	150
h	54	90	30

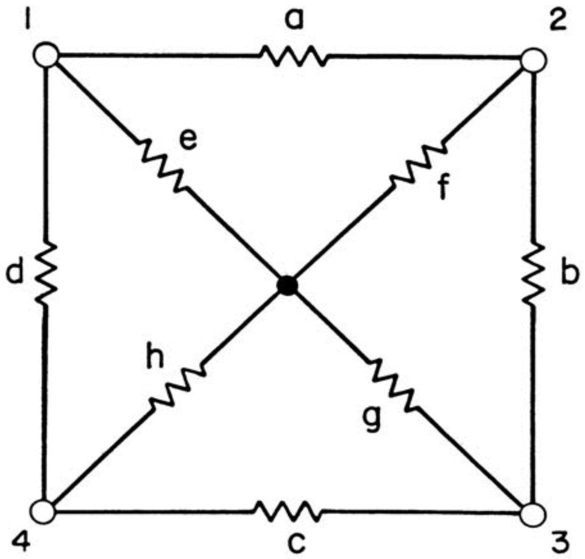


Figure 1. A four-terminal network.

5.9 FIGURE-GROUND PROBLEM FOR SOUND

Thomas M. Cover

Departments of Electrical Engineering
and Statistics
Stanford University
Stanford, CA 94305

The impossible tuning fork is a good example of a figure-ground optical illusion. Tracing the body of the tuning fork leads to the background. What is figure and what is ground?

Another famous example is the face-vase illusion. Two mirror image blue faces lie against a red background. If one stares at the picture for awhile, one sees a red vase against a blue background. Attention flickers from one foreground - background pair to its complement.

Can we create the same sort of illusion for sound? Consider a rich tone against a background of silence. This tone goes off and on in such a manner that it is perceived by the ear-brain as a rhythm, dah di da da, dah, dah . . . . Is it possible that the silence that lies between these bursts of sound also qualifies as a rhythm? Not the same rhythm, but one of equally compelling artistic merit? If so, we wish to give this background silence equal status by providing another rich tone for the silence. The whole waveform then is of roughly constant power. The "blue" tone predominates until, for some arbitrary reason, the ear-brain focuses on the "red" tone. One of two interesting rhythms is perceived against a "constant" background. This would constitute an aural figure-ground illusion.

It remains to discover a rhythm the complement of which is also a rhythm and to choose the sounds appropriately.

5.10 THE ENTROPY POWER INEQUALITY AND THE BRUNN-MINKOWSKI INEQUALITY

Thomas M. Cover

Departments of Electrical Engineering
and Statistics
Stanford University
Stanford, CA 94305

The Brunn-Minkowski inequality states that the nth root of the volume of the set sum of two sets in Euclidean n-space is greater than or equal to the sum of the nth roots of the volumes of the individual sets. The entropy power inequality states that the effective variance of the sum of two independent random variables with densities in n-space is greater than or equal to the sums of their effective variances. Formally, the inequalities can be seen to be similar. We are interested in determining whether this occurs by chance or whether there is a fundamental idea underlying both inequalities.

Brunn-Minkowski: Let $V(A)$ be the volume of A. If $A, B \subseteq \mathbf{R}^n$, then $V(A+B) \geq V(A'+B')$, where A', B' are n-spheres such that $V(A') = V(A)$ and $V(B') = V(B)$.

Entropy Power: Let $H(X) = -\int f(x) \ln f(x) dx$, where f is the probability density of X. If X and Y are independent n-vectors with probability densities, then $H(X+Y) \geq H(X'+Y')$, where X' and Y' are independent spherical normal with $H(X') = H(X)$ and $H(Y') = H(Y)$.

REFERENCE

[1] H.M. Costa and T.M. Cover, "On the Similarities Between the Entropy Power and Brunn-Minkowski Inequalities," *IEEE Trans. Inf. Theory*, 30, pp. 837-839 (Nov. 1984).

5.11 THE WEIRD AND WONDERFUL CHEMISTRY OF AUDIOACTIVE DECAY

J. H. Conway

Department of Mathematics
Princeton University
Princeton, NJ 08544

1. Introduction

Suppose we start with a string of numbers (i.e., positive integers), say

5 5 5 5 5.

We might describe this in words in the usual way as "five fives," and write down the *derived* string

5 5.

This we describe as "two fives," so it yields the next derived string

2 5

which is "one two, one five," giving

1 2 1 5

namely, "one one, one two, one one, one five," or

1 1 1 2 1 1 1 5

and so on. What happens when an arbitrary string of positive integers is repeatedly derived like this?

I note that more usually one is given a sequence such as

55555 ; 55 ; 25 ; 1215 ; 11121115 ;

and asked to guess the generating rule or the next term.

The numbers in our strings are usually single-digit ones, so we'll call them *digits* and usually cram them together as we have just done. But occasionally we want to indicate the way the number in the string was obtained, and we can do this neatly by inserting commas recalling the commas and quotes in our verbal descriptions, thus:

$$5\ 5\ 5\ 5\ 5$$
$$,5\ 5,$$
$$,2\ 5,$$
$$,1\ 2,1\ 5,$$
$$,1\ 1,1\ 2,1\ 1,1\ 5,$$
$$\ldots$$

The insertions of these commas into a string or portion thereof is called *parsing*.

We'll often denote repetitions by indices in the usual way, so that the derivation rule is

$$a^{\alpha}\ b^{\beta}\ c^{\gamma}\ d^{\delta}\ \cdots\ \rightarrow \alpha a \beta b \gamma c \delta d\ \cdots$$

When we do this, it is always to be understood that the repetitions are collected maximally, so that we must have

$$a \neq b,\ b \neq c,\ c \neq d\ , \ldots\ .$$

Since what we write down is often only a *chunk* of the entire string (i.e., a consecutive subsequence of its terms), we often use the square brackets "[" or "]" to indicate that the apparent left or right end really is the end. We also introduce the formal digits

0, as an index, to give an alternative way of indicating the ends (see below)

X for an arbitrary nonzero digit, and

$\neq n$ for any digit (maybe 0) other than n .

Thus	$X^0\ a^{\alpha}\ b^{\beta}\ c^{\gamma}$	means the same as $[\ a^{\alpha}\ b^{\beta}\ c^{\gamma}$
	$a^{\alpha}\ b^{\beta}\ c^{\gamma}\ X^0$	means the same as $a^{\alpha}\ b^{\beta}\ c^{\gamma}]$
	$a^{\alpha}\ b^{\beta}\ c^{\gamma}\ X^{\neq 0}$	means $a^{\alpha}\ b^{\beta}\ c^{\gamma}$ followed by at least another digit,
and	$a^{\alpha}\ b^{\beta}\ c^{\gamma}(\neq 2)^{\neq 0}$	means that this digit is not a 2.

I'm afraid that this heap of conventions makes it quite hard to check the proofs, since they cover many more cases than one naively expects. To separate these cases would make this article very long and tedious, and the reader who really wants to check all the details is advised first to spend some time practicing the derivation process. Note that when we write $L \to L' \to L'' \to \cdots$ we mean just that every string of type L derives to one of type L', every string of type L' derives to one of type L'', and so on. So when in our proof of the Ending Theorem we have

$$n^n] \overset{(n \neq 2)}{\to} n^{\neq n}] \to n']$$

the fact that the left arrow is asserted only when $n \neq 2$ does not excuse us from checking the right arrow for $n = 2$. (But, since $n > 1$ is enforced at that stage in the proof, we needn't check either of them for $n = 1$.)

By applying the derivation process n times to a string L, we obtain what we call its nth *descendant,* L_n. The string itself is counted among its descendants, as the 0th.

Sometimes a string factors as the product LR of two strings L and R whose descendants never interfere with each other, in the sense that $(LR)_n = L_n R_n$ for all n. In this case, we say the LR *splits* as $L.R$ (dots in strings will always have this meaning). It is plain that this happens just when (L or R is empty or) the last digit of L_n always differs from the first one of R_n. Can you find a simple criterion for this to happen? (When you give up, you'll find the answer in our Splitting Theorem.)

Obviously, we call a string with no nontrival splittings an *atom,* or *element.* Then every string is the split product, or *compound,* of a certain number of elements, which we call the elements it *involves.* There are infinitely many distinct elements, but most of them only arise from specially chosen starting strings. However, there are some very interesting elements that are involved in the descendants of every string except the boring ones [ ] and [22]. Can you guess how many of these *common elements* there are? (Hint: we have given them the names Hydrogen, Helium, Lithium , . . . , Uranium.)

It's also true (but ASTONISHINGLY hard to prove) that *every* string eventually decays into a compound of these elements, together with perhaps a few others (namely, isotopes of Plutonium and Neptunium, as defined below). Moreover, all strings except the two boring ones increase in length exponentially at the same constant rate. (This rate is roughly 1.30357726903: it can be precisely defined as the largest root of a certain algebraic equation of degree 71.) Also, the relative abundances of the elements settle down to fixed numbers (zero for Neptunium and Plutonium). Thus, of every million atoms about 91790 on average will be of Hydrogen, the commonest element, while about 27 will be of Arsenic, the rarest one.

You should get to know the common elements, as enumerated in our Periodic Table. The abundance (in atoms per million) is given first, followed by the atomic number and symbol as in ordinary chemistry. The actual digit-string defining the element is the numerical part of the remainder of the entry, which, when read in full, gives the derivate of the element of next highest atomic number, split into atoms. Thus, for example, the last line of the Periodic Table tells us that Hydrogen (H) is our name for the digit-string 22, and that the next higher element, Helium (He), derives to the compound

Hf.Pa.H.Ca.Li

which we might call

"Hafnium-Protactinium-Hydrogen-Calcium-Lithide"!

Not everything is in the Periodic Table! For instance, the single digit string "1" isn't. But watch:

1
11
21
1211
111221
312211
13112221
11132.13211 = Hf.Sn

after a few moves it has become Hafnium Stannide! This is an instance of our Cosmological Theorem, which asserts that the exotic elements (such as "1") all disappear soon after the Big Bang.

The Periodic Table (Uranium to Silver)

abundance	n	E_n	E_n inside the derivate of E_{n+1}
102.56285249	92	U	3
9883.5986392	91	Pa	13
7581.9047125	90	Th	1113
6926.9352045	89	Ac	3113
5313.7894999	88	Ra	132113
4076.3134078	87	Fr	1113122113
3127.0209328	86	Rn	311311222113
2398.7998311	85	At	Ho.1322113
1840.1669683	84	Po	1113222113
1411.6286100	83	Bi	3113322113
1082.8883285	82	Pb	Pm.123222113
830.70513293	81	Tl	111213322113
637.25039755	80	Hg	31121123222113
488.84742982	79	Au	132112211213322113
375.00456738	78	Pt	111312212221121123222113
287.67344775	77	Ir	3113112211322112211213322113
220.68001229	76	Os	1321132122211322212221121123222113
169.28801808	75	Re	111312211312113221133211322112211213322113
315.56655252	74	W	Ge.Ca.312211322212221121123222113
242.07736666	73	Ta	13112221133211322112211213322113
2669.0970363	72	Hf	11132.Pa.H.Ca.W
2047.5173200	71	Lu	311312
1570.6911808	70	Yb	1321131112
1204.9083841	69	Tm	11131221133112
1098.5955997	68	Er	311311222.Ca.Co
47987.529438	67	Ho	1321132.Pm
36812.186418	66	Dy	111312211312
28239.358949	65	Tb	3113112221131112
21662.972821	64	Gd	Ho.13221133112
20085.668709	63	Eu	1113222.Ca.Co.
15408.115182	62	Sm	311332
29820.456167	61	Pm	132.Ca.Zn
22875.863883	60	Nd	111312
17548.529287	59	Pr	31131112
13461.825166	58	Ce	1321133112
10326.833312	57	La	11131.H.Ca.Co
7921.9188284	56	Ba	311311
6077.0611889	55	Cs	13211321
4661.8342720	54	Xe	11131221131211
3576.1856107	53	I	311311222113111221
2743.3629718	52	Te	Ho.1322113312211
2104.4881933	51	Sb	Eu.Ca.3112221
1614.3946687	50	Sn	Pm.13211
1238.4341972	49	In	11131221
950.02745646	48	Cd	3113112211
728.78492056	47	Ag	132113212221

The Periodic Table (Palladium to Hydrogen)

abundance	n	E_n	E_n inside the derivate of E_{n+1}
559.06537946	46	Pd	111312211312113211
428.87015041	45	Rh	311311222113111221131221
328.99480576	44	Ru	Ho.132211331222113112211
386.07704943	43	Tc	Eu.Ca.311322113212221
296.16736852	42	Mo	13211322211312113211
227.19586752	41	Nb	1113122113322113111221131221
174.28645997	40	Zr	Er.12322211331222113112211
133.69860315	39	Y	1112133.H.Ca.Tc
102.56285249	38	Sr	3112112.U
78.678000089	37	Rb	1321122112
60.355455682	36	Kr	11131221222112
46.299868152	35	Br	3113112211322112
35.517547944	34	Se	13211321222113222112
27.246216076	33	As	11131221131211322113322112
1887.4372276	32	Ge	31131122211311122113222.Na
1447.8905642	31	Ga	Ho.13221133122211332
23571.391336	30	Zn	Eu.Ca.Ac.H.Ca.312
18082.082203	29	Cu	131112
13871.124200	28	Ni	11133112
45645.877256	27	Co	Zn.32112
35015.858546	26	Fe	13122112
26861.360180	25	Mn	111311222112
20605.882611	24	Cr	31132.Si
15807.181592	23	V	13211312
12126.002783	22	Ti	11131221131112
9302.0974443	21	Sc	3113112221133112
56072.543129	20	Ca	Ho.Pa.H.12.Co
43014.360913	19	K	1112
32997.170122	18	Ar	3112
25312.784218	17	Cl	132112
19417.939250	16	S	1113122112
14895.886658	15	P	311311222112
32032.812960	14	Si	Ho.1322112
24573.006696	13	Al	1113222112
18850.441228	12	Mg	3113322112
14481.448773	11	Na	Pm.123222112
11109.006821	10	Ne	111213322112
8521.9396539	9	F	31121123222112
6537.3490750	8	O	132112211213322112
5014.9302464	7	N	111312212221121123222112
3847.0525419	6	C	3113112211322112211213322112
2951.1503716	5	B	1321132122211322212221121123222112
2263.8860325	4	Be	111312211312113221133211322112211213322112
4220.0665982	3	Li	Ge.Ca.312211322212221121123222112
3237.2968588	2	He	13112221133211322112211213322112
91790.383216	1	H	Hf.Pa.22.Ca.Li

2. The Theory

We start with some easy theorems that restrict the possible strings after the first few moves. Any chunk of a string that has lasted at least n moves will be called an *n-day-old* string.

The One-Day Theorem. Chunks of types

$$,a\ x,\ \ b\ x,\ \ x^{4 \text{ or more}} \text{ and } x^3\ y^3$$

don't happen in day-old strings. (Note that the first one has a given parsing.)

Proof. The first possibility comes from $x^a x^b$, which, however, should have been written x^{a+b}, in the previous day's string. The other two, whichever way they are parsed, imply cases of the first.

The Two-Day Theorem. No digit 4 or more can be born on or after the second day. Also, a chunk 3×3 (in particular 3^3) can't appear in any 2-day-old list.

Proof. The first possibility comes from a chunk x^4 or more, while the second, which we now know must parse $,3x,3y,$ can only come from a chunk x^3y^3 , of the previous day's string.

When tracking particular strings later, we'll use these facts without explicit mention.

The Starting Theorem. Let R be any chunk of a 2-day-old string, considered as a string in its own right. Then the starts of its descendants ultimately cycle in one of the ways

$$[\ ] \quad \text{or} \quad [1^1X^1 \to [1^3 \to [3^1X^{\neq 3}$$

$$\text{or} \quad [2^2] \quad \text{or} \quad [2^21^1X^1 \to [2^21^3 \to [2^23^1X^{\neq 3}$$

If R is not already in such a cycle, at least three distinct digits appear as initial digits of its descendants.

Proof. If R is nonempty and doesn't start with 2^2, then it *either* starts with a 1 and is of one of the types

$$[1^1X^{0\text{ or }1} \quad\text{or}\quad [1^1(2^{2\text{ or }3}\text{ or }3^2) \quad\text{or}\quad [1^2X^{1\text{ or }\neq 1} \quad\text{or}\quad [1^3$$

or starts with a 2 and is of one of the types $[2^1X^{2\text{ or }\neq 2}$ or $[2^3$
or starts with a 3 and is of one of the types $[3^1X^{3\text{ or }\neq 3}$ or $[3^2X^{3\text{ or }\neq 3}$
or starts with some $n > 3$ and has form $[n^1$.

It is therefore visible in

$$\begin{tikzcd}[column sep=small]
 & {[1^12^3} \arrow[dr] & {[3^2X^3} \arrow[dr] & & {[1^1]} \arrow[dr] & {[3^2X^{\neq 3}} \arrow[dr] & {[n^1} \arrow[dr] & & {[2^3} \arrow[dr] & \\
{[3^1X^3} \arrow[r] & {[1^13^2} \arrow[r] & {[1^2X^1} \arrow[r] & {[2^1X^2} \arrow[r] & {[1^12^2} \arrow[r] & {[1^2X^{\neq 1}} \arrow[r] & {[2^1\,X^{\neq 2}} \arrow[r] & {[1^1X^1} \arrow[r] & {[1^3} \arrow[r] & {[3^1X^{\neq 3}} \arrow[ll, bend left]
\end{tikzcd}$$

which establishes the desired results for it.

This proves the theorem except for strings of type $[2^2R'$ all of whose descendants start with 2^2. This happens only if no descendant of R' starts with a 2, and so we can complete the proof by applying the results we've just found to R'.

The Splitting Theorem. A 2-day-old string LR splits as $L.R$ just if one of L and R is empty or L and R are of the types shown in one of

L	R
$n]$	$[m$
$2]$	$[1^1X^1$ *or* $[1^3$ *or* $[3^1X^{\neq 3}$ *or* $[n^1$
$\neq 2]$	$[2^21^1X^1$ *or* $[2^21^3$ *or* $[2^23^1X^{\neq 3}$ *or* $[2^2n^{(0\text{ or }1)}$
	$(n \geq 4\ ,\ \ m \leq 3)$

Proof. This follows immediately from the Starting Theorem applied to R and the obvious fact that the last digit of L is constant.

Now we investigate the evolution of the end of the string!

The Ending Theorem. The end of a string ultimately cycles in one of the ways:

$$\begin{tikzcd}
2.311322113212221] \arrow[r] & 2.13211322211312113211] \arrow[d] \\
2.12322211331222113112211] \arrow[u] & 2.1113122113322113111221131221] \arrow[l]
\end{tikzcd}$$

$$\begin{tikzcd}
2.31221132221222112112322211n] \arrow[d, shift left] \\
2.1311222113321132211221121332211n] \arrow[u, shift left]
\end{tikzcd} \qquad (n > 1)$$

$$\text{or} \qquad \begin{tikzcd} 2^2\,] \arrow[loop above] \end{tikzcd}$$

(Note: our splitting theorem shows that these strings actually do split at the dots, although we don't use this.)

Proof. A string with last digit 1 must end in one of the ways visible in

$$1^{\geq 3}\,] \to (\neq 2)^X\, 1^1\,] \to (\neq 2)^X\, 1^2\,] \to 2^{X \neq 2}\, 1^1\,] \to$$

$$2^{X \neq 2}\, 1^2\,] \to 2^2\, 1^1\,] \to 2^2\, 1^2\,] \to 2^3\, 1^1\,]$$

and its subsequent evolution is followed on the right-hand side of Figure 1.

A string with last digit $n > 1$ must end $n^n]$ or $n^{\neq n}]$ and so evolves via

$$\begin{tikzcd} n^n] \arrow[loop above, "(n = 2)"] \arrow[r, "(n \neq 2)"] & n^{\neq n}\,] \end{tikzcd} \to n^1] \to 1n] \to 11n] \to (\neq 1)11n] \to 211n] \to 2211n]$$

and the last string here is the first or second on the left of Figure 1.

(≠2)2211*n*] (*n* > 1)	(≠2)2221]	
(≠2)22211*n*]	3211]	
32211*n*]	31221]	
322211*n*]	3112211]	
(≠3)332211*n*]	3212221]	
2322211*n*]	312113211]	
21332211*n*]	3111221131221]	
2112322211*n*]	(≠3)331222113112211]	
221121332211*n*]	2.311322113212221]	(*period* 4)
22112112322211*n*]	2.132113222113121113211]	
2211221121332211*n*]	2.111312211332211311112211131221]	
221222112112322211*n*]	2.311311222.123222113312221131122111]	
2113221122112133221I*n*]	2.1112133.22.12.311322113212221]	
22113222122211211232221I*n*]		
2211332113221122112133221I*n*]		
22.12.31221132221222112112322211*n*]		
2.1311222113321132211221121332211*n*]		(*period* 2)
2.11132.13.22.12.31221132221222112112322211*n*]		

Figure 1. The evolution of endings other than 2^2].

This figure proves the theorem except for the trivial case 2^2]. (When any of these strings contains a dot, its subsequent development is only followed from the digit just prior to the rightmost dot.)

We are now ready for our first major result.

The Chemical Theorem.

(a) The descendants of any of the 92 elements in our Periodic Table are compounds of those elements.

(b) All sufficiently late descendants of any of these elements other than Hydrogen involve all 92 elements simultaneously.

(c) The descendants of any string other than [ ] or [22] also ultimately involve all 92 elements simultaneously.

(d) These 92 elements are precisely the common elements as defined in the introduction.

Proof.

(a) follows instantly from the form in which we have presented the Periodic Table.

(b) It also follows that if the element E_n of atomic number n appears at some time t, then for any $m < n$, all elements on the E_m line of the table will appear at the later time $t + n - m$. In particular,

$$E_n \text{ at } t \to \text{Hf \& Li at } t + n - 1 \quad (\text{if } n \geq 2)\,,$$

$$\text{Hf \& Li at } t \to \text{Hf \& Li at } t + 2 \text{ and } t + 71\,,$$

$$\text{Hf at } t \to \text{Sr \& U at } t + 72 - 38\,,$$

$$\text{U at } t \to E_n \text{ at } t + 92 - n\,.$$

From these we successively deduce that if any of these 92 elements other than Hydrogen is involved at some time t_0, Hafnium and Lithium will simultaneously be involved at some strictly later time $\leq t_0 + 100$, and then both will exist at all times $\geq t_0 + 200$, Uranium at all times $\geq t_0 + 300$, and every other one of these 92 elements at all times $\geq t_0 + 400$.

In other words, once you can fool some of the elements into appearing some of the time, then soon you'll fool some of them all of the time, and ultimately you'll be fooling all of the elements all of the time!

(c) If L is not of form $L'2^2$], this now follows from the observation that Calcium (digit-string 12) is a descendant of L, since it appears in both the bottom lines of Figure 1. Otherwise we can replace L by L', which does not end in a 2.

(d) follows from (a), (b), (c) and the definition of the common elements.

Now we'll call an arbitrary string *common* just if it is a compound of common atoms.

The Arithmetical Theorem.

(a) The lengths of all common strings other than boring old [ ] and [22] increase exponentially at the same rate $\lambda > 1$.

(b) The relative abundances of the elements in such strings tend to certain fixed values, all strictly positive.

Notes. Since each common element has at least 1 and at most 42 digits we can afford to measure the lengths by either digits or atoms: we prefer to use atoms. The numerical value of λ is 1.30357726903; the abundances are tabulated in the Periodic Table.

Proof. Let $\mathbf{v}$ be the 92-component vector whose (i)-entry is the number of atoms of atomic number i in some such string. Then at each derivation step, $\mathbf{v}$ is multiplied by the matrix $\mathbf{M}$ whose (i, j)-entry is the number of times E_j is involved in the derivate of E_i . Now our Chemical Theorem shows that some power of $\mathbf{M}$ has strictly positive (i, j)-entries for all $i \neq 1$ (the $(1, j)$-entry will be 0 for $j \neq 1$, 1 for $j = 1$, since every descendant of a single atom of Hydrogen is another such).

Let λ be an eigenvalue of $\mathbf{M}$ with the largest possible modulus, and $\mathbf{v}_0$ a corresponding eigenvector. Then the nonzero entries of $\mathbf{v}_0\,\mathbf{M}^n$ are proportional to λ^n, while the entries in the successive images of all other vectors grow at most this rate. Since the 92 coordinate vectors (which we'll call **H**, **He** , . . . , **U** in the obvious way) span the space, at least one of them must increase at rate λ

On the other hand, our Chemical Theorem shows that the descendants of each of **He**, **Li**, . . . , **U** increase as fast as any of them, and that this is at some rate > 1 , while **H** is a fixed vector (rate 1). These remarks establish our Theorem.

(We have essentially proved the Frobenius-Perron Theorem, that the dominant eigenvalue of a matrix with positive entries is positive and occurs just once, but I didn't want to frighten you with those long names.)

The Transuranic Elements.

For each number $n \geq 4$, we define two particular atoms:

an isotope of *Plutonium* (Pu) : $31221132221222112112322211n$

an isotope of *Neptunium* (Np): $1311222113321132211221121332211n$

For $n = 2$, these would be Lithium (Li) and Helium (He); for $n = 3$, they would be Tungsten (W) and Tantalum (Ta), while for $n \geq 4$ they are called the transuranic elements. We won't bother to specify the number n in our notation.

We can enlarge our 92-dimensional vector space by adding any number of new pairs of coordinate vectors **Pu**, **Np** corresponding to pairs of transuranic elements.

Our proof of the Ending Theorem shows that every digit 4 or more ultimately lands up as the last digit in one of the appropriate pair of transuranic elements, and (see the bottom left of Figure 1) that we have the decomposition

$$Pu \rightarrow Np \rightarrow Hf.Pa.H.Ca.Pu.$$

Now $\mathbf{Pu} \pm \mathbf{Np}$ is an eigenvector of eigenvalue ± 1 *modulo the subspace corresponding to the common elements,* since $\mathbf{Pu} \rightarrow\leftarrow \mathbf{Np}$ modulo that space. Because these eigenvalues are strictly less than λ in modulus, the relative abundances of the transuranic elements tend to 0.

So far, I can proudly say that this magnificent theory is essentially all my own work. However, the next theorem, the finest achievement so far in Audioactive Chemistry, is the result of the combined labors of three brilliant investigators.

The Cosmological Theorem.

Any string decays into a compound of common and transuranic elements after a bounded number of derivation steps. As a consequence, *every* string other than the two boring ones increases at the magic rate λ, and the relative abundances of the atoms in its descendants approach the values we have already described.

Proof of the Cosmological Theorem would fill the rest of this book! Richard Parker and I found a proof over a period of about a month of very intensive work (or, rather, play!). We first produced a very subtle and complicated argument, which (almost) reduced the problem to tracking a few hundred cases, and then handled these on dozens of sheets of paper (now lost). Mike Guy found a simpler proof that used tracking and back-tracking in roughly equal proportions. Guy's proof still filled lots of pages (almost all lost) but had the advantage that it found the longest-lived of the exotic elements, namely, the isotopes of *Methuselum* (2233322211n ; see Figure 2). Can you find a proof in only a few pages? Please!

2233322211n ($n > 1$)
223332211n
223322211n
222332211n
322322211n
13221332211n
111322112322211n
3113222112133221 1n
1321133221121123222 11n
La.H.123222112211213322 11n
1112133221222112112322211n
Sr.3221132211221121332211n
132221132221222112112322211n
111332211332113221122112133221 1n
3123222.Ca.(Li or W or Pu)
1311121332
11133112112.Zn
Zn.321122112
131221222112
1113112211322112
3113212221132221 12
1321131211322113322112
1113122113111221 1322.Na
3113112221133122211332
Ho.Pa.H.Ca.Ac.H.Ca.Zn

Figure 2. The descendants of Methuselum.

The Degree of λ .

Plainly, λ is an algebraic number of degree at most 92. We first reduce this bound to 71 by exhibiting a 21-dimensional invariant subspace on which the eigenvalues of $\mathbf{M}$ are 0 or ± 1.

$$\mathbf{v}_1 = \mathbf{H},\ \mathbf{v}_2 = \mathbf{He} - \mathbf{Ta},\ \mathbf{v}_3 = \mathbf{Li} - \mathbf{W},\ \ldots,\ \mathbf{v}_{20} = \mathbf{Ca} - \mathbf{Pa}\ ,$$

or, in atomic number notation,

$$\mathbf{v}_1 = \mathbf{E}_1,\ \mathbf{v}_2 = \mathbf{E}_2 - \mathbf{E}_{73},\ \ \mathbf{v}_3 = \mathbf{E}_3 - \mathbf{E}_{74},\ \ldots,\ \mathbf{v}_{20} = \mathbf{E}_{20} - \mathbf{E}_{91}\ ,$$

and also define

$$\mathbf{v}_{21} = \{\ \mathbf{Sc} + \mathbf{Sm} - \mathbf{H} - \mathbf{Ni} - \mathbf{Er} - 3\mathbf{U}\ \}/2\ ,$$

then observe that

$$\mathbf{v}_{21} \to \mathbf{v}_{20} \to \mathbf{v}_{19} \to \ \cdots\ \to \mathbf{v}_4 \to \mathbf{v}_3 \to \mathbf{v}_2,\ \mathbf{v}_1 \to \mathbf{v}_1\ .$$

An alternate base for this space consists of the eigenvectors

$$\mathbf{v}_1 \text{ and } \mathbf{v}_3 \pm \mathbf{v}_2$$

of $\mathbf{M}$ with the respective eigenvalues

$$1 \text{ and } \pm 1\ ,$$

together with the following Jordan block of size 18 for the eigenvalue 0

$$\mathbf{v}_{21} - \mathbf{v}_{19} \to \mathbf{v}_{20} - \mathbf{v}_{18} \to \mathbf{v}_5 - \mathbf{v}_3 \to \mathbf{v}_4 - \mathbf{v}_2 \to 0.$$

(This shows that $\mathbf{M}$ is one of those "infinitely rare" matrices that cannot be diagonalized. Don't expect to follow these remarks unless you've understood more of linear algebra than I fear most of your colleagues have!)

Richard Parker and I have recently proved that the residual 71st degree equation for λ is irreducible, even when it is read modulo 5. We use the fact that the numbers in a finite field of order q all satisfy $x^q = x$ (since the nonzero ones form a group of order $q - 1$, and so satisfy $x^{q-1} = 1$) .

Working always modulo 5, we used a computer to evaluate the sequence of matrices.

$$\mathbf{M}_0 = \mathbf{M},\ \mathbf{M}_1 = \mathbf{M}_0^5,\ \mathbf{M}_2 = \mathbf{M}_1^5,\ \mathbf{M}_3 = \mathbf{M}_2^5,\ \ldots,\ \mathbf{M}_{73} = \mathbf{M}_{72}^5,$$

and to verify that the nullity (modulo 5) of $\mathbf{M}_{n+2} - \mathbf{M}_2$ was 21 for $1 \le n \le 70$, but 92 for $n = 71$. Note that the 21 vectors of the above "alternate base" are *eigenvectors* of $\mathbf{M}_2$ whose eigenvalues (modulo 5) lie in the field of order 5.

If the 71st degree equation were reducible modulo 5, then $\mathbf{M}_2$ would have an eigenvector linearly independent of these with eigenvalue lying in some extension field of order $q = 5^n$ $(1 \le n \le 70)$. But then the eigenvalues ϕ of these 22 eigenvectors would all satify $\phi^q = \phi$, and the 22 eigenvectors would be nullvectors for

$$(\mathbf{M}_2)^q - \mathbf{M}_2 = \mathbf{M}_{n+2} - \mathbf{M}_2,$$

contradicting our computer calculations.

It is rather nice that we were able to do this without being able to write down the polynomial. However, Professor Oliver Atkin of Chicago has since kindly calculated the polynomial explicitly and has also evaluated its largest root λ as

$$1.3035772690342963912570991121525498$$

approximately. The polynomial is

$$x^{71} - x^{69} - 2x^{68} - x^{67} + 2x^{66} + 2x^{65} + x^{64} - x^{63} - x^{62} - x^{61}$$

$$- x^{60} - x^{59} + 2x^{58} + 5x^{57} + 3x^{56} - 2x^{55} - 10x^{54} - 3x^{53} - 2x^{52} + 6x^{51}$$

$$+ 6x^{50} + x^{49} + 9x^{48} - 3x^{47} - 7x^{46} - 8x^{45} - 8x^{44} + 10x^{43} + 6x^{42} + 8x^{41}$$

$$- 5x^{40} - 12x^{39} + 7x^{38} - 7x^{37} + 7x^{36} - x^{35} - 3x^{34} + 10x^{33} + x^{32} - 6x^{31}$$

$$- 2x^{30} - 10x^{29} - 3x^{28} + 2x^{27} + 9x^{26} - 3x^{25} + 14x^{24} - 8x^{23} - 7x^{21}$$

$$+ 9x^{20} + 3x^{19} - 4x^{18} - 10x^{17} - 7x^{16} + 12x^{15} + 7x^{14} + 2x^{13} - 12x^{12} - 4x^{11}$$

$$- 2x^{10} + 5x^{9} + x^{7} - 7x^{6} + 7x^{5} - 4x^{4} + 12x^{3} - 6x^{2} + 3x - 6$$

CHAPTER VI.
SOLUTIONS TO SIX OF THE PROBLEMS

Here we have some results. The idea at the conference was to present problems the first day, solve them the second day, and present the solutions on the third day. Good luck! Although the authors did not have their egos tied up in giving hard problems, it is still clear that open problems take more than a half a day or so to solve. Only one problem was actually solved at the conference. That was El Gamal's problem solved by Gallager -- an interesting new problem and a very nice solution.

Boyd and Hajela have contributed to Wyner's problem. The Gambler's Ruin on the Simplex by T. Cover was solved by Bruce Hajek for three dimensions. The solution does not seem to generalize but we are very happy with the techniques anyway. Finally, the ergodic process selection problem of T. Cover was successfully handled by Bruce Hajek under moment constraints. Cover still believes that the conjecture is generally true, but at this time we do not know whether the moment constraints can be removed.

So here we have it. Some of the problems of this book can actually be solved. It is conceivable that some people might use the problems in this book as a source of research inquiries. For that reason, the editors will act as a clearing house on papers published on the subject of this book, so potential researchers can inquire about the status of these problems.

Contents

6.1 ON THE SPECTRAL DENSITY OF SOME STOCHASTIC PROCESSES

S. Boyd

Department of Electrical Engineering
Stanford University
Stanford, CA 94305

D.J. Hajela

Bell Communications Research
Morristown, NJ 07960

1. Introduction.

We prove the following theorem, which was motivated by a question that Wyner raised in [1].

Theorem: Given any $\varepsilon > 0$ and $A > 0$, there is a complex stationary stochastic process $x(t, w)$ which satisfies:

(i) $|x(t, w)| \le A$ a.s.

(ii) $\| S_x(f) - B_A(f) \|_1 \le \varepsilon$,

where $S_x(f) = \int e^{-2\pi i f \tau} E\, x(t)\, \overline{x(t + \tau)}\, d\tau$ is the spectral density of x and

$$B_A(f) = \begin{cases} A^2/2 & |f| \le 1 \\ 0 & |f| > 1 \end{cases}$$

is the boxcar spectral density with bandwidth 1 and total power A^2.

In fact, we have (ii) from the following stronger set of conclusions:

(iii) $S_x(f) \ge 0$ and S_x is even.

(iv) $\int_1^\infty S_x(f)\, df < \varepsilon$ and $\left| \int_{-1}^{1} S_x(f) - A^2 \right| < \varepsilon$.

(v) $\left| \max_{|f| \le 1} S_x(f) - A^2/2 \right| < \varepsilon$.

Thus x is a process with nearly boxcar spectrum which is not only power limited to A^2 but is amplitude limited to A (a stricter constraint). Moreover, the process we construct is *ergodic*. Aaron Wyner has pointed out to us that there are quite simple constructions of processes satisfying (i) and (ii) above, but they are not ergodic. The construction of our process is more delicate and thus the verification of the properties of the process is at least as interesting as the properties themselves.

We also have the following corollary whose proof is immediate:

Corollary: The process x above satisfies:

$$\int_{-1}^{1} \log\,(1 + S_x\,(f))\; df \geq 2\,\log(1 + \frac{A^2}{2}) - \varepsilon$$

$$= \int_{-1}^{1} \log\,(1 + B_A(f))\; df - \varepsilon\,.$$

2. Proof of the Theorem.

We now prove the theorem.

Proof. In [2], p. 321, J.P. Kahane demonstrates that there are polynomials,

$$P_n(z) = \sum_{m=1}^{n} a_{mn}\, z^n, \quad |\, a_{mn} \,| = 1\;,$$

and $\varepsilon_n \to 0$ such that

$$\|\, P_n(e^{i\theta}) \,\|_\infty \leq (1 + \varepsilon_n)\, \sqrt{n}\;.$$

In fact, he even proves a stronger result, but we shall not need this. Let

$$u_n(t) = \frac{A}{\sqrt{2N+1}}\; e^{-2\pi\, i\, t/N}\, P_{2N+1}\,(e^{2\pi\, i\, t/N}\,)\;.$$

u_n is a N periodic signal with power A^2 and peak

$$\|\, u_n \,\|_\infty \leq (1 + \varepsilon_n)\, A\;.$$

Let

$$U_N(t, \omega) = u_N(t + \theta(\omega)) ,$$

where $\theta(\omega)$ is uniformly distributed on $[0, N]$. U_N is a complex stationary stochastic process such that

$$\| U_N \|_\infty \le (1 + \varepsilon_N) A \ \text{ a.s.}$$

and with spectral measure

$$S_{U_N}(f) = \frac{A^2}{2N+1} \sum_{|n| \le N} \delta(f - \frac{n}{N}).$$

These spectral measures approximate the boxcar spectrum in distribution but we want a stronger approximation of the densities.

To do this, we modulate the process U_N as follows: Let $Z_{N,\alpha}$ be random telegraph process with rate $\alpha/2\pi N$, independent of U_N, where $\alpha > 1$. Then,

$$| Z_{N,\alpha} | = 1 \ \text{ a.s.}$$

and

$$S_{Z_{N,\alpha}}(f) = \frac{\alpha\, \pi^{-1} N}{\alpha^2 + (Nf)^2}.$$

Let

$$X_{N,\alpha} = \frac{Z_{N,\alpha} U_N}{1 + \varepsilon_N}.$$

Then

$$| X_{N,\alpha} | \le A \ \text{a.s}$$

and

$$S_{X_{N,\alpha}} = \frac{1}{(1+\varepsilon_N)^2} \frac{2N}{2N+1} \frac{A^2}{2\pi} \sum_{|n| \le N} \frac{\alpha}{\alpha^2 + (Nf + n)^2} .$$

The theorem now follows at once from the lemmas below by choosing N and α large enough. (See Lemma F in particular.) □

Lemma A: For fixed $\alpha > 1$,

$$\overline{\lim_{N\to\infty}} \parallel S_{X_{N,\alpha}} - B_A \parallel_1 \le 4 \overline{\lim_{N\to\infty}} \max_{f\in[-1,1]} \left| \mid S_{X_{N,\alpha}} \mid - \frac{A^2}{2} \right|$$

Proof. Note that $S_{X_{N,\alpha}}(f)$ is an even function. We show first that

$$\int_1^\infty S_{X_{N,\alpha}}(f)\, df \to 0 .$$

Now

$$\int_1^\infty \frac{\alpha}{\alpha^2 + (Nf-n)^2}\, df = \frac{1}{N}\left[\frac{\pi}{2} - \tan^{-1}\left[N - \frac{n}{\alpha}\right]\right]$$

and so

$$\int_1^\infty \sum_{|n|\le N} \frac{\alpha}{\alpha^2 + (Nf-n)^2}\, df = \frac{2}{2N}\sum_{n=0}^{2N}\left[\frac{\pi}{2} - \tan^{-1}\left(\frac{n}{\alpha}\right)\right] \to 0$$

by Cesaro convergence. Therefore,

$$\int_1^\infty S_{X_{N,\alpha}}(f) df \to 0 .$$

Similarly, since $S_{X_{N,\alpha}}(f)$ is even,

$$\int_{-\infty}^{-1} S_{X_{N,\alpha}}(f) df \to 0 .$$

Also, by a similar calculation,

$$\int_{-\infty}^{\infty} S_{X_{N,\alpha}}(f)\, df = \frac{1}{(1+\varepsilon_N)^2} A^2 .$$

Now

$$\parallel S_{X_{N,\alpha}} - B_A \parallel_1 = \int_{-1}^{1} \left| S_{X_{N,\alpha}} - \frac{A^2}{2} \right| df + \int_1^\infty S_{X_{N,\alpha}}(f) df + \int_{-\infty}^{-1} S_{X_{N,\alpha}}(f) df$$

and so

$$\overline{\lim} \parallel S_{X_{N,\alpha}} - B_A \parallel_1 \le \overline{\lim} \int_{-1}^{1} \left| S_{X_{N,\alpha}} - \frac{A^2}{2} \right| df .$$

Now

$$\int_{-1}^{1} \left| S_{X_{N,\alpha}} - \frac{A^2}{2} \right| df = \int_{[S_{X_{N,\alpha}} \geq \frac{A^2}{2}] \cap [-1,1]} (S_{X_{N,\alpha}} - \frac{A^2}{2}) df + \int_{[S_{X_{N,\alpha}} \leq \frac{A^2}{2}] \cap [-1,1]} (\frac{A^2}{2} - S_{X_{N,\alpha}})\, df$$

$$\int_{S_{X_{N,\alpha}} \geq \frac{A^2}{2}} S_{X_{N,\alpha}} - \frac{A^2}{2}\, df \leq \left| \| S_{X_{N,\alpha}} \|_\infty - \frac{A^2}{2} \right| \lambda \left[f \,\middle|\, |f| \leq 1,\, S_{X_{N,\alpha}} \geq \frac{A^2}{2} \right]$$

$$\leq 2 \left| \| S_{X_{N,\alpha}} \|_\infty - \frac{A^2}{2} \right| ,$$

where $\| S_{X_{N,\alpha}} \|_\infty = \max_{f \in [-1,1]} | S_{X_{N,\alpha}} |$. Moreover,

$$\int_{[S_{X_{N,\alpha}} \leq \frac{A^2}{2}] \cap [-1,1]} \left[\frac{A^2}{2} - S_{X_{N,\alpha}} \right] df = A^2 - \int_{-1}^{1} S_{X_{N,\alpha}}\, df + \int_{S_{X_{N,\alpha}} > \frac{A^2}{2}} \left[S_{X_{N,\alpha}} - \frac{A^2}{2} \right] df .$$

Therefore, $\overline{\lim}\, \| S_{X_{N,\alpha}} - B_N \|_1 \leq 4\, \overline{\lim} \left| \| S_{X_{N,\alpha}} \|_\infty - \frac{A^2}{2} \right|$. □

Lemma B: Let $f(x) = \sum_{|n| \leq N} \frac{\alpha}{\alpha^2 + (x-n)^2}$. Then $\max_{x \in [-N,N]} f(x) = \max_{x \in [-1,1]} f(x)$.

Proof. Since $f(x)$ is even, it suffices to show $\max_{x \in [0,N]} f(x) = \max_{x \in [0,1]} f(x)$. Fix $y \in [0,1]$ and let $s_k = f(y + k)$ for $k = 0, 1, \ldots, N-1$. We show $s_0 \geq s_1 \geq s_2 \geq \cdots \geq s_{N-1}$. This clearly suffices to finish the proof. Now

$$s_k - s_{k+1} = \sum_{j=k-N}^{k+N} \frac{\alpha}{\alpha + (y+j)^2} - \sum_{j=k+1}^{k+1+N} \frac{\alpha}{\alpha^2 + (y+j)^2}$$

$$= \frac{\alpha}{\alpha^2 + (y + k - N)^2} - \frac{\alpha}{\alpha^2 + (y + k + 1 + N)^2} \geq 0 . \quad \square$$

Lemma C: Let C_N be a square with vertices at $(N+\frac{1}{2})(1+i)$, $(N+\frac{1}{2})(-1+i)$, $(N+\frac{1}{2})(-1-i)$, and $(N+\frac{1}{2})(1-i)$. Let $g(z)$ be a function with poles at $z = p_1, \ldots, p_k$ (and assume N is large enough so the C_N contains all these poles within its interior). Suppose that $|g(z)| = O\left[\frac{1}{|z|^2}\right]$ on C_N. Then

$$\sum_{n=-N}^{N} g(n) = \left[-\sum_{j=1}^{k} \text{Residue } (\pi \cot \pi z g(z) \text{ at } p_j)\right] + O(\frac{1}{N})$$

This is a standard fact from the theory of residues.

Lemma D: For $a, b, c, d \in \mathbf{R}$ with $a \neq 0$ we have,

$$\sum_{n=-N}^{N} \frac{d}{(an+b)^2 + c^2} = \frac{\pi d}{2i\mu a^2} (\cot w - \cot \overline{w})$$

where $w = \pi(-\lambda i - \mu)$ and $\lambda = \frac{b}{a}$, $\mu = \frac{c}{a}$. Lemma D follows at once from Lemma C after calculating residues and elementary algebra.

Lemma E:

$$\max_{f \in [-1,1]} | S_{X_{N,\alpha}} |$$

$$= \frac{1}{(1+\varepsilon_N)^2} \frac{2N}{2N+1} \frac{A^2}{2} \max_{x \in [0,1]} \frac{\sec^2 \pi x \coth \pi\alpha}{1 + \coth^2 \pi\alpha \tan^2 \pi x} + O(\frac{1}{N}).$$

Proof.

$$\| S_{X_{N,\alpha}} \|_\infty = \max_{f \in [-1,1]} | S_{X_{N,\alpha}} |$$

$$= \max_{f \in [-1,1]} S_{X_{N,\alpha}} \quad \text{(since } S_{X_{N,\alpha}} \text{ is even and positive)}$$

$$= \frac{1}{(1+\varepsilon_N)^2} \frac{2N}{2N+1} \frac{A^2}{2\pi} \max_{f \in [0,N]} \sum_{|n| \leq N} \frac{\alpha}{\alpha^2 + (Nf-n)^2}$$

$$= \frac{1}{(1+\varepsilon_N)^2} \, \frac{2N}{2N+1} \, \frac{A^2}{2\pi} \max_{x \in [0,N]} f(x),$$

where $f(x) = \sum_{|n| \le N} \dfrac{\alpha}{\alpha^2 + (x-n)^2}$. By Lemma B, $\max_{x \in [0,N]} f(x) = \max_{x \in [0,1]} f(x)$. Setting $d = \alpha$, $a = 1$, $c = \alpha$, and $b = -x$ in Lemma D gives that

$$f(x) = \frac{\pi}{2i} \left(\cot \pi (x - i\alpha) - \cot \pi (x + i\alpha)\right) + O(\frac{1}{N})$$

$$= \pi(\frac{\sec^2 \pi x \coth \pi\alpha}{1 + \coth^2 \pi\, \alpha \tan^2 \pi x})$$

The result now clearly follows. □

Lemma F: $\overline{\lim\limits_{\alpha\to\infty}} \; \overline{\lim\limits_{N\to\infty}} \; \| S_{X_{N,\alpha}} - B_A \|_1 = 0$.

Proof. For fixed $\alpha > 1$,

$$\| S_{X_{N,\alpha}} - B_A \|_1 \le 4 \; \overline{\lim_{N\to\infty}} \left| \max_{f \in [-1,1]} | S_{X_{N,\alpha}} | - \frac{A^2}{2} \right|$$

by Lemma A. By Lemma E,

$$\overline{\lim_{N\to\infty}} \left| \max_{f \in [-1,1]} | S_{X_{N,\alpha}} | - \frac{A^2}{2} \right| = \frac{A^2}{2} \left| \max_{x \in [0,1]} \frac{\sec^2 \pi x \coth \pi\alpha}{1 + \coth^2 \pi\alpha \tan^2 \pi x} \right|$$

Since $\sec^2 \pi x = 1 + \tan^2 \pi x$ and $\lim\limits_{\alpha\to\infty} \coth \pi\alpha = 1$, we have

$$\overline{\lim_{\alpha\to\infty}} \left| \max_{x \in [0,1]} \frac{\sec^2 \pi x \coth \pi\alpha}{1 + \coth^2 \pi\alpha \tan^2 \pi x} - 1 \right| = 0$$

which completes the proof. □

REFERENCES

[1] A. Wyner, this book, Chapter III, Section 3.7.

[2] J.P. Kahane, ''Sur les Polynomes a Coefficients Unimodulaire,'' *Bull. London Math Soc.,* 12, pp. 321-342 (1980).

6.2 ERGODIC PROCESS SELECTION

Bruce Hajek

Department of Electrical Engineering
University of Illinois
Urbana, IL 61801

The purpose of this note is to give a partial solution to the following problem posed by Thomas M. Cover [1]. Let $(X, Y) = (X_i, Y_i, i \in Z)$ be a jointly ergodic stationary stochastic process. A random process $\delta = (\delta_i, i \in Z)$ is called a selection strategy if $\delta_i \in \{0,1\}$ with probability one for each i, and a selection strategy δ is called sequential if for each $i \geq 1$, δ_i is measurable with respect to

$$\sigma\,(X_{i-1}, Y_{i-1}, X_{i-2}, Y_{i-2}, \ldots, X_1, Y_1),$$

which represents the finite past.

Cover's problem is to prove the conjecture that the limit

$$\lim_{n \to \infty} \frac{1}{n} \sum_{i=1}^{n} (\delta_i X_i + (1-\delta_i) Y_i)$$

is maximized over all sequential selection strategies δ by any sequential selection strategy δ^* which satisfies

$$\delta_i^* = \begin{cases} 1\,, & E[X_i - Y_i | X_{i-1}, Y_{i-1}, \ldots, X_1, Y_1] > 0 \\ 0\,, & < 0 \\ \text{arb.}, & = 0 \end{cases} \tag{1}$$

with probability one for each i. We will prove this conjecture under the assumption that

$$E(\, X_i^2 + Y_i^2 \,) < +\infty \text{ for each } i.$$

We begin by saying that a selection strategy δ' is *weakly* sequential if, for each i, δ_i' is measurable with respect to the infinite past

$$\sigma\,(X_{i-1}, Y_{i-1}, \ldots, X_0, Y_0, \ldots).$$

In the remainder of this note, we use δ to denote an arbitrary sequential selection strategy, and we use Z_i to represent the corresponding reward at state $i : Z_i = \delta_i X_i + (1-\delta_i) Y_i$. Similarly, we let δ' be an arbitrary weakly admissible selection strategy and we let (Z_i') denote the corresponding reward sequence.

We also suppose that δ^* is any sequential strategy satisfying the conjectured optimality conditions (1), and we let δ^{**} be any weakly sequential strategy satisfying the analogous conditions

$$\delta_i^{**} = \begin{cases} 1\,, & E[X_i - Y_i \mid X_{i-1}, Y_{i-1}, \ldots, X_0, Y_0, \ldots\,] > 0 \\ 0\,, & < 0 \\ \text{arb.}, & = 0\,. \end{cases}$$

Finally, we let (Z_i^*) and (Z_i^{**}) denote the reward sequences corresponding to the strategies δ^* and δ^{**}, respectively.

Lemma 1:

$$\liminf_{n \to \infty} \frac{1}{n} \sum_{i=1}^{n} Z_i^* - Z_i \geq 0 \text{ a.s.}$$

$$\liminf_{n \to \infty} \frac{1}{n} \sum_{i=1}^{n} Z_i^{**} - Z_i' \geq 0 \text{ a.s.}$$

Proof. We have $Z_i^* - Z_i = D_i + A_i$, where

$$A_i = E[\, Z_i^* - Z_i \mid X_{i-1}, Y_{i-1}, \ldots, X_1, Y_1\,] \text{ and } D_i = Z_i^* - Z_i - A_i\,.$$

The random variables D_i are pairwise orthogonal and ED_i^2 is bounded independently of i, so by the strong law of large numbers for orthogonal random variables [Doob's 1953 book, p. 158]

$$\lim_{n \to \infty} \frac{1}{n} \sum_{i=1}^{n} D_i = 0 \text{ a.s.}$$

We also have $A_i \geq 0$ a.s. for each i so that

$$\liminf_{n \to \infty} \frac{1}{n} \sum_{i=1}^{n} A_i \geq 0 \text{ a.s.}$$

Combining these facts proves the first assertion of the lemma. The second assertion can be proved in the same way. □

Let δ^K denote a sequential selection strategy such that for i with $i > K$

$$\delta_i^K = \begin{cases} 1\ , & E[\ X_i - Y_i \mid X_{i-1}, Y_{i-1}, \ldots, X_{i-K}, Y_{i-K}\ ] \geq 0 \\ 0\ , & < 0 \end{cases}$$

and let δ^∞ denote the weakly admissible rule defined by

$$\delta_i^\infty = \begin{cases} 1\ , & E[\ X_i - Y_i \mid X_{i-1}, Y_{i-1}, \ldots, X_0, Y_0, \ldots\ ] \geq 0 \\ 0\ , & < 0\ . \end{cases}$$

We let (Z_{Ki}) denote the reward sequence when rule δ^K is used for $1 \leq K \leq \infty$. Since, ignoring a finite interval in the case that K is finite, each δ^K is a stationary rule, the ergodic convergence theorem implies that

$$\frac{1}{n} \sum_{i=1}^{n} Z_{Ki} \underset{n \to \infty}{\to} J_K \text{ in } L^1 \text{ and a.s. senses,}$$

where

$$J_K = E\ \{\ E[X_0 \mid X_{-1}, Y_{-1}, \ldots, X_{-K}, Y_{-K}\ ] \vee$$

$$E\ [\ Y_0 \mid X_{-1}, Y_{-1}, \ldots, X_{-K}, Y_{-K}]\} \quad \text{for} \quad 1 \leq K < \infty$$

and

$$J_\infty = E\{\ E[X_0 \mid X_{-1}, Y_{-1}, \ldots\ ] \ \vee\ E[\ Y_0 \mid X_{-1}, Y_{-1}, \ldots\ ]\ \}$$

where $a \vee b$ denotes the maximum of a and b. By the martingale convergence theorem for uniformly integrable martingales, the conditional expectations in the above expression for J_K converge in L^1 to the corresponding conditional expectations in the above expression for J_∞. Therefore,

$$\lim_{K \to \infty} J_K = J_\infty\ .$$

Since each δ^K is a sequential selection strategy, we conclude from the first assertion of Lemma 1 that

$$\left[\liminf_{n\to\infty} \frac{1}{n} \sum_{i=1}^{n} Z_i^*\right] - J_K \geq 0 \text{ a.s.}$$

On the other hand, taking δ' in Lemma 1 equal to δ^* and δ^{**} in Lemma 1 equal to δ^∞, the second assertion of Lemma 1 implies that

$$J_\infty + \left[\liminf_{n\to\infty} -\frac{1}{n} \sum_{i=1}^{n} Z_i^*\right] \geq 0 \text{ a.s.}$$

Combining these two inequalities, we get that with probability one,

$$J_K \leq \liminf_{n\to\infty} \frac{1}{n} \sum_{i=1}^{n} Z_i^* \leq \limsup_{n\to\infty} \frac{1}{n} \sum_{i=1}^{n} Z_i^* \leq J_\infty.$$

Since J_K converges to J_∞ as K tends to infinity, this yields that

$$\lim_{n\to\infty} \frac{1}{n} \sum_{i=1}^{n} Z_i^* = J_\infty \text{ with probability one.}$$

Once again applying the second part of Lemma 1, we can deduce the following theorem.

Theorem:

$$\limsup_{n\to\infty} \frac{1}{n} \sum_{i=1}^{n} Z_i' \leq J_\infty = \lim_{n\to\infty} \frac{1}{n} \sum_{i=1}^{n} Z_i^* \text{ a.s.}$$

for any sequence (Z_i') arising from a weakly sequential (in particular a sequential) selection strategy.

Remark. By using sharper convergence results and a truncation argument, we believe that our proof extends to cover the case that

$$E[\ |X_i| \log |X_i| + |Y_i| \log |Y_i|\ ] < +\infty.$$

We hesitate to conjecture exactly what happens under the sole assumption that $E[\ |X_i| + |Y_i|\ ] < +\infty$, although we can prove the result if it can be shown that

$$\lim_{n \to \infty} \frac{1}{n} \sum_{i=1}^{n} E[\, X_i \mid X_1, \ldots, X_{i-1} \,]$$

exists and is finite with probability one for any ergodic random process X with $E|X_i|$ finite.

REFERENCE

[1] T. Cover, "Ergodic Process Selection," this book, Chapter V, Section 5.2.

6.3 GAMBLER'S RUIN: A RANDOM WALK ON THE SIMPLEX

Bruce Hajek

Department of Electrical Engineering
University of Illinois
Urbana, IL 61801

The purpose of this note is to give a solution to a problem of Thomas M. Cover (see Chapter V, Section 5.4). Suppose there are three gamblers with respective capital p_a, p_b, and p_c, where $p_a + p_b + p_c = 1$. The players engage in a symmetric three-way game modeled by Brownian motion in the two-dimensional simplex $p_i \geq 0, p_a + p_b + p_c = 1$. When one of the players goes broke, play continues between the remaining two players, where the play is now modeled by a Brownian motion in one dimension, until a second player loses, and the remaining player is declared a winner. Doob's optional sampling theorem implies that player i will be a winner with probability p_i. Cover's problem is to find the probability that the players lose in a specific order. For example, we would like to find the probability that player 3 loses first and then player 2 loses. We provide a "messy" solution.

It is convenient to represent the simplex by the region bounded by an equilateral triangle. For convenience, we choose the triangle to be a subset of the complex plane as shown in Figure 1. Δ is a positive constant determined below and $\alpha = \exp(2\pi i/3)$ is a cube root of unity. A point ω within the triangle at respective distances $3p_a \Delta/2$, $3p_b \Delta/2$, and $3p_c \Delta/2$ from sides bc, ac, and ab of the triangle represents a point (p_a, p_b, p_c) in the game simplex.

The key to solving the problem is to find the hitting distribution on the boundary of the triangle for Brownian motion started at a given point inside the triangle. To solve this problem we conformally map the triangle to a disk. Since the map is conformal, it maps Brownian motion into Brownian motion modulo a random time change, and it thus preserves the hitting distribution. In turn, the hitting distribution for a disk is given explicitly by the classical Poisson kernel.

The mapping $\omega = F(z)$, where

$$F(z) = \int_0^z \frac{dt}{[(t-1)\,(t-\alpha)\,(t-\overline{\alpha}\,)]^{2/3}} = \int_0^z \frac{dt}{[t^3-1]^{2/3}}$$

conformally maps the interior of the unit disk shown in Figure 2 onto the open region bounded by the triangle in Figure 1, with the provisions that a branch of $x^{2/3}$ is chosen so that $(-1)^{2/3} = 1$ and that we set

$$\Delta = F(1).$$

This mapping is a variant of the Schwarz-Christoffel formula [1]. To see that it has the desired property, note that at the singular points 1, α, and $\overline{\alpha}$, the mapping reduces angles by one-third since it locally looks like $z^{1/3}$. Then direct calculations show that

$$\operatorname{Arg}\left[\frac{dF\,(e^{i\theta)}}{d\theta}\right] = \begin{cases} 5\pi/6\,, & 0 < \theta < 2\pi/3 \\ -\pi/2\,, & 2\pi/3 < \theta < 4\pi/3 \\ \pi/6\,, & 4\pi/3 < \theta < 2\pi\,, \end{cases}$$

which shows that arcs $a'b'$, $b'c'$, and $c'a'$ of the unit circle are mapped to the respective sides of the equilateral triangle.

The distribution of where a Brownian motion hits the boundary of the unit disk when the starting point is a point z in the disk is

$$K(\theta, z)d\,\theta/2\pi \quad 0 < \theta < 2\pi\,,$$

where K is the Poisson kernel [2],

$$K(\theta,z) = \frac{1-|z|^2}{|e^{i\theta}-z|^2}.$$

Given that the process starting inside the triangle reaches the boundary at a point u in side ab, the conditional probability that the process will be absorbed at point a is

$$\frac{\alpha - u/\Delta}{\alpha - 1}$$

since this probability is proportional to the distance between u and a.

We thus have that

$$P[\, c \text{ loses first, then } b \text{ loses} \mid \text{start at } \omega_0 \,]$$

is equal to

$$\frac{1}{2\pi} \int_0^{2\pi/3} \frac{\alpha - F(e^{i\theta})/\Delta}{\alpha - 1} K\,(\theta, F^{-1}\,(\omega_0))\, d\theta$$

We do not know if this expression can be simplified, nor do we know how to proceed if there are more than three players.

REFERENCES

[1] Z. Nehari, *Conformal Mapping,* McGraw-Hill, New York, 1952.

[2] J.L. Doob, *Classical Potential Theory and its Probabilistic Counterpart,* Springer-Verlag, New York, 1984.

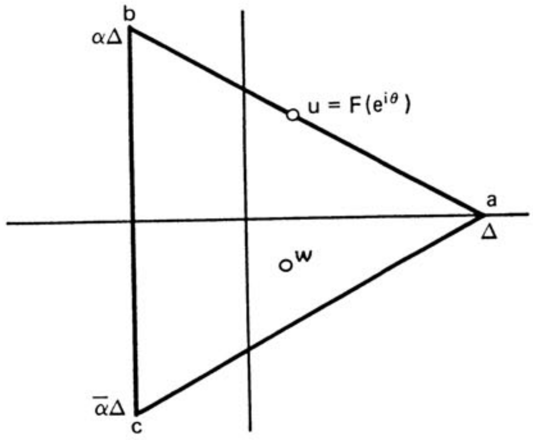


Figure 1. An equilateral triangle in the complex plane.

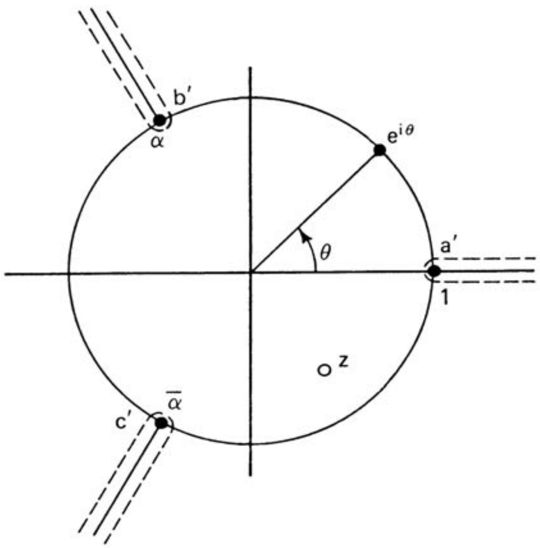


Figure 2. A disk in the complex plane. The dashed lines encircle rays which are not to be integrated over in the definition of $F(z)$.

6.4 FINDING PARITY IN A BROADCAST NETWORK

R.G. Gallager

Department of Electrical Engineering
and Computer Science
M.I.T.
Cambridge, MA 02139

Consider a broadcast network of N nodes in which each binary digit transmitted by each node is received by each other node via a binary symmetric channel whose crossover probability ε is independent over transmitters, receivers, and time. Each note has a binary state and the problem is to construct a distributed algorithm to find the parity of the set of states with some given reliability. This problem was first formulated by A. El Gamal (see Chapter III, Section 3.10) and is of interest because it is one of the simplest distributed algorithm problems involving noise.

The straightforward approach is for each node to send its own state j times for some integer j. A receiving node will make an error in detecting a given node's state with probability ε_j closely upper bounded by α^j, where $\alpha = [\ 4\varepsilon(1-\varepsilon)\ ]^{1/2}$. The probability that a receiving node will make an error in calculating the parity of the states is then proportional to $N\varepsilon_j$ (for $N\varepsilon_j$ small). This means that j must grow as $\log N$.

A more sophisticated approach is to partition the nodes into subsets of k nodes each for some k. Each node again sends its own state j times but then estimates parity of its own set of k nodes and sends this parity. A receiving node will then receive k different estimates for the parity of each subset. A given estimate is incorrect if an odd number of errors occur, first, in the sending node's transmission and, second, in the sending node's estimates of the other states in the subset; the probability of this is $B = [1 - (\ 1 - 2\varepsilon_j\ )^{k-1}\ (\ 1 - 2\varepsilon\ )\ ]\ /2$. Finally, a receiving node will estimate this parity incorrectly if more than half of the k received parity estimates are incorrect, which is upper bounded by $[\ 4B(1-B)\ ]^{k/2}$.

The optimum subset size k for a given ε_j can now be calculated as approximately $1/(4\varepsilon_j)$. The overall parity of the N states can be calculated by a receiving node from the subset parities. With the above value for k and with a constraint P on the overall error probability, it is easy to see that the required number of binary digits required to be transmitted from each node (i.e., $j + 1$) is $(\ln \ln (N/P)) / |\ln \alpha|$ plus a constant which is independent of N and P.

The above constant can be improved slightly by allowing nodes to transmit a limited number of parities of other subsets, but no way is known of improving the log log dependence on N and P.

Essentially the same strategy can be used if each node must reliably determine all the states. We simply generate a larger set of subsets in such a way that each subset contains k nodes, each node is contained in k subsets, and no pair of subsets contains more than one node in common. Each node, as before, sends its own state j times and then sends its estimate of one of the subset parities; remember each subset parity is thus sent once. A receiving node then estimates the state of each node from the j receptions and generates an internal estimate of the parity of each subset. For each subset, the internal parity estimate is compared with the received parity. The node changes the state of a given node from its original estimate if more than half the above comparisons disagree on the subsets containing the given node.

The number of transmissions per node, for this scheme, is again $(\ln \ln (N/P)) / |\ln \alpha|$ plus a constant that is slightly larger than in the case where only parity is calculated.

6.5 AN OPTIMAL STRATEGY FOR A CONFLICT RESOLUTION PROBLEM

V. Anantharam and P. Varaiya

Department of Electrical Engineering
University of California
Berkeley, CA 94720

Relevant to the design of multiple access protocols is the problem of finding the largest of N i.i.d. number $X_1, \ldots, X_N$ uniformly distributed over [0,1] using the minimum number of questions of the following type. We pick a set $A(1) \subset [0,1]$ and ask which $X_i \in A(1)$. Depending on the response, we pick another subset $A(2)$ and ask which $X_i \in A(2)$, and so on, until we identify the largest X_i. It is shown that the optimum sequence of question must be of the type $A(k) = (a(k), 1]$: the best sequence $\{ a(k) \}$ can then be determined by dynamic programming following the work of Arrow, Pesotchinsky, and Sobel. Thus [3] is resolved.

1. Introduction.

In their paper [1], Arrow, Pesotchinsky, and Sobel, considered problem P:

> P: Let $X_1, \ldots, X_N$ be i.i.d. random variables uniformly distributed in [0,1]. The aim is to decide which X_i is the largest with the minimum expected number of *binary* questions, namely, questions to which the response is a simple yes or no. We ask a question, and each X_i responds. Based on the responses we ask the next question, and so on, until the largest X_i is determined.

This problem is relevant to the design of multiple access protocols. Here there are N contenders each of which has a message that it desires to transmit over a single channel. A fair scheme to ensure this is for each contender to be assigned a random priority, for example, according a random number uniformly distributed on [0,1], and give the channel to the leader, that is, the contender with the highest priority. Each contender only knows the number assigned to it. To begin, based on its number, each contender sends a bit to a decision maker. If these bits are not enough to determine the leader, the decision maker requests a second bit, and so on. At any stage the only information available to the decision maker is the set of past responses. To determine the leader as quickly as possible we would like to minimize the expected number of stages the decision maker has to go through. It is clear that any good solution to the problem P in [1] translates directly into a good solution to this multiple access problem. For further discussion of multiple access problems, see [2].

In [1], the optimal strategy (and the minimum expected number of questions) is found within the class of strategies of the following form: Given N, pick a number $a(1) \in [0,1]$ and ask "Whose number is bigger than $a(1)$?". Depending on the responses, pick a number $a(2)$ and ask "Whose number is bigger than $a(2)$?", and so on. Call such questions *right-handed.* A question is right-handed if it is of the type: "Whose number belongs to the set A ?", where A is of the form $(a,1]$, for some $a \in [0,1)$. It is straightforward to set up a dynamic programming recursion to determine the optimal right-handed strategy and this is done in [1].

It is natural to ask whether we can decrease the expected number of questions required when arbitrary binary questions are allowed. For such questions, one picks an arbitrary (measurable) set $A \subset [0,1]$ and asks "Does your number belong to the set A ?". Thus the most general strategy is one that picks a subset $A(1)$ of $[0,1]$ and asks: "Does your number belong to $A(1)$?". Then, based on the responses it picks a subset $A(2)$ and asks "Does your number belong to the set $A(2)$?", and so on, until the leader is found. Can we do any better with such general strategies as compared to the strategies considered in [1]? The fundamental difficulty in answering this question is that there is no obvious way to set up a dynamic programming recursion. Our main result is that the added generality cannot help to reduce the minimum expected number of questions.

2. Theorem.

The best right-handed strategy is also optimal in the class of all strategies.

Proof of the Theorem.

The proof proceeds in two steps. We use the result of [1] that the expected number of questions required to determine the leader using the best right-handed strategy is strictly less than 2.5. We will show first, by induction on the number of contenders, that any strategy entails at least 2 questions on average to determine the leader. Using this, a "bootstrapping" argument shows that any strategy whose first question is not right-handed requires on average more than 2.5 questions to resolve conflict. This suffices to establish the theorem.

Before proceeding, we make a preliminary remark. Since every question is equivalent to its complement, we can assume without loss of generality that a question (more precisely, the corresponding set) contains 1. This will be implicit in the following.

Step 1: We first show that for any strategy K, $\mathbf{E}\,K \geq 2$, where $\mathbf{E}\,K$ denotes the expected number of questions required to resolve conflict under strategy K.

1. Consider the case of two contenders, $N = 2$. Suppose

$$\inf_K \mathbf{E}\,K = \Delta < 2 .$$

If the first question of K is not right handed, the leader cannot be determined immediately, so K requires at least 2 questions on *every* sample path, in particular $\mathbf{E}\,K \geq 2$. (Note: We do not distinguish between sets that differ by zero measure; in particular, A is right-handed if it differs by zero measure from a set of the form $(1\text{-}a,\, 1]$.)

We may therefore assume that K has a right-handed first question, $(1\text{-}a,\, 1]$. If the number of contenders answering yes to this first question is 0 or 2, we are left with a problem identical to the one we started with, and we need at least Δ more questions on average to resolve conflict. If only one of the contenders answers yes to the first question, we are immediately through. Thus

$$\mathbf{E}\,K \geq 2a(1-a) + (1+\Delta)(1-2a)(1-a)\ .$$

Observe that for any $a \in [0,1]$ we have $2a(1-a) \leq 1/2$, so

$$\mathbf{E}\,K \geq 1 + \frac{\Delta}{2}\ .$$

Since this holds for any K, $\Delta \geq 1 + \dfrac{\Delta}{2}$, or $\Delta \geq 2$.

2. Consider now the case of general N . Assume as induction hypothesis that, for any $m < N$, the expected number of questions to resolve conflict for any strategy is at least 2. We will show that for any strategy K with N contenders, the same holds. Suppose, to the contrary that

$$\inf_K \mathbf{E}\,K = \Delta < 2\ .$$

Reasoning as before, we may assume that the first question of K is right-handed and of the form $(1-a,1]$. Three types of responses are possible to this first question.

(a) Each contender, or none of them, responds yes to the question. In this case, we are left with a problem identical to the one we started with and require at least Δ more questions to resolve conflict.

(b) Exactly one contender responds yes to the question. Then we are immediately through. This event has probability $N(1-a)^{N-1}\,a$.

(c) Anywhere from 2 to $N-1$ contenders respond yes to the question. By the induction hypothesis, we then require at least 2 more questions to resolve conflict.

Thus we have

$$\mathbf{E}\,K \geq N(1-a)^{N-1}\,a + (1+\Delta)\,(1 - N\,(1-a)^{N-1}\,a\,)\ ,$$

where for the event (c) we used $\Delta < 2$. Since for $a \in [0,1]$, $N(1 - a)^{N-1} a \leq 1/2$, this gives

$$\mathbf{E}\, K \geq 1 + \frac{\Delta}{2} .$$

This holds for any K, and so $\Delta \geq 1 + \dfrac{\Delta}{2}$, $\Delta \geq 2$.

Step 2: The final step is to use the result above to show that $\mathbf{E}\, K \geq 2.5$ for any strategy K for which the first question, $A \subset [0,1]$, is not right handed. We directly consider the case of general N. Let $A°$ denote the complement of A.

1. Consider the event where either every contender or no contender responds yes to the first question; that is, every X_i is in A or in $A°$. Then we are left with a problem identical to the one we started with restricted to the set A or $A°$, and by Step 1 above, we need at least 2 more questions on average to resolve conflict. Thus, on this event, we need on average at least 3 questions to resolve conflict.
2. Consider the complementary event where the number of contenders reponding yes to the first question is between 1 and $N - 1$. We postulate the following genie:
   - The genie tells us which of the sets A and $A°$ contains the leader.
   - If A contains the leader, the genie tells us the value of the leader among the contenders whose values are in $A°$, and the identities of the contenders whose values are in A and which exceed the leading contender in $A°$.
   - Similarly, if $A°$ contains the leader, the genie tells us the value of the leader among the contenders in A, and the identities of the contenders whose values are in $A°$ and which exceed the leading contender in A.

By postulating a genie, we mean that we permit ourselves to use different strategies on events for which the genie gives us different answers. Clearly, we can do no better without the genie than we can with it.

If A contains the leader, the genie leaves us with the problem of determining the leader among the contenders in A that exceed the leading contender in A°, and these contenders are independently and uniformly distributed on the portion of A which exceeds the leader in A°. Similar remarks apply when the leader is in A°.

Thus, except on the event where the leader is in A and the second best contender is in A° or vice versa, which event we denote Γ, we require, by Step 1 above, at least two more questions on average to determine the leader. On the other hand, if the genie is absent, then we require at least two questions on every sample in Γ. Thus, if we can prove that the measure of Γ is at most 1/2, we will have proved the Theorem. Note: We do not distinguish between sets which differ by zero measure; in particular, a question A is right-handed if A differs by zero measure from a set of the form (a,1].

Let $\mu(X)$ denote the measure of X , for $X \subset [0,1]$. Define two functions F and F° on [0,1] by

$$F(x) = \mu(A \cap (x,1]\,) ,$$

$$F^\circ(x) = \mu(A^\circ \cap (x,1]\,) .$$

Notice that $F(x) + F^\circ(x) = 1 - x$. Next, define functions S and D (mnemonics for same and different, respectively) by

$$S(x) = F(x)1(x \in A) + F^\circ(x)1(x \in A^\circ) ,$$

$$D(x) = F(x)1(x \in A^\circ) + F^\circ(x)1(x \in A) .$$

Then $S(x) + D(x) = 1 - x$. Now

$$\mu(\Gamma) = \sum_{i \neq j} \int_0^1 P\{\, X_k < x \ \text{ for } \ k \neq i, j, X_i \in A^\circ \cap [x, x + dx), X_j \in A \cap (x,1] \,\}$$

$$+ \sum_{i \neq j} \int_0^1 P\{\, X_k < x \ \text{ for } \ k \neq i, j, X_i \in A \cap [x, x + dx), X_j \in A^\circ \cap (x,1] \,\},$$

so that

$$\mu(\Gamma) = \int_0^1 N(N-1)\, x^{N-2}\, D(x)dx.$$

One can now easily check that

$$1 - \mu(\Gamma) = \int_0^1 N(N-1)\, x^{N-2}\, S(x)dx\ .$$

If we define

$$P(x) = \int_x^1 (S(y) - D(y))dy\ ,$$

we can easily prove that $P(x) \geq 0$, for $x \in [0,1]$, and since

$$\int_{x=0}^1 x^{N-2} [\, S(x) - D(x)\,]dx = -\int_{x=0}^1 x^{N-2} \frac{d}{dx} P(x)dx = \int_{x=0}^1 P(x) \frac{d}{dx} x^{N-2} \geq 0\ ,$$

we have shown that $\mu(\Gamma) \leq 1/2$ and the proof is complete.

Acknowledgment: Research supported by Office of Naval Research Contract N 00014-80-C-0507 and Joint Services Electronics Program Contract AFOSR 49620-79-C-0178.

REFERENCES

[1] Kenneth J. Arrow, Leon Pesotchinsky, and Milton Sobel, "On Partitioning of a Sample with Binary Questions in Lieu of Collecting Observations," Technical Report No. 295, Center for Research on Organizational Efficiency, Stanford University, September 1979.

[2] Special Issue on Random-Access Communications, *IEEE Trans. Inf. Theory,* IT-31(2), Mar. 1985.

[3] This book, Chapter V, Section 5.3.

6.6 COORDINATION COMPLEXITY AND THE RANK OF BOOLEAN FUNCTIONS

B. Gopinath and V.K. Wei

Bell Communications Research
Morristown, NJ 07960

The MEX machine is a model for describing the coordination between concurrent processes in a distributive protocol. (See Figure 1.) The discrete recursion operates as follows: Every second is divided into two equal periods. There is a bus connecting all processes, and all information needed for the coordination of the processes is transmitted over the bus. During the first period, a state of the bus is selected. In the second period, each process "resolves" its task by changing its state according the selected bus state. Once the bus state is given, the state transitions at the processes are independent.

The MEX machine is a useful model in protocol specification and validation. The complexity of the MEX machine is the number of bus lines required for the coordination of the processes. It is the logarithm of the number of bus states. Here, we derive the coordination complexity of the MEX machines corresponding to many well-known Boolean functions, including AND, OR, NAND, k-Threshold, and Adder.

Each process is assumed to have only two states. The operation of the MEX machine can be described by a directed graph consisting of 2^n nodes and a number of edges. The nodes correspond to all possible binary n-tuples. There is an edge from node i to node j if and only if "cause" i produces the "effect" j in the MEX machine. For example, for the AND function, there is an edge from node i to node j if and only if the most significant bit of j is equal to the AND of all bits in the binary expansion of i. For the Adder, there is an edge from node i to node j if and only if the numerical value of the first $n/2$ bits is equal to the sum of the numerical values of the first $n/2$ bits of i and the last $n/2$ bits of i .

Some nodes in the directed graph may have out-degree zero; this corresponds to some unacceptable "causes." Some nodes may have out-degree greater than one; this corresponds to don't-care "effects" -- given some particular "causes," one of several possible "effects" is produced with equal consequences.

The graph representation of the composite MEX machine which consists of two smaller MEX machines placed side by side is the tensor product of the two graphs representing the component machines. The new graph has 2^{m+n} nodes, if the two component graphs have 2^m and 2^n nodes, respectively. There is an edge from the composite node (i, i') to (j, j') if and only if there are edges from i to j and from i' to j' in the component graphs.

The *sum* of two graphs with 2^n nodes is a graph with 2^n nodes whose edges are the union of the edges of the summand graphs. The smallest possible graph consists of only two nodes. There are 16 such graphs; they are called *atoms*.

The *rank* of a Boolean function is the logarithm of the minimum number of products of atoms which sum up to its representing graph. It is a measure of the coordination complexity of the MEX machine. It is equal to the minimum number of bus lines required to coordinate the processes. In the first period of a discrete recursion, one of the atom products is selected, and in the second period, each process changes state independently as an atom.

The ranks of several well-known Boolean functions are shown in Table 1. For convenience, the graphs for the Comparator and the Adder are assumed to have 2^{2n} nodes. The ranks of the sum, the product, the tandem, and the overlap of two Boolean functions are also studied.

These results answer several open problems posed by Gopinath in the 1984 SPOC Conference. The proofs of our results are contained in a longer version of the paper.

Table 1. Ranks of Well-Known Boolean Functions

Function	Rank
AND	$\log\,(n+1)$
OR	$\log\,(n+1)$
NAND	$\log\,(n+1)$
NOR	$\log\,(n+1)$
INVERT	0
Counter	$log(n)$
Parity	$log(2^n)$
Sequence Reverser	$log(2^n)$ (n even)
Cyclic Shifter	$log(2^n)$
k-Threshold	$\log \begin{bmatrix} n+1 \\ k \end{bmatrix}$
$n/2$ bi-input AND	$\log\,(3^{n/2})$
Maximum possible rank	$log(4^{n-1})$
Comparator	$\log\,(2^{n+1} - 2)$ ($2n$ inputs)
Adder	$log(3^n)$

LIST OF CONTRIBUTORS

Abu-Mostafa, Yaser S.
California Institute of Technology
M/S 116-81
Pasadena, CA 91125

Ahlswede, R.
Universität Bielefeld
Postach 8640
4800 Bielefeld 1
W. Germany

Anantharam, V.
Cornell University
Phillips Hall
Ithaca, New York 14853

Barron, Andrew R.
Department of Statistics
University of Illinois
Champaign, IL 61820

Boyd, S.
Department of Electrical Engineering
Stanford University
Stanford, CA 94305

Chaitin, Gregory J.
IBM Corporation
P.O. Box 218
Yorktown Heights, NY 10598

Conway, J.H.
Department of Mathematics
Fine Hall
Princeton University
Princeton, NJ 08544

Coppersmith, Don
IBM Corporation
P.O. Box 218
Yorktown Heights, NY 10598

Cover, Thomas M.
Durand Bldg., Rm. 121
Department of Electrical Engineering
Stanford University
Stanford, CA 94305

Csiszár, I.
Mathematical Institute of the
Hungarian Academy of Sciences
Budapest, Realtanoda u. 13-15
H-1053
Hungary

El Gamal, Abbas
Department of Electrical Engineering
Stanford University
Stanford CA 94305

Fredman, Michael L.
Department of Electrical Engineering
and Computer Science
C014
University of California at San Diego
La Jolla, CA 92093

Gacs, Peter
Department of Computer Science
Boston University
Boston, MA 02215

Gallager, R.G.
Department of Electrical Engineering
and Computer Science
M.I.T.
Cambridge, MA 02139

Gilbert, E.N.
AT&T Bell Labs
600 Mountain Avenue
2C-381
Murray Hill, NJ 07974

Gopinath, B.
Bell Communications Research
Rm. 2K-306
435 South Street
Morristown, NJ 07960

Hajek, Bruce
Department of Electrical Engineering
University of Illinois
Urbana, IL 61801

Hajela, D.J.
Bell Communications Research
Room 2P-372
435 South Street
Morristown, NJ 07960

Honig, Michael L.
Bell Communications Research
Room 2L-343
435 South Street
Morristown, NJ 07960

Kelly, F.P.
Department of Electrical Engineering
and Computer Science
Bldg. 35, Rm. 203
M.I.T.
Cambridge, MA 02139

Körner, János
Mathematical Institute of
the Hungarian Academy of Sciences
Budapest, Realtanoda u. 13-15
Hungary

Levin, Leonid A.
Department of Electrical Engineering
and Computer Science
Division of Computer Science
University of California
Berkeley, CA 94720

Odlyzko, A.M.
AT&T Bell Labs
2C-380
600 Mountain Avenue
Murray Hill, NJ 07974

Posner, Edward C.
Department of Electrical Engineering
California Institute of Technology
Pasadena, CA 91125

Shamir, Adi
Weizmann Institute of Sciences
Rehovot, Israel

Shepp, L.A.
AT&T Bell Labs
2C-374
600 Mountain Avenue
Murray Hill, NJ 07974

Sleator, Daniel D.
Dept. of Computer Science
Carnegie-Mellon University
Pittsburgh, PA 15213

Sloane, N.J.A.
AT&T Bell Labs
2C-376
600 Mountain Avenue
Murray Hill, NJ 07974

Tarjan, Robert E.
AT&T Bell Labs
2C-362
600 Mountain Avenue
Murray Hill, NJ 07974

Thurston, William P.
Department of Mathematics
Princeton University
Princeton, NJ 08544

Tsitsiklis, John N.
Laboratory for Information
and Decisions
Room 35-214
M.I.T.
Cambridge, MA 02139

Varaiya, Pravin
Department of Electrical Engineering
University of California
Berkeley, CA 94720

Wei, V.K.
Bell Communications Research
2L-339
435 South Street
Morristown, NJ 07960

Witsenhausen, H.S.
AT&T Bell Labs
2C-361
600 Mountain Avenue
Murray Hill, NJ 07974

Wyner, A.D.
AT&T Bell Labs
2C-361
600 Mountain Avenue
Murray Hill, NJ 07974

Ziv, Jacob
Department of Electrical Engineering
Technion I.I.T.
Haifa 32000 Israel

INDEX