XIV. PROCESSING AND TRANSMISSION OF INFORMATION

Prof. E. Arthurs
Prof. P. Elias
Prof. R. M. Fano
Prof. J. B. Dennis
Prof. S. W. Golomb
Prof. E. M. Hofstetter
Prof. D. A. Huffman
Prof. W. W. Peterson
Prof. W. F. Schreiber
Prof. C. E. Shannon
Prof. W. M. Siebert
Prof. J. M. Wozencraft

Dr. M. Eden
Dr. M. P. Schützenberger
S. Asano
J. Borsuk
D. C. Coll
H. S. Ekre
H. A. Ernst
E. F. Ferretti
R. G. Gallager
T. J. Goblick, Jr.
U. F. Gronemann
F. C. Hennie III
M. Horstein

T. S. Huang
F. Jelinek
T. Kailath
D. H. Pratt
D. L. Reich
B. Reiffen
L. G. Roberts
J. L. Rosenfeld
I. G. Stiglitz
N. K. H. Tam
W. L. Wells
H. P. Zeiger

RESEARCH OBJECTIVES

This group continues its investigations of sources that generate information, channels that transmit it, and machines that process it.

For sources, the main objective is to estimate the rate at which they generate information and to determine how to encode their output economically, in order to decrease the channel capacity required for transmission. Several different procedures for processing pictures in digital form have been reported in the Quarterly Progress Reports of April 15, July 15, and October 15, 1959.

The research on channels continues with more emphasis on results that bear on the application of coding theory to communication systems. Practical coding and decoding systems for use in binary noisy channels have been investigated and reported on in all of the Quarterly Progress Reports during the past year. Two relevant contributions appear in this issue. Rapid progress is being made, and more results in this direction will be reported during 1960.

Two related topics that are still under investigation, from both theoretical and applied points of view, are the use of feedback in communication systems, and the use of sequential decision-making procedures by the receiver in a feedback communication system. There was a report in this field in Quarterly Progress Report No. 53 (pp. 117-121), and there is one in this issue on two-way communication systems. Further work along these lines is in progress.

The availability of a feedback path makes possible the measurement of the characteristics of a time-variant channel, and the modification of the signals used. In long-distance radio circuits the time-variant channel is often linear. Technical Report 352 ("Sampling Models for Linear Time-Variant Filters," by T. Kailath) gives sampling theorems for such channels, and work on their description will go forward.

The research on storage and retrieval of information continues. The design and evaluation of a literature retrieval system was reported in Quarterly Progress Report No. 55 (pp. 130-131).

In the design of coding and decoding devices, finite-state binary logical circuits play a critical role. A binary circuit can be considered as a transducer that transforms an input stream of digits into a related output stream. In the process, information may be lost, and the coded form of the stream changed drastically. Thus a finite-state circuit is a rather general information channel. Recent research has led to a canonical block-diagram form for information-lossless circuits. This canonical representation is valid for any information-preserving transformation whatsoever that is achievable by a finite-state machine. This research was published with the title "Canonical Forms for

*This research was supported in part by Purchase Order DDL-B222 with Lincoln Laboratory, a center for research operated by M.I.T., which is supported by the U.S. Air Force under Air Force Contract AF19(604)-5200.

From an alternative point of view, any finite-state circuit classifies each of the infinitely many possible input sequences of digits into one of the finite number of states. Studies made of minimal descriptions of finite-state circuits and of approximate models thereof are important, in that they show how to describe efficiently the patterns of digits in a sequence. More closely applicable to the pattern-recognition problem is a study of logical circuits whose description is most conveniently given in more than one dimension. For example, the study of circuits whose logical elements can be arranged in a uniform planar array, like that formed by the squares on an indefinitely large chessboard, is particularly pertinent to possible schemes for filtering and logical processing of an ordinary black and white photograph.

A slightly different form of the multidimensional problem involves one-dimensional arrays whose elements possess memory properties. As a first step in the ultimate description of these networks, we must investigate such fundamental properties as stability and equivalence. As we have reported in this issue, there is no hope of finding general methods that would enable us to test for even these basic properties.

E. Arthurs, P. Elias, R. M. Fano, D. A. Huffman

A. NOISY FEEDBACK CODING

Although a feedback channel — even a noiseless one — does not increase the forward capacity of a memoryless channel, the existence of such a channel can still be exploited in the design of two-way communication systems. Examples of noisy two-way systems in use today include the IBM Data Transceiver and the RCA ARQ. Even more closely related to the concepts that we explore briefly in this report is the usual telephone system: Small errors in transmission are automatically corrected by the listener, and gross errors are detected and stimulate a request for retransmission. With exceedingly high probability, error-free information transfer is the result.

We consider a similar model for a two-way discrete system operating over noisy, memoryless, but not necessarily uncorrelated, channels. An endless stream of information digits to be transmitted is assumed to be available in serial storage at each end of the system. Each transmitter can therefore call up new digits whenever it is ready for them, but need not accept them otherwise.

By means of coding $n_1$ information digits together — that is, by transmitting a signal each instantaneous value of which depends upon all $n_1$ digits — we can communicate over the individual noisy one-way links of our two-way pair with an error probability that decreases exponentially with $n_1$. In general, however, the average amount of decoding computation used to correct transmission errors with this exponentially small probability of failure grows with $n_1$. The existence of a fixed computational facility at the receiving terminals will therefore constrain us either with respect to rate of transmission or with respect to probability of error.

This situation can be considerably altered by what may be called "composite" operation. We encode with a constraint length $n_1$, and thereby obtain a theoretical probability
of error $P_1 \propto \exp(-n_1 E)$. The length $n_1$ is chosen to be so great that $P_1$ is truly negligible. At the same time, the decoding computer may be seriously overloaded if it attempts in fact to correct all of the errors that the code is capable of handling. We choose to decode, therefore, with a shorter constraint length, $n_o < n_1$ (and a correspondingly higher probability of error, $P_o \propto \exp(-n_o E)$), where $n_o$ is sufficiently small that the fixed decoder can provide the average computation required. This may be done either by embedding a short block code into a longer one or by constraining a sequential decoder to search only $n_o$ digits back into a convolutional code of length $n_1$.

The more powerful $n_1$ constraint is used only to detect errors, not to correct them. The effect of this is to correct errors with a probability $(1-P_0)$ and to detect any remaining uncorrected errors with probability $(1-P_1)$ ≈ 1.

When uncorrected errors are detected, the computation-limited decoder will not, in general, be able to do more than sound an alarm; we take advantage of the reverse channel to ask automatically for a repeat of the undeciphered transmission. In doing so, however, we must be careful; this reverse channel is itself noisy.

One acceptable strategem is the following. At each end of the system, we divide incoming information digits into successive blocks of length $n_2$, where now $n_2 > n_1 > n_0$. The length $n_0$ is chosen to be sufficiently long that fluctuations in the decoding computational demands are smoothed out. Ideally, the decoding computer should, with a probability of about $(1-n_2 P_o)$, have successfully decoded one block of length $n_2$ by the time the transmitted message corresponding to the next block has been received. The length $n_0$ is chosen so that $n_2 P_o \propto n_2 \exp(-n_0 E) \ll 1$.

The first information digit in each block is usurped as a "service" bit: The receiver at each end causes a "0" to be transmitted back over the reverse channel if the second-preceding received block has been completely decoded; a "1" is transmitted back if an uncorrected error has been detected, or if the decoding has not yet been completed.

The rules of the game are these.

(a) If a receiving terminal sends back a service "0", it proceeds with decoding the next undeciphered block. The transmitter at this terminal likewise proceeds with encoding and transmitting a new block of information digits.

(b) If a receiving terminal sends back a service "1", it disables itself for two blocks, and then proceeds to receive as if four blocks had been elided. The transmitter at this terminal, immediately upon sending back the service "1", proceeds to retransmit from four blocks back.

(c) If a receiving terminal decodes a service "1", it disregards the rest of the block, disables itself for two additional blocks, and then proceeds to receive as if four blocks had been elided. The transmitter at this terminal waits until the end of the block in which the service "1" appeared, and then proceeds to retransmit from four blocks back.

With a little thought, and considerable scribbling, it will be clear that the same
action is taken at a terminal whether it decodes a service "1", detects an undecoded error, or falls behind. Furthermore, both terminals remain in information synchronization. Communication will proceed without mistakes, so long as undetectable transmission error patterns do not occur. Since the probability of undetected errors ($P_1 \propto \exp(-n_1 E)$) can be made arbitrarily close to zero without substantially increasing the complexity of the decoding operation, it seems that both performance and efficiency can be improved. At worst, the complexity cost can be held linear with $n_1$ because data storage proportional to $n_2$ can be handled on paper or magnetic tape.

Further modification of the scheme described above appears to be straightforward. In sequential decoding with convolutional codes, the actual decoding effort required per information digit is a correlated random variable with a small mean but with a large variance. In this case, $n_o$ can be freely variable: The decoder can search farther back towards $n_1$ whenever time permits.

If the decoding computer runs out of time, and a traffic backlog greater than $n_2$ builds up, it requests retransmission. If $n_2$ is large, the usual cause of this, in practice, will be a deterioration of the channel capacity. In these circumstances, it would be wise to automatically couple retransmission with a decrease in the information transmission rate (in bits per transmitted symbol, since the pulse clock rate is fixed). A second information bit could then be usurped to signal for an increase in information rate whenever the receiver consistently finds itself with a near-zero waiting line.

The appealing prospect unfolds of designing communications systems that work effectively without error at whatever maximum efficiency the channel permits, consistent with the complexity built into the decoding computer.

J. M. Wozencraft

B. ENCODING AND ERROR-CORRECTION PROCEDURES FOR THE BOSE-CHAUDHURI CODES

Bose and Chaudhuri (1) have recently discovered a new class of codes with some remarkable properties. For any positive integers $m$ and $t$ there is a code in this class that consists of blocks of length $2^m - 1$, corrects $t$ errors, and requires no more than $mt$ parity check digits. Thus the codes cover a wide range in rate and error-correcting ability, unlike most other known classes of codes. These codes are a generalization of the Hamming codes (2); the case $t = 1$ gives the Hamming code in each case.

A procedure for error correction for these codes has been found. It is a generalization of the simple error-correction procedure that can be used with Hamming codes. The procedure requires a number of operations which increases only as a small power of the length of the codes.

It has also been found that these are cyclic codes (3), and therefore the encoding can
be accomplished very efficiently with a shift-register generator. The theory of the cyclic structure provides, in addition, a closer bound on the number of parity checks required to correct a given number of errors.

A detailed account of these results is being prepared for publication.

W. W. Peterson

References

1. R. C. Bose and D. K. Ray-Chaudhuri, On a class of error-correcting binary group codes (to be published in Information and Control).


C. RECEIVERS FOR NOISY DISPERSIVE CHANNELS

Matrix algebra has been found to be an effective tool in studying optimum detection techniques for channels containing both multiplicative and additive disturbances which are governed by Gaussian statistics. In particular, the work of Price (1), and Turin (2) can be considered as a unit.

Among other results, it has been possible to generate a rather simple proof for, and at the same time to generalize, a result of Price (1). His earlier work states that for a channel consisting of a single scatter path, followed by additive white gaussian noise that is independent of the scatter, the optimum receiver can be interpreted as a bank of optimum estimators of the Wiener type, each estimator being followed by a crosscorrelator. The number of estimator-correlator elements in the bank is equal to the number of possible transmitted waveforms. Each estimator provides the best possible measurement of the instantaneous path fluctuation over the duration of the transmission, if it is assumed that one of the possible waveforms has been transmitted. The associated correlator takes the received signal and crosscorrelates it with the assumed waveform after the waveform has been corrected for the estimated path fluctuations. (An alternative description would be that the receiver crosscorrelates the received signal with optimum estimates of each possible waveform that could have been received had no additive noise been present.) After suitable biases are applied to the correlator outputs, minimum-probability-of-error decision is achieved by selecting the final output of an estimator-correlator pair that is the largest.
It can now be shown that for a channel containing many relatively delayed scatter paths, or, more generally, a time-variant linear network described by Gaussian statistics, and for additive noise that is gaussian but not necessarily white, the optimum receiver operates in essentially the same manner as it does in the simpler channel. That is, optimum estimates are made of the waveforms that could have been received had no additive noise been present, and the received signal is then processed in a set of optimum detectors of the type that would be used for the given additive disturbance had each estimate been perfect. Such optimum processing can be realized by passing the received signal through a (minimum-phase) filter that "whitens" the additive noise portion of the receiver signal, and then crosscorrelating the filter output with the outputs of a bank of separate filters that are identical to the whitening filter and have the estimates as their inputs.

This work, together with some new results on communication through such multipath-scatter channels, will be more fully discussed in a later report. The writer would like to thank Dr. R. Price, of Lincoln Laboratory, M.I.T., for suggestions and helpful discussions.

T. Kailath

References


D. MAXIMAL POWER GAIN IN A DIODELESS MAGNETIC PULSE AMPLIFIER WITH THE USE OF MULTIPLE-APERTURE CORES

Recent improvement in the quality of multiple-aperture cores has enabled me to start a program of research with the following objectives:

(a) To achieve information transfer (diodeless, of course) from one core to another without any deterioration of the "1" level or build-up of the "0" level – that is, with zero information loss.

(b) To improve the resolution and power output of this system so that one core will be able to drive two others, permitting distribution of digital information.

(c) To develop a logical negation element with zero information loss.

All circuits will be reasonably simple and very uncritical in their operation. Note that since a logical "or" function is simply realized by placing more than one input winding on one core, a negation element is all that is needed to achieve logical completeness (that is, to realize any switching function).
At present, objective (a) has been accomplished, and circuits have been improved to allow wide operating margins. Some improvement, I believe, over the system described by Crane (2, 3) has been accomplished. Although objective (b) is only partially accomplished and work on objective (c) is still in the planning stage, experimental results are becoming coherent enough to hint at a possible general description of multiple-hole-core behavior.

The three references given represent the pioneer work in this field, and all have been heavily relied upon.

References


E. UNILATERAL ITERATIVE NETWORKS WITH MEMORY

An iterative switching circuit is one that consists of an indefinite number of identical components, or cells, interconnected in a regular array. The individual cells may be either combinational or sequential switching circuits. Each cell has as its primary input one of the inputs of the entire network; and one of the cell outputs may also be an output for the entire network. Other leads serve to interconnect the cells in the array. Although the size of the array is not restricted, the boundary conditions to which the peripheral cells are subjected must be specified.

The class of iterative networks discussed in this report is illustrated in Fig. XIV-1. These networks are one-dimensional arrays of identical sequential switching circuits whose interconnections are such that information can "flow" only from left to right.

![Fig. XIV-1. Unilateral iterative network with memory.](image-url)
through the chain. That is, the present behavior of any cell is dependent only upon the past behavior of that cell and of those cells to its left. The sequential nature of the cell is indicated by the use of a delay loop around a block containing combinational logic. The internal state of any cell is then represented by the signal that appears in its feedback loop. Any cell's next internal state, primary output, and signal transmitted to its right neighbor are uniquely determined by that cell's present internal state, primary input, and the signal received from its left neighbor. A complete specification of this correspondence between cell input and output values will be referred to as the "cell description." The cell description, boundary conditions, and primary input values completely determine the behavior of the entire chain of cells. For simplicity, the entire operation of the network is assumed to be synchronous; hence, unit delays are shown in the intercell leads. Note that the signal entering the leftmost cell from the left is fixed by the boundary conditions and is the same for all time.

Two problems of fundamental importance in the analysis of an iterative network concern the existence of cyclic behavior and the testing of a pair of networks for equivalence. With the class of networks represented in Fig. XIV-1 we shall restrict ourselves to the following type of operation. Each cell of a chain of finite length is initially placed in the same predesignated internal state. Some arbitrary combination of "0's" and "1's" is applied to the primary inputs; these inputs remain fixed throughout the ensuing computation. The network is then allowed to operate without any further outside interference. After a number of changes of the internal states of the various cells, and the passage of various signals on the intercell leads, the entire network may reach an equilibrium situation, in which the internal states of the cells no longer change with time. On the other hand, the network may fall into a cycle, in which the internal state of at least one cell changes periodically. Our first question is, "If we have given the cell description, is there some number of cells and some combination of primary input values for which the network will enter a cycle when it is started from the designated initial conditions?"

We shall consider two iterative networks of the same length to be equivalent if and only if they ultimately produce the same primary outputs when presented with the same primary inputs. Our second question is, "If we have given two different cell descriptions, are the corresponding networks made up of an arbitrary number of these cells always equivalent?" Unfortunately, both of these questions turn out to be recursively undecidable. The proof of this statement is based upon an undecidability result from Post (1), known as the "correspondence problem." In essence, Post's result states that it is not possible to determine whether or not there exists a finite sequence of "0's" and "1's" which can be partitioned according to certain rules. However, any given finite sequence of "0's" and "1's" can readily be checked to see whether or not it satisfies the required conditions. By using an iterative network of the type described above
to perform this checking operation, it is possible to construct an iterative network which has a cycle if and only if the correspondence problem has a solution. Then any method that could decide whether the iterative network has a cycle could also decide whether the correspondence problem has a solution, and Post has shown that this is impossible. By means of a slight further modification, we can also prove that there does not exist a general test for determining whether or not two given cell structures yield equivalent networks.

It can be shown that if we allow an iterative network to be started with its cells in any arbitrary combination of initial states, rather than with each cell in the same state, it is possible to determine whether or not there exists a primary input combination for which a cycle occurs. In other words, given the structure of a single cell, it is possible to determine whether a network made up of such cells can exhibit cyclic behavior, but there is no general method for determining whether the networks will enter such a cycle when started with a specific set of initial conditions.

The recursive undecidability of these two questions – that is, the lack of a finite algorithm that will always work – implies that there is no general analysis procedure for networks of the class described. In particular, there is no unique canonic form to which we can reduce any given network for the purpose of describing its behavior or comparing it with another network.

F. C. Hennie III

References


F. EXTRACTION OF INFORMATION FOR A PAIR OF PERIODICALLY VARYING RANDOM WAVEFORMS*

In order to determine position by triangulation it is necessary to devise a system whose output is an indication of the time shift between signals received at two or more distinct positions. In this study we have investigated statistical methods for estimating the time shift between a pair of signals that are both random and periodic in some sense. Since noise is usually present, the received waveforms can be represented by

\[ f_1(t) = s(t) + n_1(t) \]  

and

\[ f_2(t) = s(t) + n_2(t) \]  

\[ f_3(t) = s(t) + n_3(t) \]

*This work was supported in part by the Office of Naval Research under Contract Nonr-1841(57).
where \( s(t) \) is the periodically varying random signal, \( \tau \) is the time shift, \( n_1(t) \) and \( n_2(t) \) are the additive noises, and \( T \) is the length of the waveform sample. We have considered two different statistical models for the signal, which will be described. The choice of model for a particular situation will, of course, depend upon the actual signal characteristics. The additive noises \( n_1(t) \) and \( n_2(t) \) have been assumed throughout this report to be samples from identical statistically independent processes.

The first and simplest model for a periodic, yet random, signal is to represent it as a stationary Gaussian process with a correlation function

\[
R_s(t) = E[s(u)s(u+t)] = \sum_{-\infty}^{\infty} \sigma_n^2 e^{i\omega_o nt}
\]

which is periodic. Under the assumptions that the noise is white and gaussian, and that \( T \) is an integral multiple of \( 2\pi/\omega_o \), the a posteriori probability distribution for \( \tau \) is monotonically related to

\[
\mu_1(\tau) = \sum_{-\infty}^{\infty} \sigma_n^2 \frac{1}{N_o + \sigma_n^2/2T} \int_0^T \int_0^T f_1(u) f_2(v) \exp[j\omega_o(u-v+\tau)] \, du \, dv
\]

where \( N_o \) is the noise power density. The value of \( \tau \) for any particular set of received waveforms that maximizes \( \mu_1(\tau) \) is the most probable value of the time delay.

In the second model chosen, the signal can be represented as a periodically modulated random process; that is,

\[
s(t) = g(t) w(t)
\]

where \( g(t) \) is a periodic modulation, and \( w(t) \) is a sample function from a stationary nonperiodic random process. If we choose both the signal and the noise to be bandlimited white Gaussian processes, and make the additional requirement that the expected signal power for any particular periodic modulation is always much greater than the expected noise power, then the a posteriori probability is monotonically related to a correlation function; that is,

\[
\mu_2(\tau) = \int_{-\tau/2}^{\tau/2} f_1(t+\tau/2) f_2(t-\tau/2) \, dt
\]

Again, the value of \( \tau \) which maximizes \( \mu_2(\tau) \) for a given set of received waveforms is the most probable value of time shift. If, however, the expected signal power for any particular periodic modulation is always less than the expected noise power, we must further specify the periodic modulation in order to obtain a system. If we now allow \( g(t) \) to
be a random process with
\[ R_2(t) = \mathbb{E}[g^2(u)g^2(u+t)] = \sum_{n=-\infty}^{\infty} S_n e^{j\omega_0 nt} \] (6)
then Eq. 5 is replaced by
\[ \mu_3(\tau) = \sum_{n=-\infty}^{\infty} S_n \int_{-\tau/2}^{T+\tau/2} f_1(t+\tau/2) f_2(t-\tau/2) \exp[j\omega_0 n(t-\tau/2)] dt \] (7)

Future work will be aimed at evaluating the solutions obtained and devising practical schemes for approximating them.

W. M. Siebert, I. G. Stiglitz

G. A MECHANICAL HAND

Digital computers have been used successfully for nonnumerical tasks like solving geometry problems, setting up equilibrium equations for electrical networks, or playing chess. In all of these cases a human programmer has to translate the physical situation of the outside world into a corresponding model situation within the computer. The computer then performs operations in its model world according to rules specified by the human programmer. The results of these operations are finally converted back to our own language, and applied to the physical world, by a human operator.

If we could provide the computer with a direct bilateral coupling organ to the physical world, we could study both the problems of setting up efficient models and rules of operation within an information-processing system and of translating between these models and the real world. A mechanical hand has been proposed as a possible coupling device by Prof. C. E. Shannon and Prof. M. L. Minsky.

During the past year a mechanical hand with 15 degrees of freedom was constructed. Kinetically, it is similar to a human hand except for the use of a simplified, solid (rather than flexible) palm. Finger points are of the tongue-and-groove type, each joint permitting a 90° flexion in palmar direction from the extended rest position. A spring in each joint provides the extensor action. Flexing is controlled by braided nylon line and can cause a curling of the finger or a motion of the extended finger about the joint between the third segment and the palm. The thumb is mounted on the palm so as to allow proper opposition of all fingers. The device is constructed mainly of aluminum.

Several tactile sensing devices employing beryllium copper strips have been tried out. A more satisfactory method uses a rubber material that changes its electric resistance with changes in pressure. The material is sensitive down to 0.5 ounce/cm² and provides a useful continuous response over a wide range of pressures.
In order to reduce the amount of equipment development, we are now considering the possibility of using commercial equipment for the construction of an arm. This will be essentially a motorized mechanical servomanipulator like the ones used for handling radioactive material. This relatively simple (7 degrees of freedom) arm-tong combination will be linked to the TX-0 computer as soon as possible because it is felt that experimental feedback is needed for the continuation of the project. At a later stage of the project we plan to use the hand described above, together with the arm.

D. L. Reich, H. A. Ernst