Coordinated
Science
Laboratory

UNIVERSITY OF ILLINOIS – URBANA, ILLINOIS

CONVOLUTIONAL TRANSFORMATIONS OF BINARY SEQUENCES: BOOLEAN FUNCTIONS AND THEIR RESYNCHRONIZING PROPERTIES

F. P. Preparata

REPORT R-283 MARCH, 1966

This work was supported by the Joint Services Electronics Program (U. S. Army, U. S. Navy, and U. S. Air Force) under Contract No. DA 28 043 AMC 00073(E).

CONVOLUTIONAL TRANSFORMATIONS OF BINARY SEQUENCES: BOOLEAN FUNCTIONS AND THEIR RESYNCHRONIZING PROPERTIES

F. P. Preparata

ABSTRACT

Non-feedback shift registers (finite-memory encoders) can be profitably adopted to perform transformations of binary sequences. The output sequence is convolutionally obtained by "sliding" the encoding device along the input sequence and producing a symbol at each shift. Invertible transformations are characterized and decoding schemes are analyzed. The crucial point in the decoding problem is that the simply finite-memory feedback decoder presents the undesirable well-known error propagation effect, while the non-feedback decoder contains, in general, an indefinite number of stages. Finite-memory non-feedback decoding is feasible, however, if some constraint is imposed on the input sequences, or, equivalently, if some decoding error is tolerated. The analysis is conducted through the concepts of resynchronizing states of Boolean functions. The algebraic properties of resynchronizing states are carefully analyzed; it is shown that they can be assigned only in special sets, termed clusters, which form a lattice. Moreover, each cluster of resynchronizing states is possessed by a set of Boolean functions, which form a subspace of the vector space of all Boolean functions. The presented analysis provides a formal tool to relate finite-memory non-feedback decoding to the constraint imposed on the input generating source.

I. Introduction

The transformation of a symbol sequence into another symbol sequence is an important necessity in several practical cases of information processing and transmission. Particularly, the need may arise in the area of coding for noisy channels or, for example, in the area of cryptology. These possible applications stimulated some research over the past years, and especially Huffman's work [1] deserves mention as a fundamental investigation of finite-state machines as sequence transducers.

The theoretical analysis presented in this paper confines itself to a more limited class of finite-state transducers, which, nevertheless, for its intrinsic simplicity and flexibility is felt to be of considerable interest in practical realizations. We refer specifically to sequence transformations performed by convolutional finite-memory encoders, without feedback, which we shall introduce in the next section.

The central problem connected with sequence transformations is the unique reconstruction of the original (input) sequence from the transformed (output) sequence, i.e., the inversion of the transformation. The requirement of invertibility confines the analysis to information-lossless transformations, according to the appropriate terminology of Huffman. The problem, however, is not only the characterization of information lossless transformations, but also the circuit implementation of them.

These and other related topics are the subject of the following sections.

II. Formulation of the Problem, Preliminary Analysis

Time is subdivided into units defined by clock pulses, and during each time unit a sequence symbol occurs. The clock pulses also operate as shifting pulses for shift registers. The sequence symbols are chosen from the alphabet (0,1); and hereafter we shall use indifferently the terms "symbol" and "digit." Time units t_s are numbered in natural order, and each sequence symbol is given the index of the time unit at which it occurs. With x_s we denote an input symbol, with y_s the output symbol occurring at the same time unit t_s. Similarly, $\{x\}$ and $\{y\}$ denote corresponding input and output sequences irrespective of their number of symbols. Boolean functions f, g, ... are always assumed in ring form, i.e., in sum-of-product form with the connectives AND and EXCLUSIVE OR (see, e.g. [2]), the latter being denoted by the symbol +. Arguments of Boolean functions, i.e., Boolean variables, are generally designed with the letter z.

The general form of a convolutional finite-memory encoder is given in Fig. 1.

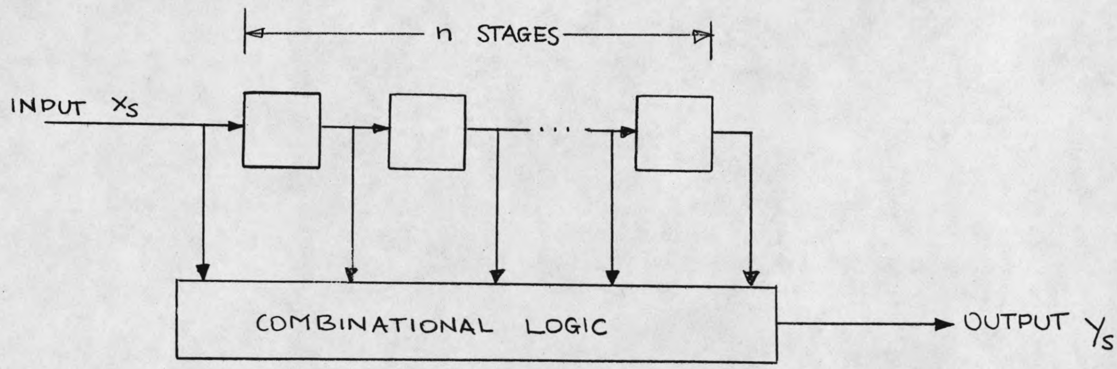

Fig. 1. Convolutional Finite-Memory Encoder.

Input symbols are fed to the shift register at the rate determined by the clock pulses. The output of each register stage and the input line feed a combinational block consisting of a single Boolean function g of (n+1) variables. The generic output symbol y_s is given by

$$y_s = g(x_s, x_{s-1}, \ldots, x_{s-n}).$$

This justifies the term <u>convolutional</u> given to the transformation, although "recurrent" may be equally appropriate. The transformation, in fact, may be thought of as performed by an encoding device which "slides" along the input sequence producing, at each shift, an output symbol.

The first step is the characterization of the function g in order that the transformation be invertible. We refer to the state graph of the encoder of Fig. 1, which has the well-known structure of a shift-register graph (see, for example [8]). States are determined by the contents of the encoder; each state is identified with a vertex, and each vertex has two incoming and two outgoing branches. Each branch is labeled with a symbol pair (x,y), designating respectively the input symbol which determines the transition and the output symbol produced.

The well-known condition for invertibility of the transformation [1] can be formulated as follows: for any pair of states s_1 and s_2 of the encoder and any pair of different input sequences $\{x\}$ and $\{x'\}$ of equal length, leading from s_1 to s_2, the corresponding sequences $\{y\}$ and $\{y'\}$ are different. Let us suppose, without loss of generality, that $\{x\}$ and $\{x'\}$ differ in their first symbol (should they not differ, there will be some other state s_3, following s_1, after which $\{x\}$ and $\{x'\}$ differ; in this case we assume s_3 as initial state). If the transformation is invertible, the output symbols are also different, i.e., the symbol pairs relative to the branches pointing out of s_1 must be $(0,y_o)$, $(1,\overline{y}_o)$. Reciprocally, if $(0,y_o)$ and $(1,\overline{y}_o)$ are pairs associated with branches leaving s_1, no two input sequences with different first symbols can yield the same output sequence. Since s_1 is arbitrary, we may conclude that the above stated condition holds for each state if and only if the transformation is invertible. It is now easy to recognize that this is equivalent to saying that $g(z_{n+1},z_n,\ldots,z_1)$ must be of the form

$$g(z_{n+1}, z_n,\ldots,z_1) = z_{n+1} + f(z_n,z_{n-1},\ldots,z_1)$$

where f is an arbitrary function of n Boolean variables. Our discussion is summarized by the following theorem.

<u>Theorem 1</u>: A necessary and sufficient condition that the transformation operated by a finite-memory non-feedback encoder be invertible is that

$$g(z_{n+1},z_n,\ldots,z_1) = z_{n+1} + f(z_n,z_{n-1},\ldots,z_1). \tag{1}$$

We may now say that $f(z_n,z_{n-1},\ldots,z_1)$ completely specifies an n-stage finite memory encoder, and that the sequence transformation is governed by the following equation

$$y_s = x_s + f(x_{s-1}, x_{s-2},\ldots,x_{s-n}). \tag{2}$$

Correspondingly, the encoder for invertible transformations is illustrated in Fig. 2 (with obvious significance of the adopted symbols).

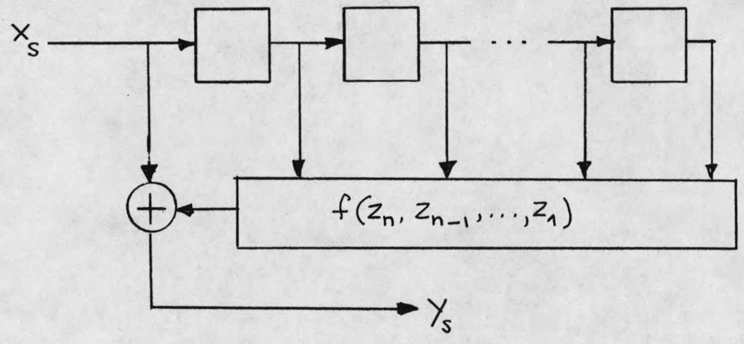

Fig. 2. Convolutional Finite-Memory Encoder for Invertible Transformations.

Obviously, Eq. (2) is not sufficient to determine the sequence $\{y\}$ resulting from a given sequence $\{x\}$, since the initial state of the encoder (i.e., its content when the first digit of $\{x\}$ is fed to it) must also be known. Therefore, if x_1 is the first symbol of $\{x\}$, and $(x_0, x_{-1}, x_{-2}, \dots, x_{-n+1})$ is the initial content of the encoder, the sequence $\{y\}$ is entirely known.

It is also apparent that, given the initial state $(x_0, x_{-1}, \dots, x_{-n+1})$ Eq. (2) leads to the relation governing the inverse transformation, i.e.,

$$x_s = y_s + f(x_{s-1}, x_{s-2}, \dots, x_{s-n}) \ . \tag{2'}$$

Clearly, (2') is physically implemented by a <u>feedback</u> shift-register decoder as given in Fig. 3, which is initially loaded with $(x_0, x_{-1}, \dots, x_{-n+1})$.

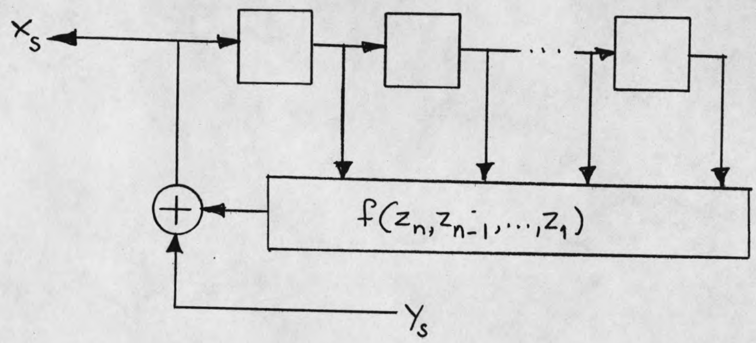

Fig. 3. Feedback Decoder Corresponding to the Encoder of Fig. 2.

This very simple realization has, however, a major inconvenience, as soon as we take into account the possibility that some symbols of the $\{y\}$ sequence are altered by effect, for example, of transmission through a naturally or artifically noisy channel. In fact, if one symbol y_s is altered, the corresponding x_s will be affected by error, and this error will in turn affect the decoding of further symbols of $\{x\}$, thereby corrupting the recovered sequence further beyond the injected error. Essentially, we are confronted with the familiar error propagation effect which is typical of feedback convolution decoding (see, e.g. [3]).

In our case, particularly, we are facing the possibility that a single erroneous y symbol may cause an indefinite corruption of the decoded sequence. This, of course, would rule out the feedback decoder as a practical device for the reconstruction of the original sequence. It may be conjectured, however, that by proper selection of the function $f(z_n, z_{n-1}, \ldots, z_1)$, there is a non-zero probability that the error propagation terminate at a finite distance from the injected errors. This would happen when, after the error, n consecutive correct x symbols are produced so that the decoder is free from errors. If we could prove that some functions possess the statistical property of a rapid error termination, the feedback decoder could retain some importance because of its simplicity in applications where the transmission error rate is low and the receiver has a reasonable error tolerance. A preliminary study has been conducted, which shows that there are functions for which the error may not propagate indefinitely. But since no conclusion can so far be drawn as to how likely and how far from its origin the error will die out, the feedback decoder must, in general, be considered impractical.

To circumvent this basic drawback, the question now arises whether it is possible to reconstruct the $\{x\}$ sequence by means of a finite-memory decoder without feedback. The attractive feature of such a device is that, due to the lack of regenerative effects, any injected error will affect the recovered sequence at most for a finite and constant number of digits. The general answer to this question is in the negative. In fact, a little thought shows that x_s is, in general, a function of all preceding y symbols, so that for correct decoding the non-feedback decoder should contain an indefinite number of stages if no bound is placed on the length of the sequences.

The intuition suggests, however, that if y_s depends only on a finite segment of length n of the sequence $\{x\}$, the dependence of

x_s on the symbol y_{s-j} should become weaker as j grows. In other words, x_s should depend strongly on immediately preceding y symbols and weakly on remote ones. This rather rough conjecture can be formalized into the following problem: given a transformation specified by the function $f(z_n, z_{n-1}, \ldots, z_1)$, given the sequence $\{x\}$ and its transform $\{y\}$ of length s, which is the lowest value of r such that x_s depends only on $y_s, y_{s-1}, \ldots, y_{s-r}$?

Before tackling this problem, we need some introductory remarks and definitions. We restrict our attention to the functions f for which

$$f(0,0,\ldots,0) = 0 \tag{3}$$

with negligible loss in generality, since only those functions are excluded which contain, in ring form, the constant term [2,7]. Further we assume that the encoder contains 0's when the first symbol of $\{x\}$ is fed to it; we fix hereby the initial state of the encoder, or think of the sequence $\{x\}$ as being extended with 0's indefinitely into the past. This assumption and relation (3) imply that the first non-zero symbols of $\{x\}$ and $\{y\}$ occur simultaneously.

If the sequence $\{y\} = y_1, y_2, \ldots, y_s, \ldots$, transformed from the sequence $\{x\} = x_1, x_2, \ldots, x_s$, is such that the sequences

$$y_1, y_2, \ldots, y_m, 0, 0, \ldots$$

and

$$0, 0, \ldots, 0, y_{m+1}, y_{m+2}, \ldots, y_s, \ldots$$

are respectively the transforms of

$$x_1, x_2, \ldots, x_m, 0, 0, \ldots$$

and

$$0, 0, \ldots, 0, x_{m+1}, x_{m+2}, \ldots, x_s, \ldots,$$

we say that $\{x\}$ possesses a resynchronizing point (RP) $x_m | x_{m+1}$ under f. This is equivalent to saying that $y_{m+1}, y_{m+2}, \ldots$ do not depend upon $x_m, x_{m-1}, \ldots$, etc.

The concept of RP of a sequence plays a central role in the solution of the aforestated problem. In fact, let $x_m | x_{m+1}$ be an RP of $\{x\}$ under f, with $m < s$, if we restrict our attention to the sequences $\{x'\} \equiv x_{m+1}, x_{m+2}, \ldots, x_s$ and $\{y'\} \equiv y_{m+1}, y_{m+2}, \ldots, y_s$, we see that x_s depends at most on $y_s, y_{s-1}, \ldots, y_{m+1}$. Consequently, we may see that the dependence of x_s on previous y symbols extends back to the closest RP of $\{x\}$ under f. This completely defines the parameter r mentioned in the problem statement.

It must be explicitly pointed out that the value of <u>r</u> is by no means a characteristic of the transformation, nor of the sequence, but it depends jointly upon the transformation and the particular sequence under consideration. More precisely, for a given function f, any sequence $\{x\}$ can be thought of as the concatenation of <u>irreducible</u> subsequences contained between consecutive RP's: if m is the length of the longest irreducible subsequence of $\{x\}$, then $r = m-1$.

The search for RP's of $\{x\}$ under f is greatly simplified by the concept of <u>resynchronizing state</u> (RS) of the function f. We say that the n-tuple $Z = (z_n, z_{n-1}, \ldots, z_1)$ is an RS of f if and only if the following conditions hold:

$$
\begin{aligned}
& f(0,0,\ldots,0) = 0 \\
& f(z_n,z_{n-1},\ldots,z_1) = f(0,0,\ldots,0) \\
& f(\delta_1,z_n,\ldots,z_2) = f(\delta_1,0,\ldots,0) \qquad (4) \\
& \ldots\ldots \\
& f(\delta_{n-1},\ldots,\delta_1,z_n) = f(\delta_{n-1},\ldots,\delta_1,0)
\end{aligned}
$$

where $\delta_1,\delta_2,\ldots,\delta_{n-1}$ are arbitrary binary parameters. The previous set of equations, referred to hereafter as "system (4)," completely defines the RS's of f. Due to the arbitrariness of $\delta_1,\delta_2,\ldots,\delta_{n-1}$, it is evident that if $(z_n,z_{n-1},\ldots,z_1)$ is an RS of f, $\{x\}$ has $x_m|x_{m+1}$ as RP under f if

$$x_m = z_n,\ x_{m-1} = z_{n-1},\ldots,x_{m-n+1} = z_1.$$

Therefore, the RP's of $\{x\}$ under f are obtained by sliding an n-symbol window along $\{x\}$ and verifying whether the intercepted configuration coincides with any RS of f. The sets of RS's of Boolean functions enjoy interesting algebraic properties, which will be carefully investigated in the two following sections.

We conclude this section by noting that the unboundedness of r for all possible sequences $\{x\}$ is another formal confirmation that finite-memory non-feedback decoding is not possible, in general. The introduced formalism, however, allows an exact definition of the conditions under which finite-memory non-feedback decoding is possible. Precisely, let us consider the indefinite non-feedback decoder illustrated in Fig. 4.

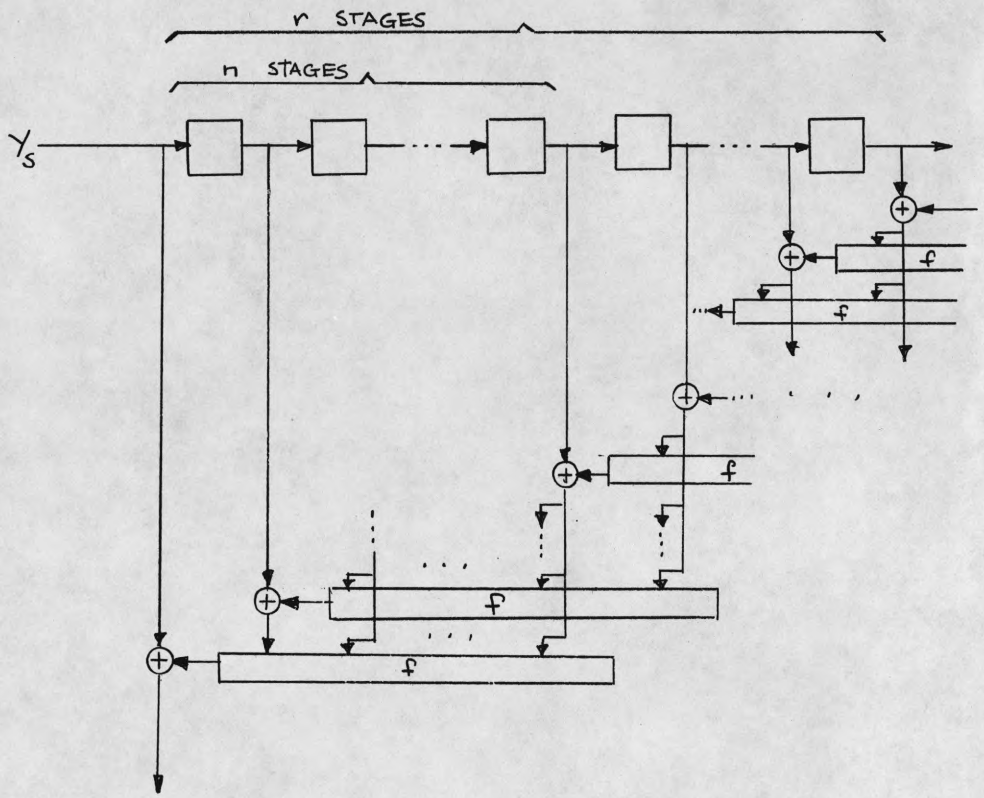

Fig. 4. General Form of Indefinite Non-Feedback Decoder.

If we truncate this decoder after its r-th stage, we obtain a finite-memory decoder which reconstructs correctly any sequence $\{x\}$ which does not contain any irreducible subsequence of length greater than (r+1). It is therefore evident that finite memory non-feedback decoding is possible, only at the price of some constraint on the input language. It conforms with our intuition that this constraint becomes weaker as r increases. We shall return to this topic at the conclusion of the paper.

III. The Algebra of Clusters of Resynchronizing States

In this section we shall show that, generally, RS's are not independently assignable, and that only given subsets of RS's are possible. These subsets are called RS-clusters, or simply clusters, and we shall show that their set is a lattice.

Let $Z = (z_n, z_{n-1}, \ldots, z_1)$ be a binary n-tuple, and let z denote the integer spelled by Z. The n-tuple Z is an RS of f, if and only if the conditions expressed by system (4) hold for it. We have then the following lemma.

Lemma 1: If Z is an RS of f, then $z_n = 0$.

Proof: The function f can be expressed, in ring form, as

$$f(z_n, z_{n-1}, \ldots, z_1) = f_0(z_n, \ldots, z_2) + z_1 f_1(z_n, \ldots, z_2)$$

with $f_1(z_n, \ldots, z_2)$ not identically 0. If we put the last row of (4) in this form, we obtain

$$f_0(\delta_{n-1}, \ldots, \delta_1) + z_n f_1(\delta_{n-1}, \ldots, \delta_1) = f_0\,(\delta_{n-1}, \ldots, \delta_1).$$

It follows that $z_n \cdot f_1(\delta_{n-1}, \ldots, \delta_1) = 0$; and since $f_1(\delta_{n-1}, \ldots, \delta_1)$ is not identically 0, $z_n = 0$. Q.E.D.

By lemma 1, the last row of system (4) becomes an identity, and is therefore omitted. After this preliminary restriction on possible RS's, the following lemmas estlabish the interdependences among them.

Lemma 2: If $(0, z_{n-1}, \ldots, z_1)$ is an RS of f, so is $(0, 0, z_{n-1}, \ldots, z_2)$.

Proof: Let us write system (4) for $(0,z_{n-1},\dots,z_1)$. If we set $\delta_1 = 0$, we obtain

$$f(0,0,\dots,0) = 0$$

$$f(0,0,z_{n-1},\dots,z_2) = f(0,0,\dots,0)$$

$$f(\delta_2,0,\dots,z_3) = f(\delta_2,0,\dots,0)$$

$$\dots\dots$$

$$f(\delta_{n-2},\dots,0,z_{n-1}) = f(\delta_{n-2},\dots,0,0)$$

which, for arbitrary $\delta_2,\delta_3,\dots,\delta_{n-2}$, are exactly the conditions that $(0,0,z_{n-1},\dots,z_2)$ be an RS of f. Q.E.D.

The lemma just given has the following direct corollary.

Corollary 1: If $(0,z_{n-1},\dots,z_1)$ is an RS of f, so are $(0,0,z_{n-1},\dots,z_2)$, $(0,0,0,z_{n-1},\dots z_3),\dots,(0,0,\dots,0)$. Corollary 1 says, in other words, that given an RS of f all the right shifts of it are RS's of f. A still wider set of RS's associated with, or implied by, a given RS of f is given by lemma 3.

Lemma 3: If $(0,z_{n-1},\dots,z_s,0,\dots,0)$ is an RS of f, so is $(0,z_{n-1},\dots,z_s 0,z_{n-1},\dots,z_r)$ if $n-s \geq [n/2]$[1] $(r \geq s)$, or $(0,z_{n-1},\dots,z_s,0,z_{n-1},\dots,z_s,0,\dots,0)$ if $n-s < [n/2]$; and vice versa.

Proof: Since the proofs of the two cases $n-s \geq [n/2]$ and $n-s < [n/2]$ are identical, we shall only prove the first case and leave the other to the reader.

We rewrite system (4) for $(0,z_{n-1},\dots,z_s,0,\dots,0)$ and obtain

---

[1] With [a] we denote the highest integer contained in a.

$$f(0,0,\ldots,0) = 0$$

$$f(0,z_{n-1},\ldots,z_s,0,\ldots,0) = f(0,0,\ldots,0)$$

$$f(\delta_1,0,\ldots,z_{s+1},z_s,\ldots,0) = f(\delta_1,0,\ldots,0) \tag{4a}$$

$$\ldots$$

$$f(\delta_{n-2},\ldots,\delta_1,0,z_{n-1}) = f(\delta_{n-2},\ldots,\delta_1,0,0)$$

the (r+1)-th row of (4a) reads

$$f(\delta_{r-1},\ldots,\delta_1,0,z_{n-1},\ldots,z_r) = f(\delta_{r-1},\ldots,\delta_1,0,\ldots,0) .$$

If we let $\delta_{r-1} = 0$, $\delta_{r-2} = z_{n-1},\ldots,\delta_1 = z_s$, we have

$$f(0,z_{n-1},\ldots,z_s,0,z_{n-1},\ldots,z_r) = f(0,z_{n-1},\ldots,z_s,0,\ldots,0),$$

the right member of which is the left member of the 2nd row of (4a). Therefore, by the transitive property of equalities,

$$f(0,z_{n-1},\ldots,z_s,0,z_{n-1},\ldots,z_r) = f(0,0,\ldots,0).$$

Similarly, we consider the (r+j)th row of (4a). We let $\delta_{r-1} = 0$, $\delta_{r-2} = z_{n-1},\ldots, \delta_1 = z_s$ and obtain ($j = 1,2,\ldots,s-3$)

$$f(\delta_{r+j-2},\ldots,\delta_r,0,z_{n-1},\ldots,z_s,0,z_{n-1},\ldots,z_{r+j-1})$$

$$= f(\delta_{r+j-2},\ldots,\delta_r,0,z_{n-1},\ldots,z_s,0,\ldots,0).$$

By comparing this relation with the (j+1)th row of (4a) and letting $\delta_{r+k-1} = \delta_k = \delta'_k$ ($k = 1,2,\ldots,j-1$) we obtain

$$f(\delta'_{j-1},\ldots,\delta'_1,0,z_{n-1},\ldots,z_s,0,z_{n-1},\ldots,z_{r+j-1}) = f(\delta'_{j-1},\ldots,\delta'_1,0,\ldots,0).$$

For all possible values of j, we obtain

$$f(0,z_{n-1},\ldots,z_s,0,z_{n-1},\ldots,z_1) = f(0,0,\ldots,0)$$

$$f(\delta_1',0,z_{n-1},\ldots,z_s,0,\ldots,z_{r+1}) = f(\delta_1',0,\ldots,0)$$

$$\ldots$$

$$f(\delta'_{s-3},\ldots,\delta_1',0,z_{n-1},\ldots,z_s,0z_{n-1}) = f(\delta'_{s-3},\ldots,\delta'_{s-3},\ldots,\delta_1',0,\ldots,0).$$

If we add to this list the s-th,(s+1)-th,...,n-th rows of (4a), together with $f(0,0,\ldots,0) = 0$, we obtain the conditions that $(0,z_{n-1},\ldots,z_s,0,z_{n-1},\ldots,z_1)$ be an RS of f.

The proof of the reciprocal part of the lemma follows exactly the steps of the one just given. Q.E.D.

It may be worth mentioning that the relation established by lemma 3 is an equivalence between n-tuples. Verification that the reflexive, symmetric and transitive properties hold is immediate, and is therefore omitted. Lemma 3 has the following corollary.

Corollary 2: If $(0,z_{n-1},\ldots,z_p,0,\ldots,0)$ is an RS of f, with $z_p = 1$, so are $(0,z_{n-1},\ldots,z_p,0,\ldots,0,z_{n-1}),(0,z_{n-1},\ldots,z_p,0,\ldots,$ $z_{n-1},z_{n-2}),\ldots,(0,z_{n-1},\ldots,z_p,0,z_{n-1},\ldots,z_p,0,\ldots,0)$, and vice versa.

Proof: The proof follows directly from lemma 3 when appropriate values are assigned to $z_{p-1},z_{p-2},\ldots,z_s (s < p)$. Q.E.D.

An example should provide further insight into the meaning of lemmas 2 and 3.

Example: If 010000 is an RS of f, by Corollary 2 010001, 010010, 010100 are also RS's of f. Further application of Corollary 2 to 010100 shows that 010101 is also an RS of f. Therefore 010000, 010001, 010010, 010100, 010101 are equivalent in the relation established by lemma 3. By lemma 2, we have the following implications

$$010000 \Longrightarrow 001000,\ 000100,\ 000010,\ 000001,\ 000000$$
$$010001 \Longrightarrow 001000,\ 000100,\ 000010,\ 000001,\ 000000$$
$$010010 \Longrightarrow 001001,\ 000100,\ 000010,\ 000001,\ 000000$$
$$010100 \Longrightarrow 001010,\ 000101,\ 000010,\ 000001,\ 000000$$
$$010101 \Longrightarrow 001010,\ 000101,\ 000010,\ 000001,\ 000000$$

Therefore, the distinct RS's implied by 010000 are

010001, 010010, 010100, 010101
001000, 001001, 001010
000100, 000101
000010
000001
000000

It may be convenient at this point to introduce a compact representation for the equivalence classes yielded by lemma 3. We make partial use of the formalism of regular expressions[1] [4].

Let the symbol 0 denote exclusively the binary zero and let $P_1, P_2, P_3, \ldots$ be binary configurations beginning with a 0. The numbers of digits $\nu_1, \nu_2, \nu_3, \ldots$ contained respectively in $P_1, P_2, P_3, \ldots$ are generally different, but all satisfy the condition $\nu_j \leq n$. With the expression

$$[(P_j 0^*)^*]_n$$

---

[1] We recall, briefly, for the reader's convenience, that if A and B denote sets of sequences: 1) (A+B) is the set union of the sequences of A and B, 2) (A.B) is the set of sequences obtained by concatenation of a sequence of A and of a sequence of B, 3) if λ is the zero-length sequence, A* is defined as

$$A^* = \lambda + A + AA + \ldots$$

we denote the set of n-tuples obtained by truncating after n symbols the sequences of the set $(P_j0^*)^*$ of length not smaller than n. We say that P_j is a minimal configuration if there is no other configuration P_i with $\nu_i < \nu_j$ such that

$$P_j = [(P_i0^*)^*]_n$$

Therefore, for any n, it is possible to list a complete set of minimal configurations. Hereafter, we shall refer only to minimal configurations.

Example: For n = 5, the minimal configurations are

0, 01, 011, 0111, 01111, 01011, 001, 0011, 00111,
0001, 00011, 00001

With this formalism, lemma 2 states that if $[P0^*]_n$ is an RS of f, so are $[0^*P0^*]_n$; lemma 3 states that if $[P0^*]_n$ is an RS of f, so are $[(P0^*)^*]_n$. The combination of lemmas 2 and 3 ensures that if $[P0^*]_n$ is an RS of f, so are $[0^*(P0^*)^*]_n$.

We can now state the following lemma, which establishes a further equivalence relation between RS's.

Lemma 4: If $[P_10^*]_n$ and $[P_20^*]_n$ are two RS's of f so are $[0^*\{(P_10^*)^*(P_20^*)^*\}^*]_n$.

Proof: We write the conditions that $[P_10^*]_n$ and $[P_20^*]_n$ be RS's of f. If Z is an n-tuple of $[0^*\{(P_10^*)^*(P_20^*)^*\}^*]_n$, by comparing appropriate relations of the two systems we can prove that Z is an RS of f. Since the details of the proof are very similar to those used for proving lemma 3, they are omitted. Q.E.D.

Example: If $P_1 = 01$, $P_2 = 011$ and n = 5 we have

$$[0^*(010^*)^*]_5 = 01000,\ 01001,\ 01010,\ 00100,\ 00101,\ 00010,\ 00001,\ 00000.$$

$$[0^*(0110^*)^*]_5 = 01100,\ 01101,\ 00110,\ 00011,\ 00001,\ 00000.$$

In addition to the distinct n-tuples belonging to $[0^*(010^*)^*]_5$ and to $[0^*(0110^*)^*]_5$, the set $[0^*\{(010^*)^{**}(0110^*)^*\}^*]_5$ also contains 01011.

We now make the incidental remark that, although we have referred so far to RS's of f, the interdependence among n-tuples as RS's is not related to a particular function. In fact system (4) expresses a pairwise association of binary n-tuples under the condition that Z be a RS; and lemmas 2,3,4, which express the interdependence between RS's, are entirely based on this pairwise association. Therefore, the original problem of finding the RS's of a given function, leads to the following dual problem: to find the functions that have a given set of RS's. The solutions of these two problems, the latter of which is just now taking shape, will be given in the following section. At this stage, we only state that sets of RS's can be considered autonomously, and this standpoint will be assumed in the rest of the paper.

Returning now to our main theme, we define <u>basic RS-clusters</u>, or basic clusters of order n as the sets of n-tuples identified by $[0^*(P0^*)^*]_n$, for every minimal configuration P. Basic clusters are denoted with the capital letter B. Given r basic clusters $B_1 = [0^*(P_1 0^*)^*]_n$, $B_2 = [0^*(P_2 0^*)^*]_n, \ldots, B_r = [0^*(P_r o^*)^*]_n$, we define as <u>join</u> of $B_1, B_2, \ldots, B_r$ the set $C = [0^*\{(P_1 0^*)^*(P_2 0^*)^* \ldots (P_r 0^*)^*\}^*]_n$ and denote it with the expression

$$C = B_1 \cup B_2 \cup \ldots \cup B_r$$

which is not to be confused with the usual set union. Clusters of order n are the basic clusters of order n and all their possible distinct joins. Clusters are generally designated with the capital letter C. A cluster $[0^*(PO^*)^*]_n$ is said to be of level ℓ, if z_ℓ is the highest indexed non-zero variable of $[PO^*]_n$. The cluster 00...0 is conventionally of level 0.

We define as the meet of two clusters C_1 and C_2 the usual set intersection of C_1 and C_2, and denote it with $C_1 \cap C_2$. For any clusters C_1, C_2, C_3 of order n we notice that

1) $C_1 \supseteq C_1$ (reflexive property)
2) if $C_1 \supseteq C_2$ and $C_2 \supseteq C_1$, then $C_2 = C_1$ (antisymmetric property)
3) if $C_1 \supseteq C_2$ abd $C_2 \supseteq C_3$, then $C_1 \supseteq C_3$ (transitive property)

The set of clusters is therefore partly ordered. Further, from the definitions of the join and meet operations, we can immediately verify that

a) $C_1 \cup C_1 = C_1$, $C_1 \cap C_1 = C_1$ (idempotent law)
b) $C_1 \cup C_2 = C_2 \cup C_1$, $C_1 \cap C_2 = C_2 \cap C_1$ (commutative law)
c) $C_1 \cup (C_2 \cup C_3) = (C_1 \cup C_2) \cup C_3$, $C_1 \cap (C_2 \cap C_3) = (C_1 \cap C_2) \cap C_3$ (associative law)
d) $C_1 \cup (C_1 \cap C_2) = C_1$, $C_1 \cap (C_1 \cup C_2) = C_1$ (absorption law)

Since 1, 2, 3, abcd are verified, we conclude that the set of clusters of order n form a lattice [5].

Example: We designate an n-tuple with the integer it spells. The basic clusters of order 4 are (0), (1,0), (2,1,0), (3,1,0), (5,4,2,1,0), (6,3,1,0), (7,3,1,0) and the lattice diagram [see 5,6] is given in Fig. 5. Each vertex represents a cluster, which contains the n-tuples given in parentheses. Encircled vertices denote basic clusters, and clusters with the same number of 4-tuples are drawn on the same horizontal line.

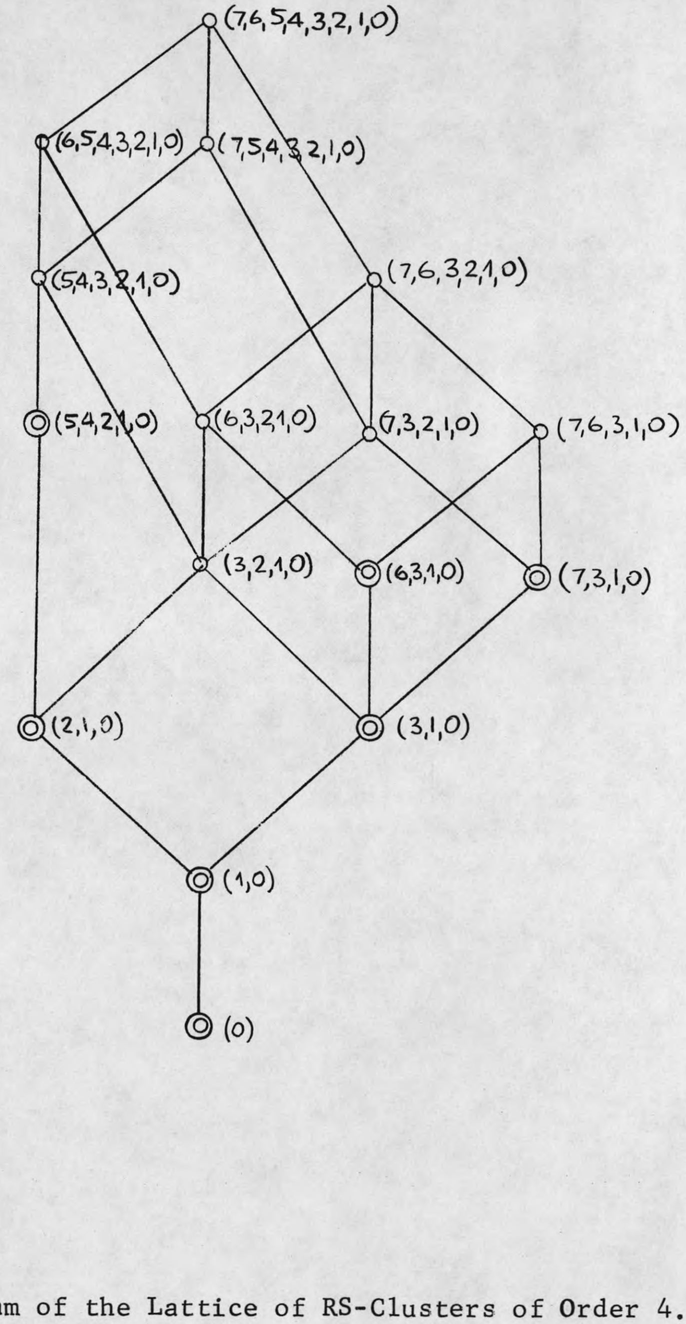

Fig. 5. Diagram of the Lattice of RS-Clusters of Order 4.

Further insight into the structure of cluster lattices is provided by the following considerations. Basic clusters $B_1, B_2, \ldots, B_k$ are said to be <u>independent</u> if for any pair of distinct indices i,j $(i,j = 1,2,\ldots,k)$ neither one of the relations $B_2 \subset B_j$ or $B_i \supset B_j$ holds. We can now prove the following decomposition theorem.

<u>Theorem 2</u>: Each cluster C of order n has a unique expression as join of basic independent clusters.

<u>Proof</u>: Cluster C certainly has an expression as

$$C = B_{j_1} \cup B_{j_2} \cup \ldots \cup B_{j_s} .$$

Suppose now that C has some other expression

$$C = B_{i_1} \cup B_{i_2} \cup \ldots \cup B_{i_r} .$$

We now select B_{i_h} and form the join

$$B_{j_1} \cup \ldots \cup B_{j_s} \cup B_{i_h} ,$$

and still obtain C. Since B_{i_h} is a basic cluster, it cannot be the join of any two clusters: therefore, there is some B_{j_k} such that

$$B_{j_k} \supseteq B_{i_h} . \tag{5}$$

If we now form the join

$$B_{i_1} \cup \ldots \cup B_{i_r} \cup B_{j_k}$$

by similar reasoning we find

$$B_{i_m} \supseteq B_{j_k} . \tag{5a}$$

By the transitive property, (5) and (5a) yield

$$B_{i_m} \supseteq B_{i_h} .$$

Since all B_i's are independent, it follows that

$$B_{i_m} = B_{i_h} = B_{j_k} .$$

It can be similarly proved that every element of the set $\{B_i\}$ coincides with an element of the set $\{B_j\}$, whence the thesis. Q.E.D.

Our previous discussion (lemmas 2, 3, 4, and the concept of cluster) shows that any cluster is an admissible set of Rs. Suppose now that a choice of RS's is made (for instance, by giving a function f and solving system (4) for <u>all</u> possible n-tuples) and their set is denoted with D: D is certainly an admissible set of RS. We now prove the stronger statement that D is a cluster. In fact let $z_1, z_2, \ldots, z_k$ be the elements (n-tuples) of D. We express each z_j in the form $[(PO^*)^*]_n$, with minimal P, and form the cluster $C_j = [0^*(PO^*)^*]_n$. Further we form the join

$$W = C_1 \cup C_2 \cup \ldots \cup C_k.$$

Certainly W contains each element of D, i.e., in set theory notation, $W \supseteq D$. Suppose that $z' \in W$ but that $z' \notin D$. The n=tuple z' is an RS (lemmas 2, 3, 4). This, however, contradicts the hypothesis that D contains <u>all</u> RS's, hence W = D. This result is summarized by the following theorem.

<u>Theorem 3</u>: Every admissible set of RS's of n-variables is a cluster of order n.

Theorem 3 completely describes the freedom of selection of n-variables RS's. In the next section we shall characterize the correspondence between sets of Boolean function and RS-clusters.

IV. The Relation Between RS-Clusters and Sets of Boolean Functions

This section is devoted to the characterization of the set of the Boolean functions which possess a given RS-cluster. A central role in this link is played by a matrix M(C) associated with each cluster C, which we shall now introduce.

Let z be the integer spelled by the binary n-tuple $\underline{z} \equiv (z_n z_{n-1}, \ldots, z_1)$. We denote with σ_z the 2^n-component column vector, the only non-zero component of thich is its (z+1)-th one.

Let $\underline{b}$ be a 2^n component column vector, the (i+1)-th component of which is $z_n^{i_n}, z_{n-1}^{i_{n-1}}, \ldots, z_1^{i_1}$ with $\underline{i} \equiv (i_n, i_{n-1}, \ldots, i_1)$. The vector representation of a Boolean function f of n variables, in ring form, is a row vector v' such that

$$v' \cdot b = f \ .$$

Finally, let S_n be a $2^n \times 2^n$ matrix given by the following recursive relation

$$S_n = \begin{bmatrix} S_{n-1} & S_{n-1} \\ 0 & S_{n-1} \end{bmatrix} \qquad \text{with } S_1 = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$$

(for a more extensive definition of S_n, see [7].

With this nomenclature, if $\underline{z}$, and $\underline{w}$ are two distinct n-tuples, the equations

$$f(\underline{z}) = f(\underline{w}) \quad , \quad f(z) = 0$$

are replaced respectively by the following vectorial expressions over GF(2)

$$v' \cdot S_n \cdot (\sigma_z + \sigma_w) = 0 \quad , \quad v \cdot S_n \cdot \sigma_z = 0 \ .$$

We further denote with σ_{zw} the vector $\sigma_z + \sigma_w$, with the convention that $z < w$.

Let us now consider system (4) written for a basic cluster B of level (n-1). We notice that the 2nd, 3rd, ..., n-th rows of (4) express, globally, $2^{n-1}-1$ pairing relations. Each of them can therefore be put into the form

$$v' \cdot S_n \cdot \sigma_{zw} = 0.$$

We order all vectors σ_{zw} in ascending order according to the index z, and, for fixed z, in descending order according to w. This ordered collection of vectors forms a $2^n \times (2^{n-1}-1)$ matrix $A_{n-1}(B)$. The matrix M(B), associated with the cluster B, is then given by the following relation

$$M(B) = S_n \cdot [\sigma_o, A_{n-1}(B)]. \tag{6}$$

<u>Example</u>: The cluster B = $[0*(010*)*]_4$ contains the 4-tuples:

0100, 0101, 0010, 0001, 0000 .

System (4) can be written with reference to any of the equivalent 4-tuples 0100, 0101. Let us choose 0100. We have then

$$\begin{cases} f(0,0,0,0) = 0 \\ f(0,1,0,0) = f(0,0,0,0) \\ f(\delta_1,0,1,0) = f(\delta_1,0,0,0) \\ f(\delta_2,\delta_1,0,1) = f(\delta_2,\delta_1,0,0) \ . \end{cases} \tag{4b}$$

Depending upon the values given to δ_1, δ_2, the last 3 rows of (4b) express 7 pairing relations. These are summarized by the following matrix

$$A_4(B) = [\sigma_{04}, \sigma_{02}, \sigma_{01}, \sigma_{4,5}, \sigma_{8,10}, \sigma_{8,9}, \sigma_{12,13}]$$

M(B) is then given by

Let us now consider system (4) written for a basic cluster B of level (n-1). We notice that the 2nd, 3rd, ..., n-th rows of (4) express, globally, $2^{n-1}-1$ pairing relations. Each of them can therefore be put into the form

$$v' \cdot S_n \cdot \sigma_{zw} = 0.$$

We order all vectors σ_{zw} in ascending order according to the index z, and, for fixed z, in descending order according to w. This ordered collection of vectors forms a $2^n \times (2^{n-1}-1)$ matrix $A_{n-1}(B)$. The matrix M(B), associated with the cluster B, is then given by the following relation

$$M(B) = S_n \cdot [\sigma_o, A_{n-1}(B)]. \qquad (6)$$

Example: The cluster $B = [0*(010*)*]_4$ contains the 4-tuples:

0100, 0101, 0010, 0001, 0000 .

System (4) can be written with reference to any of the equivalent 4-tuples 0100, 0101. Let us choose 0100. We have then

$$\begin{cases} f(0,0,0,0) = 0 \\ f(0,1,0,0) = f(0,0,0,0) \\ f(\delta_1,0,1,0) = f(\delta_1,0,0,0) \\ f(\delta_2,\delta_1,0,1) = f(\delta_2,\delta_1,0,0) \;. \end{cases} \qquad (4b)$$

Depending upon the values given to δ_1, δ_2, the last 3 rows of (4b) express 7 pairing relations. These are summarized by the following matrix

$$A_4(B) = [\sigma_{04}, \sigma_{02}, \sigma_{01}, \sigma_{4,5}, \sigma_{8,10}, \sigma_{8,9}, \sigma_{12,13}]$$

M(B) is then given by

$$M(B) = S_4[\sigma_0, A_4(t) = S_4 \cdot \begin{bmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & & & & \\ 0 & 0 & 1 & 0 & & & & \\ 0 & 0 & 0 & 0 & 0 & & & \\ 0 & 1 & 0 & & 1 & & & \\ 0 & 0 & & & 1 & & & \\ 0 & & & & 0 & & & \\ 0 & & & & & 0 & 0 & \\ 0 & & & & & 1 & 1 & \\ 0 & & & & & 0 & 1 & \\ 0 & & & & & 1 & 0 & \\ 0 & & & & & 0 & 0 & 0 \\ 0 & & & & & 0 & & 1 \\ 0 & & & & & 0 & & 1 \\ 0 & & & & & 0 & & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ & 1 & 0 & & 0 & & & 0 \\ & 0 & & & 1 & & & 1 \\ & & & & 0 & & & 0 \\ & & & & & & & 0 \\ & & & & & 0 & 0 & 0 \\ & & & & & 0 & 1 & 1 \\ & & & & & 1 & 0 & 0 \\ & & & & & 0 & & 0 \\ & & & & & 0 & & 0 \\ & & & & & 0 & & 1 \\ & & & & & 0 & & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

It is worth noticing that, by selecting 0101 instead of 0100, we should have obtained a matrix M(B) column equivalent to the one just given.

We now prove the following statement.

<u>Theorem 4</u>: If the basic cluster B has order n and level (n-1), M(C) has rank 2^{n-1}.

<u>Proof</u>: We first show that $A_{n-1}(B)$ has rank $2^{n-1}-1$. To this end, we note that if $A_{n-1}(B)$ contains the column σ_{ij} $(j < 2^{n-1})$, it also contains $\sigma_{2^{n-1}+2^{n-1}+j}$, (depending upon the value assigned to the δ parameter appearing in most significant position of the n-tuples in (4)). Therefore if $\underline{m}_0$ is the (n-1)-th level n-tuple used in writing system (4), $A_{n-1}(B)$ has the following structure

$$A_{n-1}(B) = \begin{bmatrix} \sigma_{0,m_0}, & A_{n-2} & 0 \\ & 0 & A_{n-2} \end{bmatrix}$$

Similarly, if $m_1 = [m_0/2]$, we have

$$A_{n-1}(B) = \left[\begin{array}{c|c|c} \sigma_{0,m_0}, \sigma_{0,m_1}, & \begin{array}{c|c} A_{n-3} & 0 \\ \hline 0 & \boxed{A_{n-3}} \end{array} & 0 \\ \hline & 0 & A_{n-2} \end{array}\right] \tag{7}$$

The same decomposition can be carried out exhaustively, until we obtain

$$A_1 = \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \end{bmatrix} .$$

(See, for reference, the example given above.)

Due to this iterative structure, if σ_{0,m_0} cannot be a linear combination of the remaining columns, the columns of $A_{n-1}(B)$ are linearly independent. We notice therefore that the column σ_{0,m_0} contains a <u>single</u> 1 between its $(2^{n-2}+1)$-th and 2^{n-1}-th positions: the only other columns whose non-zero terms are (only) in the same positions are those belonging to the submatrix A_{n-3} enclosed within heavy lines in (7). But, since each of these columns contains two 1's, any linear combination of them contains an <u>even</u> number of 1's: hence the rank of $A_{n-1}(B)$ is $2^{n-1}-1$.

By the same argument we can prove that σ_0 is linearly independent of the columns of $A_{n-1}(B)$, and, due to the non-singularity of S_n, the thesis follows.

Q.E.D.

If A is an r×s matrix and B an r×t matrix $(s > t)$, we indicate with the notation $A > B$ that B is column equivalent to a proper subset of the columns of A.

Let B_1 be a basic cluster of order n of the maximal level, and let B a basic cluster of order n such that $B_1 \supset B$. This entails that the pairing relations between n-tuples required by B_1 contain all the pairing relations required by B. In other words, we may say that $M(B_1) > M(B)$. We have then the following corollary of Theorem 4.

<u>Corollary 3</u>: The rank of the matrix M(B) of an n-th order, r-th level basic cluster B, is 2^r.

Proof: If $r = n-1$ we have theorem 4. If $r < n-1$, there is a cluster B_1 of maximal order (n-1), such that $B_1 \supset B$. Hence $M(B_1) >$ M(B). But since $M(B_1)$ has rank 2^{n-1}, the columns of M(B) are linearly independent. Since they are 2^r in number, the statement is proved. Q.E.D.

To complete the characterization of the matrix M(C), we have to consider the case of non-basic clusters (i.e., of joint clusters). The solution of this problem follows easily after lemma 5.

<u>Lemma 5</u>: If B_1 and B_2 are two basic clusters of level r ($r = 2,3,\ldots,n-1$) and $s < r$ is the level of $B_3 = B_1 \cap B_2$, the rank of $M(B_1 \cup B_2)$ is $2^r + 2^{r-s} - 1$.

<u>Proof</u>: If we write system (4) for both B_1 and B_2, we notice that only the 2-nd, 3-rd,...,(r-s+1)-th rows of the two systems are distinct. Therefore to the 2^r relations determined by B_1, B_2 adds $2^{r-s}-1$ pairing relations. To prove that the column vectors representing these $2^r + 2^{r-s}-1$ relations are linearly independent, we construct the matrix $A_r(B_1 \cup B_2)$ according to the same criterion given at the beginning of the section. Then the proof follows exactly the lines of that of Theorem 4, and is therefore omitted. Q.E.D.

Lemma 5 yields a significant corollary.

<u>Corollary 4</u>: If B_1 and B_2 are two basic clusters of levels

r_1 and r_2 respectively ($r_1 > r_2$), and $s < r_2$ is the level of $B_1 \cap B_2$, the rank of $M(B_1 \cup B_2)$ is $2^{r_1} + 2^{r_2-s} - 1$.

<u>Proof</u>: Let B_2^* be an r_1-th level basic cluster such that $B_2^* \supset B_2$. Since the columns of $M(B_1 \cup B_2^*)$ are linearly independent, so are the columns of $M(B_1 \cup B_2) < M(B_1 \cup B_2^*)$. It is now easy to verify that to the 2^{r_1} conditions required by B_1, B_2 adds $2^{r_2-s} - 1$ pairing relations. Q.E.D.

Given the basic clusters $B_1, B_2, \ldots, B_m$, let D_k denote the join $B_1 \cup B_2 \cup \ldots \cup B_{k-1}$ ($k = 2,3,\ldots,m$). We can now state the following theorem.

<u>Theorem 5</u>: Let $B_1, B_2, \ldots, B_m$ be basic cluster and $r_1 \geq r_2 \geq \ldots \geq r_m$ be their respective levels. If s_j is the level of $D_k \cap B_k$ ($k = 2,3,\ldots,m$), we have

$$\mathrm{rank}\{M(B_1 \cup B_2 \cup \ldots \cup B_m)\} = 2^{r_1} + \sum_{j=2}^{m} (2^{r_j - s_j} - 1). \qquad (8)$$

<u>Proof</u>: If m = 2, corollary 5 reduces to corollary 4 (or lemma 5). If $m > 2$, B_3 only adds the conditions not already required by $B_1 \cup B_2 = D_3$. If s_3 is the level of $D_3 \cap B_3$, B_3 exactly add $2^{r_3-s_3}-1$ new pairing relations: their corresponding vectors are shown, as in Theorem 4, to be linearly independent of the columns of $M(B_1 \cup B_2)$. This argument is then iteratively applied to $B_4, \ldots, B_m$. Q.E.D.

Theorem 5 summarizes all previous partial results, and, since each cluster C is the unique join of a subset of basic independent clusters, it provides a simple formula to compute the rank of the matrix M(C) associated with any given cluster C. It is worth noticing, at this point, that only the levels, and not the order of the clusters participate in the determination of the rank of M(C).

Particular case: It is convenient to compute the rank of M(U), if U is the unity element of the cluster lattice (i.e., for every $C \neq U$, $C \subset U$).

The cluster U contains all n-tuples which are 0 in their most significant position. Every such n-tuple is expressible as a unique concatenation of the (n-1) digit sequences 01, 011,...,01...1. Therefore, letting $B_{n-1} = [0^*(010^*)^*]_n$, $B_{n-2} = [0^*(0110^*)^*]_n, \ldots, B_1 = [0^*(01\ldots1)]_n$, U is obviously given by the relation

$$U = B_1 \cup B_2 \cup \ldots \cup B_{n-1}$$

$B_1, B_2, \ldots, B_{n-1}$ are all of level n-1. We construct now $D_2, D_3, \ldots, D_{n-1}$. The level of $D_2 \cap B_2 = B_1 \cap B_2$ is n-2, of $D_3 \cap B_3$ is n-3, etc. In general, the level of $D_j \cap B_j$ is n-j for j = 2,3,...,n-1. If we now use relation (8) to compute the rank of U, we obtain

$$\text{rank } M(U) = 2^{n-1} + \sum_{j=2}^{n-1} (2^{n-1-n+j} - 1) = 2^n - n$$

M(U) is a $2^n \times (2^n - n)$ matrix.[1]

The definition of M(C) and the analysis of its rank jointly yield the following important result.

Theorem 6: The set of Boolean functions which possess the cluster C as set of RS's is the null space of M(C), i.e., a vector

[1] It is worthwhile mentioning that any function which possesses U induces a resynchronizing point after each 0 of the input sequence.

subspace of dimension $2^n - w$, if w is the rank of M(C).

Theorem 6 provides a solution to the problem of finding all functions which possess a given RS-cluster C. In fact from C we can immediately construct M(C) and from this derive a basis of the vector subspace of the Boolean functions which possess C. Before solving its reciprocal problem we need some simple additional results.

For every $C \neq U$, $M(C) < M(U)$, i.e., a proper subset of the columns of M(U) is column equivalent to M(C). Let v' represent a function which possesses C. It follows that

$$v' \cdot M(C) = 0 \quad .$$

If we now postmultiply v' by M(U) we obtain an (2^n-1)-component vector

$$u(v') = v' \cdot M(U)$$

which, by analogy with a similar concept in the theory of error correcting codes, we call the <u>syndrome</u> of v'. Obviously u(v') is 0 at least in the positions corresponding to the subset of the columns of M(U) which is equivalent to M(C).

We also say that, if u and w are two vectors of the same space over GF(2), u <u>covers</u> w if and only if u has 0's at least in those positions in which w has 0's (i.e., the 0's of w are a subset, proper or improper, of the 0's of u).

Finally, we say that the function <u>v</u>' possesses C as maximal RS-cluster if it does not have any other RS outside C.

With this nomenclature, we can now give a solution to the problem of determining all the RS's of a given function v.

Let $B_1, B_2, \ldots, B_N$ be the basic clusters of order n. With each B_j we associate a (2^n-1)-component syndrome vector u_j which is 0 only in the positions corresponding to the subset of the columns of M(U) which is equivalent to $M(B_j)$. The following theorem follows directly from our definitions.

Theorem 7: A function v' possesses $C = B_{i_1} \cup B_{i_2} \cup \ldots \cup B_{i_k}$ as maximal cluster if and only if u(v') covers only $u_{i_1}, u_{i_2}, \ldots, u_{i_k}$ in the set $u_1, u_2, \ldots, u_N$.

It should be noted that at this point if the test for coverage is carried over the entire set $u_1, u_2, \ldots, u_N$, the selected set $B_{i_1}, B_{i_2}, \ldots, B_{i_k}$ is, in general, not composed of independent basic clusters (in fact any time a high level cluster satisfies the test, the lower level basic clusters it contains necessarily satisfy it). To avoid the selection of a redundant set of B_i's and to reduce the length of the process, the exhaustive "single stage" test, consisting of N comparisons, may be profitably replaced by a more elaborate sequential test. In the latter, by properly choosing the order of the comparisons, and using the knowledge provided by previous comparisons to direct the test, it is possible to obtain a non-redundant set of B_i's in a minimal number of steps (on the average, considerably smaller than N). This subject, however, although formally elegant, will not be analyzed in this paper.

V. Final Remarks - Conclusion

At the end of Section II, we showed that finite-memory non-feedback decoding is feasible only if the input sequence $\{x\}$ is composed or irreducible subsequences of bounded length. This, it was noted, imposes a definite constraint on the symbol generating source, in the sense that some interdependence is established between consecutive symbols of $\{x\}$ if the source is to match the adopted decoder.

This constraint can be expressed in a quantitative form in terms of the entropy loss per generated symbol (in bit/digit). A preliminary study has been conducted in which relations have been established between the selected RS-cluster, the decoder length and the source entropy. Although a deeper analysis is felt necessary it appears that for a reasonable number $\underline{r}$ of stages of the decoder ($4n < r < 10n$) the entropy loss becomes negligible. From a different point of view, it seems possible to evaluate the error rate if an unconstrained sequence is decoded by a finite-memeory device. These preliminary results, however, because of their incompleteness and for the sake of brevity, are not reported in the present paper.

As regards the circuit implementation of the decoding process, it appears convenit to illustrate in Fig. 6 a realization of the finite-memory decoder which is possible if the clock rate is uniform and the required circuit speed is attainable. Each time unit, of constant duration, is subdivided into (r+1) intervals, identified by a set of periodic timing signals $\tau_0, \tau_1, \ldots, \tau_r$, with period equal to the time unit. The symbol y_s is entered into the decoder at time τ_0 and the decoded x_s is emitted at time τ_r.

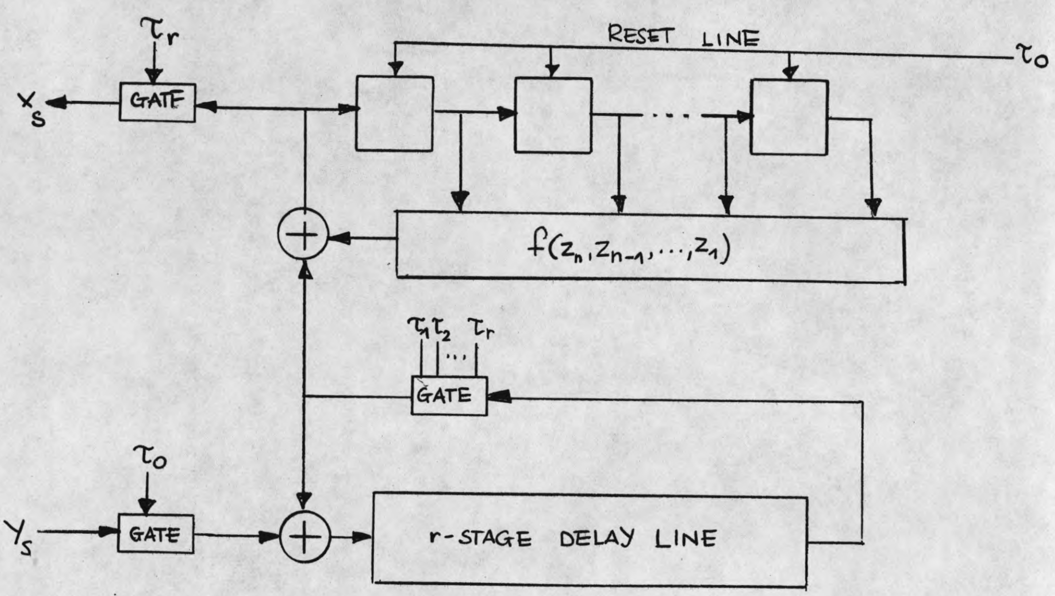

Fig. 6. A Realization of a Finite-Memory Non-Feedback Decoder.

The inclusion of the n-stage feedback shift-register as a portion of the decoder should not be misleading to the reader. The decoder, in its entirety, is in fact without feedback: the feedback shift-register, which is reset to 0 any time a new symbol of $\{y\}$ is received, only performs an iterative operation on digits contained in the r-stage delay line. In this way erroneous symbols of $\{y\}$ will produce erroneous symbols of the decoded $\{x\}$ only as long as they are contained in the delay line. It is therefore evident that a single error on the $\{y\}$ sequence may affect at most r consecutive digits of the $\{x\}$ sequence.

The reasonable simplicity of implementation of sequence transformations by means of finite-memory non-feedback shift-registers appears as a sufficient motivation of interest. The theoretical analysis given in the previous section provides a formal tool for the selection of the numbers n and r of encoder and decoder stages, respectively, and, as the need may be, of adequately wide classes of transformations possessing "good" resynchronizing properties. It is felt that further analysis may show a useful formal connection between choices of RS-clusters and constraints on the input sequences.

References

1. D. A. Huffman, "Canonical Forms for Information-Lossless Finite-State Logical Machines," IRE Trans. on Circuit Theory, Vol. CT-6, Special Supplement, pp. 41-59; May, 1959.

2. W. L. Parker and B. A. Berstein, "On Uniquely Solvable Boolean Equations," Univ. of Calif. Publ. in Math., New Series, Vol. 3, No. 1, pp. 1-30; 1955.

3. J. Massey and R. Liu, "Application of Lyapunov's Direct Method to the Error-Propagation Effect in Convolutional Codes," IEEE Trans. on Information Theory (correspondence), Vol. IT-10, pp. 248-250; July, 1964.

4. J. A. Brzozowski, "A Survey of Regular Expressions and Their Applications," IRE Trans. on Electronic Computers, Vol. EC-11, No. 3, pp. 324-355; June, 1962.

5. G. Birkhoff, "Lattice Theory," American Mathematical Society, Providence, R.I., 1961.

6. G. Birkhoff and S. MacLane, A Survey of Modern Algebra, MacMillan, New York, N.Y.; 1961.

7. F. P. Preparata, "State-Logic Relations for Autonomous Sequential Networks," IEEE Trans. on Electronic Computers, Vol. EC-13, No. 5, pp. 542-548; October, 1964.

8. E. J. Good, "Normal Recurring Decimals," J. London Math. Soc., Vol. 21, Pt. 3, pp. 167-169; 1946.

Acknowledgment

The author acknowledges with gratitude the valuable comments and criticism of G. Metze, R. T. Chien and other colleagues at the Coordinated Science Laboratory. This work was initiated before the tragic death of Professor S. Seshu, whose helpful guide was of extreme value to the author.

Distribution list as of March 1, 1965

1 Dr. Chalmers Sherwin
Deputy Director (Research & Technology)
DD&RE Rm 3E1060
The Pentagon
Washington, D. C. 20301

1 Dr. Edward M. Reilley
Asst. Director (Research)
Ofc. of Defense Res & Eng
Department of Defense
Washington, D. C. 20301

1 Dr. James A. Ward
Office of Deputy Director (Research and Information Rm 3D1037)
Department of Defense
The Pentagon
Washington, D. C. 20301

1 Director
Advanced Research Projects Agency
Department of Defense
Washington, D. C. 20301

1 Mr. Charles Yost, Director
for Materials Sciences
Advanced Research Projects Agency
Department of Defense
Washington, D. C. 20301

20 Defense Documentation Center
Cameron Station, Bldg. 5
Alexandria, Virginia 22314
Attn: TISIA

1 Director
National Security Agency
Fort George G. Meade, Maryland 20755
Attn: Librarian C-332

1 Chief of Research and Development
Headquarters, Department of the Army
Washington, D. C. 20310
Attn: Physical Sciences Division P & E

1 Chief of Research and Development
Headquarters, Department of the Army
Washington, D. C. 20310
Attn: Mr. L. H. Geiger, Rm 34442

1 Research Plans Office
U. S. Army Research Office
3045 Columbia Pike
Arlington, Virginia 22204

1 Commanding General
U. S. Army Materiel Command
Attn: AMCRD-RS-PE-E
Washington, D. C. 20315

1 Commanding General
U. S. Army Strategic Communications Command
Washington, D. C. 20315

1 Commanding Officer
U. S. Army Materials Research Agency
Watertown Arsenal
Watertown, Massachusetts 02172

1 Commanding Officer
U. S. Army Ballistics Research Lab.
Aberdeen Proving Ground
Aberdeen, Maryland 21005
Attn: V. W. Richards

1 Commanding Officer
U. S. Army Ballistics Research Lab.
Aberdeen Proving Ground
Aberdeen, Maryland 21005
Attn: Keats A. Pullen, Jr.

1 Commanding Officer
U. S. Army Ballistics Research Lab.
Aberdeen Proving Ground
Aberdeen, Maryland 21005
Attn: George C. Francis, Computing Lab.

1 Commandant
U. S. Army Air Defense School
P. O. Box 9390
Fort Bliss, Texas 79916
Attn: Missile Sciences Div., C&S Dept.

1 Commanding General
U. S. Army Missile Command
Redstone Arsenal, Alabama 35809
Attn: Technical Library

1 Commanding General
Frankford Arsenal
Philadelphia, Pa. 19137
Attn: SMUFA-1310 (Dr. Sidney Ross)

1 Commanding General
Frankford Arsenal
Philadelphia, Pa. 19137
Attn: SMUFA-1300

1 U. S. Army Munitions Command
Picatinney Arsenal
Dover, New Jersey 07801
Attn: Technical Information Branch

1 Commanding Officer
Harry Diamond Laboratories
Connecticut Ave. & Van Ness St., N.W.
Washington, D. C. 20438
Attn: Mr. Berthold Altman

1 Commanding Officer
Harry Diamond Laboratories
Attn: Library
Connecticut Ave. & Van Ness St., N.W.
Washington, D. C. 20438

1 Commanding Officer
U. S. Army Security Agency
Arlington Hall
Arlington, Virginia 22212

1 Commanding Officer
U. S. Army Limited War Laboratory
Aberdeen Proving Ground
Aberdeen, Maryland 21005
Attn: Technical Director

1 Commanding Officer
Human Engineering Laboratories
Aberdeen Proving Ground, Maryland 21005

1 Director
U. S. Army EngineerGeodesy, Intelligence and Mapping, Research & Devel. Agency
Fort Belvoir, Virginia 22060

1 Commandant
U. S. Army Command and General Staff College
Fort Leavenworth, Kansas 66207
Attn: Secretary

1 Dr. H. Robl, Deputy Director
U. S. Army Research Office (Durham)
Box CM, Duke Station
Durham, North Carolina 27706

1 Commanding Officer
U. S. Army Research Office (Durham)
P. O. Box CM, Duke Station
Durham, North Carolina 27706
Attn: CRD-AA-IP (Richard O. Ulsh)

1 Commanding General
U. S. Army Electronics Command
Fort Monmouth, New Jersey 07703
Attn: AMSEL-SC

1 Director
U. S. Army Electronics Laboratories
Fort Monmouth, New Jersey 07703
Attn: Dr. S. Benedict Levin, Director
Institute for Exploratory Research

1 Director
U. S. Army Electronics Laboratories
Fort Monmouth, New Jersey 07703
Attn: Mr. Robert O. Parker, Executive
Secretary, JSTAC (AMSEL-RD-X)

1 Superintendent
U. S. Military Academy
West Point, New York 10996

1 The Walter Reed Institute of Research
Walter Reed Army Medical Center
Washington, D. C. 20012

1 Director
U. S. Army Electronics Laboratories
Fort Monmouth, New Jersey 07703
Attn: AMSEL-RD-DR

1 Director
U. S. Army Electronics Laboratories
Attn: AMSEL-RD-X
Fort Monmouth, New Jersey 07703

1 Director
U. S. Army Electronics Laboratories
Fort Monmouth, New Jersey 07703
Attn: AMSEL-RD-XE

1 Director
U. S. Army Electronics Laboratories
Fort Monmouth, New Jersey 07703
Attn: AMSEL-RD-XC

1 Director
U. S. Army Electronics Laboratories
Fort Monmouth, New Jersey 07703
Attn: AMSEL-RD-XS

1 Director
U. S. Army Electronics Laboratories
Fort Monmouth, New Jersey 07703
Attn: AMSEL-RD-NR

1 Director
U. S. Army Electronics Laboratories
Fort Monmouth, New Jersey 07703
Attn: AMSEL-RD-NE

1 Director
U. S. Army Electronics Laboratories
Fort Monmouth, New Jersey 07703
Attn: AMSEL-RD-NO

1 Director
U. S. Army Electronics Laboratories
Fort Monmouth, New Jersey 07703
Attn: AMSEL-RD-NP

1 Director
U. S. Army Electronics Laboratories
Fort Monmouth, New Jersey 07703
Attn: AMSEL-RD-SA

1 Director
U. S. Army Electronics Laboratories
Fort Monmouth, New Jersey 07703
Attn: AMSEL-RD-SE

1 Director
U. S. Army Electronics Laboratories
Fort Monmouth, New Jersey 07703
Attn: AMSEL-RD-SR

1 Director
U. S. Army Electronics Laboratories
Fort Monmouth, New Jersey 07703
Attn: AMSEL-RD-SS

1 Director
U. S. Army Electronics Laboratories
Fort Monmouth, New Jersey 07703
Attn: AMSEL-RD-PE

1 Director
U. S. Army Electronics Laboratories
Fort Monmouth, New Jersey 07703
Attn: AMSEL-RD-PF

1 Director
U. S. Army Electronics Laboratories
Fort Monmouth, New Jersey 07703
Attn: AMSEL-RD-PR

1 Director
U. S. Army Electronics Laboratories
Fort Monmouth, New Jersey 07703
Attn: * AMSEL-RL-GF

1 Director
U. S. Army Electronics Laboratories
Fort Monmouth, New Jersey 07703
Attn: AMSEL-RD-ADT

1 Director
U. S. Army Electronics Laboratories
Fort Monmouth, New Jersey 07703
Attn: AMSEL-RD-FU#1

1 Commanding Officer
U. S. Army Electronics R&D Activity
Fort Huachuca, Arizona 85163

1 Commanding Officer
U. S. Army Engineers R&D Laboratory
Fort Belvoir, Virginia 22060
Attn: STINFO Branch

1 Commanding Officer
U. S. Army Electronics R&D Activity
White Sands Missile Range
New Mexico 88002

1 Director
Human Resources Research Office
The George Washington University
300 N. Washington Street
Alexandria, Virginia

1 Commanding Officer
U. S. Army Personnel Research Office
Washington 25, D. C.

1 Commanding Officer
U. S. Army Medical Research Laboratory
Fort Knox, Kentucky

1 Commanding General
U. S. Army Signal Center and School
Attn: Chief, Office of Academic Operations
Fort Monmouth, New Jersey 07703

2 Dr. Richard H. Wilcox, Code 437
Department of the Navy
Washington, D. C. 20360

1 Chief, Bureau of Weapons
Attn: Technical Library, DL1-3
Department of the Navy
Washington, D. C. 20360

1 Chief, Bureau of Ships
Department of the Navy
Washington, D. C. 20360
Attn: Code 680

1 Chief, Bureau of Ships
Department of the Navy
Washington, D. C. 20360
Attn: Code 732

1 Commander
U. S. Naval Air Development Center
Johnsville, Pennsylvania
Attn: NADC Library

1 Commanding Officer
Naval Electronics Laboratory
San Diego, California 92052
Attn: Code 2222(Library)

1 Commanding Officer
Naval Electronics Laboratory
San Diego, California 92052
Attn: Code 2800, C. S. Manning

1 Commanding Officer and Director
(Code 142 Library)
David W. Taylor Model Basin
Washington, D. C. 20007

6 Director
Naval Research Laboratory
Washington, D. C. 20390
Attn: Technical Information Office
(Code 2000)

1 Commanding Officer
Office of Naval Research Branch Office
219 S. Dearborn Street
Chicago, Illinois 60604

1 Chief of Naval Operations
Department of the Navy
Washington, D. C. 20350
Attn: OP-07T

1 Chief of Naval Operations
Department of the Navy
Washington, D. C. 20350
Attn: OP-03EG

1 Commanding Officer
Office of Naval Research Branch Office
1000 Geary Street
San Francisco, California 94109

1 Commanding Officer
U. S. Naval Weapons Laboratory
Asst. Director for Computation
Dahlgren, Virginia 22448
Attn: G. H. Gleissner (Code K-4)

1 Inspector of Naval Material
Bureau of Ships Technical Representative
1902 West Minnehaha Avenue
St. Paul 4, Minnesota

5 Lt. Col. E. T. Gaines, SREE
Chief, Electronics Division
Directorate of Engineering Sciences
Air Force Office of Scientific Research
Washington, D. C. 20333

1 Director of Science & Technology
Deputy Chief of Staff (R & D)
USAF
Washington, D. C.
Attn: AFRST-EL/GU

1 Director of Science & Technology
Deputy Chief of Staff (R & D)
USAF
Washington, D. C.
Attn: AFRST-SC

1 Karl M. Fuechsel
Electronics Division
Director of Engineering Sciences
Air Force Office of Scientific Research
Washington, D. C. 20333

1 Lt. Col. Edwin M. Myers
Headquarters, USAF (AFRDR)
Washington 25, D. C.

1 Director, Air University Library
Maxwell Air Force Base
Alabama 36112
Attn: CR-4803a

1 Commander
Research & Technology Division
AFSC (Mr. Robert L. Feik)
Office of the Scientific Director
Bolling AFB 25, D. C.

1 Commander
Research & Technology Division
Office of the Scientific Director
Bolling AFB 25, D. C.
Attn: RTHR

1 Commander
Air Force Cambridge Research Laboratories
Attn: Research Library
CRMXL-R
L. G. Hanscom Field
Bedford, Massachusetts 01731

1 Dr. Lloyd Hollingsworth
AFCRL
L. G. Hanscom Field
Bedford, Massachusetts 01731

1 Commander
Air Force Cambridge Research Laboratories
Attn: Data Sciences Lab
(Lt. S. J. Kahne, CRB)
L. G. Hanscom Field
Bedford, Massachusetts 01731

1 Commander
Air Force Systems Command
Office of the Chief Scientist
(Mr. A. G. Wimer)
Andrews AFB, Maryland 20331

1 Commander
Air Force Missile Development Center
Attn: MDSGO/Major Harold Wheeler, Jr.
Holloman Air Force Base, New Mexico

1 Commander
Research & Technology Division
Attn: MAYT (Mr. Evans)
Wright-Patterson Air Force Base
Ohio 45433

1 Directorate of Systems Dynamics Analysis
Aeronautical Systems Division
Wright-Patterson AFB, Ohio 45433

1 Hqs. Aeronautical Systems Division
AF Systems Command
Attn: Navigation & Guidance Laboratory
Wright-Patterson AFB, Ohio 45433

1 Commander
Rome Air Development Center
Attn: Documents Library, RAALD
Griffiss Air Force Base
Rome, New York 13442

1 Commander
Rome Air Development Center
Attn: RAWI-Major W. H. Harris
Griffiss Air Force Base
Rome, New York 13442

1 Lincoln Laboratory
Massachusetts Institute of Technology
P. O. Box 73
Lexington 73, Massachusetts
Attn: Library A-082

Continued next page

Distribution list as of March 1, 1965 (Cont'd.)

1 Lincoln Laboratory
Massachusetts Institute of Technology
P. O. Box 73
Lexington 73, Massachusetts
Attn: Dr. Robert Kingston

1 APGC (PGAPI)
Eglin Air Force Base
Florida

1 Mr. Alan Barnum
Rome Air Development Center
Griffiss Air Force Base
Rome, New York 13442

1 Director
Research Laboratory of Electronics
Massachusetts Institute of Technology
Cambridge, Massachusetts 02139

1 Polytechnic Institute of Brooklyn
55 Johnson Street
Brooklyn, New York 11201
Attn: Mr. Jerome Fox
Research Coordinator

1 Director
Columbia Radiation Laboratory
Columbia University
538 West 120th Street
New York, New York 10027

1 Director
Coordinated Science Laboratory
University of Illinois
Urbana, Illinois 61803

1 Director
Stanford Electronics Laboratories
Stanford University
Stanford, California

1 Director
Electronics Research Laboratory
University of California
Berkeley 4, California

1 Professor A. A. Dougal, Director
Laboratories for Electronics and Related
Science Research
University of Texas
Austin, Texas 78712

1 Professor J. K. Aggarwal
Department of Electrical Engineering
University of Texas
Austin, Texas 78712

1 Director of Engineering & Applied Physics
210 Pierce Hall
Harvard University
Cambridge, Massachusetts 02138

1 Capt. Paul Johnson (USN Ret.)
National Aeronautics & Space Agency
1520 H. Street, N. W.
Washington 25, D. C.

1 NASA Headquarters
Office of Applications
400 Maryland Avenue, S.Q.
Washington 25, D. C.
Attn: Code FC Mr. A. M. Greg Andrus

1 National Bureau of Standards
Research Information Center and Advisory
Serv. on Info. Processing
Data Processing Systems Division
Washington 25, D. C.

1 Dr. Wallace Sinaiko
Institute for Defense Analyses
Research & Eng. Support Div.
1666 Connecticut Avenue, N. W.
Washington 9, D. C.

1 Data Processing Systems Division
National Bureau of Standards
Conn. at Van Ness
Room 239, Bldg. 10
Washington 25, D. C.
Attn: A. K. Smilow

1 Exchange and Gift Division
The Library of Congress
Washington 25, D. C.

1 Dr. Alan T. Waterman, Director
National Science Foundation
Washington 25, D. C.

1 H. E. Cochran
Oak Ridge National Laboratory
P. O. Box X
Oak Ridge, Tennessee

1 U. S. Atomic Energy Commission
Office of Technical Information Extension
P. O. Box 62
Oak Ridge, Tennessee

1 Mr. G. D. Watson
Defense Research Member
Canadian Joint Staff
2450 Massachusetts Avenue, N. W.
Washington 8, D. C.

1 Martin Company
P. O. Box 5837
Orlando, Florida
Attn: Engineering Library MP-30

1 Laboratories for Applied Sciences
University of Chicago
6220 South Drexel
Chicago, Illinois 60637

1 Librarian
School of Electrical Engineering
Purdue University
Lafayette, Indiana

1 Donald L. Epley
Dept. of Electrical Engineering
State University of Iowa
Iowa City, Iowa

1 Instrumentation Laboratory
Massachusetts Institute of Technology
68 Albany Street
Cambridge 39, Massachusetts
Attn: Library WI-109

1 Sylvania Electric Products, Inc.
Electronics System
Waltham Labs. Library
100 First Avenue
Waltham 54, Massachusetts

2 Hughes Aircraft Company
Centinela and Teale Streets
Culver City, California
Attn: K. C. Rosenberg, Supervisor
Company Technical Document Center

3 Autonetics
9150 East Imperial Highway
Downey, California
Attn: Tech. Library, 3041-11

1 Dr. Arnold T. Nordsieck
General Motors Corporation
Defense Research Laboratories
6767 Hollister Avenue
Goleta, California

1 University of California
Lawrence Radiation Laboratory
P. O. Box 808
Livermore, California

1 Mr. Thomas L. Hartwick
Aerospace Corporation
P. O. Box 95085
Los Angeles 45, California

1 Lt. Col. Willard Levin
Aerospace Corporation
P. O. Box 95085
Los Angeles 45, California

1 Sylvania Electronic Systems-West
Electronic Defense Laboratories
P. O. Box 205
Mountain View, California
Attn: Documents Center

1 Varian Associates
611 Hansen Way
Palo Alto, California 94303
Attn: Tech. Library

1 Huston Denslow
Library Supervisor
Jet Propulsion Laboratory
California Institute of Technology
Pasadena, California

1 Professor Nicholas George
California Institute of Technology
Electrical Engineering Department
Pasadena, California

1 Space Technology Labs., Inc.
One Space Park
Redondo Beach, California
Attn: Acquisitions Group
STL Technical Library

1 The Rand Corporation
1700 Main Street
Santa Monica, California
Attn: Library

1 Miss F. Cloak
Radio Corp. of America
RCA Laboratories
David Sarnoff Research Center
Princeton, New Jersey

1 Mr. A. A. Lundstrom
Bell Telephone Laboratories
Room 2E-127
Whippany Road
Whippany, New Jersey

1 Cornell Aeronautical Laboratory, Inc.
4455 Genesee Street
Buffalo 21, New York
Attn: J. P. Desmond, Librarian

1 Sperry Gyroscope Company
Marine Division Library
155 Glenn Cove Road
Carle Place, L. I., New York
Attn: Miss Barbara Judd

1 Library
Light Military Electronics Dept.
General Electric Company
Armament & Control Products Section
Johnson City, New York

1 Dr. E. Howard Holt
Director
Plasma Research Laboratory
Rennselaer Polytechnic Institute
Troy, New York

1 Battele-DEFENDER
Battelle Memorial Institute
505 King Avenue
Columbus 1, Ohio

1 Laboratory for Electroscience Research
New York University
University Heights
Bronx 53, New York

1 National Physical Laboratory
Teddington, Middlesex
England
Attn: Dr. A. M. Uttley, Superintendent,
Autonomics Division

1 Dr. Lee Huff
Behavioral Sciences
Advanced Research Projects Agency
The Pentagon (Room 3E175)
Washington, D. C. 20301

1 Dr. Glenn L. Bryan
Head, Personnel and Training Branch
Office of Naval Research
Navy Department
Washington, D. C. 20360

1 Instituto de Fisica Aplicado
"L. Torres Quevedo"
High Vacuum Laboratory
Madrid, Spain
Attn: Jose L. de Segovia

1 Stanford Research Institute
Attn: G-037 External Reports
(for J. Goldberg)
Menlo Park, California 94025

REVISED U. S. ARMY DISTRIBUTION LIST

(As received at the Coordinated Science Laboratory 27 July 1965)

1 Dr. Chalmers Sherwin
Deputy Director (Research & Technology)
DD&RE Rm 3E1060
The Pentagon
Washington, D. C. 20301

1 Dr. Edward M. Reilley
Asst. Director (Research)
Ofc. of Defense Res. & Eng.
Department of Defense
Washington, D. C. 20301

1 Dr. James A. Ward
Office of Deputy Director (Research and Information Rm 3D1037)
Department of Defense
The Pentagon
Washington, D. C. 20301

1 Director
Advanced Research Projects Agency
Department of Defense
Washington, D. C. 20301

1 Mr. E. I. Salkovitz, Director for Materials Sciences
Advanced Research Projects Agency
Department of Defense
Washington, D. C. 20301

1 Colonel Charles C. Mack
Headquarters
Defense Communications Agency (333)
The Pentagon
Washington, D. C. 20305

20 Defense Documentation Center
Attn: TISIA
Cameron Station, Building 5
Alexandria, Virginia 22314

1 Director
National Security Agency
Attn: Librarian C-332
Fort George G. Meade, Maryland 20755

1 U. S. Army Research Office
Attn: Physical Sciences Division
3045 Columbia Pike
Arlington, Virginia 22204

1 Chief of Research and Development
Headquarters, Department of the Army
Attn: Mr. L. H. Geiger, Rm 3D442
Washington, D. C. 20310

1 Research Plans Office
U. S. Army Research Office
3045 Columbia Pike
Arlington, Virginia 22204

1 Commanding General
U. S. Army Materiel Command
Attn: AMCRD-RS-PE-E
Washington, D. C. 20315

1 Commanding General
U. S. Army Strategic Communications Command
Washington, D. C. 20315

1 Commanding Officer
U. S. Army Materials Research Agency
Watertown Arsenal
Watertown, Massachusetts 02172

1 Commanding Officer
U. S. Army Ballistics Research Laboratory
Attn: V. W. Richards
Aberdeen Proving Ground
Aberdeen, Maryland 21005

1 Commanding Officer
U. S. Army Ballistics Research Laboratory
Attn: Keats A. Pullen, Jr.
Aberdeen Proving Ground
Aberdeen, Maryland 21005

1 Commanding Officer
U. S. Army Ballistics Research Laboratory
Attn: George C. Francis, Computing Lab.
Aberdeen Proving Ground, Maryland 21005

1 Commandant
U. S. Army Air Defense School
Attn: Missile Sciences Division, C&S Dept.
P. O. Box 9390
Fort Bliss, Texas 79916

1 Commanding General
U. S. Army Missile Command
Attn: Technical Library
Redstone Arsenal, Alabama 35809

1 Commanding General
Frankford Arsenal
Attn: SMUFA-1310 (Dr. Sidney Ross)
Philadelphia, Pennsylvania 19137

1 Commanding General
Frankford Arsenal
Attn: SMUFA-1300
Philadelphia, Pennsylvania 19137

1 U. S. Army Munitions Command
Attn: Technical Information Branch
Picatinney Arsenal
Dover, New Jersey 07801

1 Commanding Officer
Harry Diamond Laboratories
Attn: Mr. Berthold Altman
Connecticut Avenue and Van Ness St.,N.W.
Washington, D. C. 20438

1 Commanding Officer
Harry Diamond Laboratories
Attn: Library
Connecticut Avenue and Van Ness St.,N.W.
Washington, D. C. 20438

1 Commanding Officer
U. S. Army Security Agency
Arlington Hall
Arlington, Virginia 22212

1 Commanding Officer
U. S. Army Limited War Laboratory
Attn: Technical Director
Aberdeen Proving Ground
Aberdeen, Maryland 21005

1 Commanding Officer
Human Engineering Laboratories
Aberdeen Proving Ground, Maryland 21005

1 Director
U. S. Army Engineer Geodesy, Intelligence & Mapping
Research and Development Agency
Fort Belvoir, Virginia 22060

1 Commandant
U. S. Army Command and General Staff College
Attn: Secretary
Fort Leavenworth, Kansas 66207

1 Dr. H. Robl, Deputy Chief Scientist
U. S. Army Research Office (Durham)
Box CM, Duke Station
Durham, North Carolina 27706

1 Commanding Officer
U. S. Army Research Office (Durham)
Attn: CRD-AA-IP (Richard O. Ulsh)
Box CM, Duke Station
Durham, North Carolina 27706

1 Superintendent
U. S. Army Military Academy
West Point, New York 10996

1 The Walter Reed Institute of Research
Walter Reed Army Medical Center
Washington, D. C. 20012

1 Commanding Officer
U. S. Army Electronics R&D Activity
Fort Huachuca, Arizona 85163

1 Commanding Officer
U. S. Army Engineers R&D Laboratory
Attn: STINFO Branch
Fort Belvoir, Virginia 22060

1 Commanding Officer
U. S. Army Electronics R&D Activity
White Sands Missile Range, New Mexico 88002

1 Director
Human Resources Research Office
The George Washington University
300 N. Washington Street
Alexandria, Virginia 22300

1 Commanding Officer
U. S. Army Personnel Research Office
Washington, D. C.

1 Commanding Officer
U. S. Army Medical Research Laboratory
Fort Knox, Kentucky 40120

1 Commanding General
U. S. Army Signal Center and School
Fort Monmouth, New Jersey 07703
Attn: Chief, Office of Academic Operations

1 Dr. S. Benedict Levin, Director
Institute for Exploratory Research
U. S. Army Electronics Command
Fort Monmouth, New Jersey 07703

1 Director
Institute for Exploratory Research
U. S. Army Electronics Command
Attn: Mr. Robert O. Parker, Executive Secretary, JSTAC (AMSEL-XL-D)
Fort Monmouth, New Jersey 07703

1 Commanding General
U. S. Army Electronics Command
Fort Monmouth, New Jersey 07703

Attn: AMSEL-SC
RD-D
RD-G
RD-MAF-I
RD-MAT
RD-GF
RD-MN (Marine Corps LnO)
XL-D
XL-E
XL-C
XL-S
HL-D
HL-L
HL-J
HL-P
HL-O
HL-R
NL-D
NL-A
NL-P
NL-R
NL-S
KL-D
KL-E
KL-S
KL-T
VL-D
WL-D

1 Mr. Charles F. Yost
Special Assistant to the Director of Research
National Aeronautics & Space Admin.
Washington, D. C. 20546

1 Director
Research Laboratory of Electronics
Massachusetts Institute of Technology
Cambridge, Massachusetts 02139

1 Polytechnic Institute of Brooklyn
55 Johnson Street
Brooklyn, New York 11201
Attn: Mr. Jerome Fox
Research Coordinator

1 Director
Columbia Radiation Laboratory
Columbia University
538 West 120th Street
New York, New York 10027

1 Director
Stanford Electronics Laboratories
Stanford University
Stanford, California 94301

1 Director
Electronics Research Laboratory
University of California
Berkeley, California 94700

1 Director
Electronic Sciences Laboratory
University of Southern California
Los Angeles, California 90007

1 Professor A. A. Dougal, Director
Laboratories for Electronics and Related Science Research
University of Texas
Austin, Texas 78712

1 Professor J. K. Aggarwal
Department of Electrical Engineering
University of Texas
Austin, Texas 78712

1 Division of Engineering and Applied Physics
210 Pierce Hall
Harvard University
Cambridge, Massachusetts 02138

Security Classification

DOCUMENT CONTROL DATA R&D

(Security classification of title, body of abstract and indexing annotation must be entered when the overall report is classified)

1. ORIGINATING ACTIVITY (Corporate author) University of Illinois Coordinated Science Laboratory Urbana, Illinois 61801	2a. REPORT SECURITY CLASSIFICATION Unclassified 2b. GROUP
3. REPORT TITLE CONVOLUTIONAL TRANSFORMATIONS OF BINARY SEQUENCES: BOOLEAN FUNCTIONS AND THEIR RESYNCHRONIZING PROPERTIES	
4. DESCRIPTIVE NOTES (Type of report and inclusive dates)	
5. AUTHOR(S) (Last name, first name, initial) Preparata, Franco P.	

6. REPORT DATE	7a TOTAL NO. OF PAGES	7b. NO. OF REFS.
March, 1966	36	8
8a. CONTRACT OR GRANT NO. DA 28 043 AMC 00073(E) b. PROJECT NO. 20014501B31F c. d.	9a. ORIGINATOR'S REPORT NUMBER(S) R-283 9b. OTHER REPORT NO(S) (Any other numbers that may be assigned this report)	

10. AVAILABILITY/LIMITATION NOTICES

Qualified requesters may obtain copies of this report from DDC. This report may be released to OTS.

11. SUPPLEMENTARY NOTES	12. SPONSORING MILITARY ACTIVITY
	U. S. Army Electronics Command Fort Monmouth, New Jersey 07703

13. ABSTRACT

Non-feedback shift registers (finite-memory encoders) can be profitably adopted to perform transformations of binary sequences. The output sequence is convolutionally obtained by "sliding" the encoding device along the input sequence and producing a symbol at each shift. Invertible transformations are characterized and decoding schemes are analyzed. The crucial point in the decoding problem is that the simply finite-memory feedback decoder presents the undesirable well-known error propagation effect, while the non-feedback decoder contains, in general, an indefinite number of stages. Finite-memory non-feedback decoding is feasible, however, if some constraint is imposed on the input sequences, or, equivalently, if some decoding error is tolerated. The analysis is conducted through the concepts of resynchronizing states of Boolean functions. The algebraic properties of resynchronizing states are carefully analyzed; it is shown that they can be assigned only in special sets, termed clusters, which form a lattice. Moreover, each cluster of resynchronizing states is possessed by a set of Boolean functions, which form a subspace of the vector space of all Boolean functions. The presented analysis provides a formal tool to relate finite-memory non-feedback decoding to the constraint imposed on the input generating source.

DD FORM 1 JAN 64 1473

Security Classification

Security Classification

KEY WORDS	LINK A		LINK B		LINK C	
	ROLE	WT	ROLE	WT	ROLE	WT
convolutional transformations						
binary sequences						
Boolean functions						
resynchronizing						

INSTRUCTIONS

1. ORIGINATING ACTIVITY: Enter the name and address of the contractor, subcontractor, grantee, Department of Defense activity or other organization (corporate author) issuing the report.

2a. REPORT SECURITY CLASSIFICATION: Enter the overall security classification of the report. Indicate whether "Restricted Data" is included. Marking is to be in accordance with appropriate security regulations.

2b. GROUP: Automatic downgrading is specified in DoD Directive 5200.10 and Armed Forces Industrial Manual. Enter the group number. Also, when applicable, show that optional markings have been used for Group 3 and Group 4 as authorized.

3. REPORT TITLE: Enter the complete report title in all capital letters. Titles in all cases should be unclassified. If a meaningful title cannot be selected without classification, show title classification in all capitals in parenthesis immediately following the title.

4. DESCRIPTIVE NOTES: If appropriate, enter the type of report, e.g., interim, progress, summary, annual, or final. Give the inclusive dates when a specific reporting period is covered.

5. AUTHOR(S): Enter the name(s) of author(s) as shown on or in the report. Enter last name, first name, middle initial. If military, show rank and branch of service. The name of the principal author is an absolute minimum requirement.

6. REPORT DATE: Enter the date of the report as day, month, year; or month, year. If more than one date appears on the report, use date of publication.

7a. TOTAL NUMBER OF PAGES: The total page count should follow normal pagination procedures, i.e., enter the number of pages containing information.

7b. NUMBER OF REFERENCES: Enter the total number of references cited in the report.

8a. CONTRACT OR GRANT NUMBER: If appropriate, enter the applicable number of the contract or grant under which the report was written.

8b, 8c, & 8d. PROJECT NUMBER: Enter the appropriate military department identification, such as project number, subproject number, system numbers, task number, etc.

9a. ORIGINATOR'S REPORT NUMBER(S): Enter the official report number by which the document will be identified and controlled by the originating activity. This number must be unique to this report.

9b. OTHER REPORT NUMBER(S): If the report has been assigned any other report numbers (either by the originator or by the sponsor), also enter this number(s).

10. AVAILABILITY/LIMITATION NOTICES: Enter any limitations on further dissemination of the report, other than those imposed by security classification, using standard statements such as:

(1) "Qualified requesters may obtain copies of this report from DDC."

(2) "Foreign announcement and dissemination of this report by DDC is not authorized."

(3) "U. S. Government agencies may obtain copies of this report directly from DDC. Other qualified DDC users shall request through

______________________________."

(4) "U. S. military agencies may obtain copies of this report directly from DDC. Other qualified users shall request through

______________________________."

(5) "All distribution of this report is controlled. Qualified DDC users shall request through

______________________________."

If the report has been furnished to the Office of Technical Services, Department of Commerce, for sale to the public, indicate this fact and enter the price, if known.

11. SUPPLEMENTARY NOTES: Use for additional explanatory notes.

12. SPONSORING MILITARY ACTIVITY: Enter the name of the departmental project office or laboratory sponsoring (paying for) the research and development. Include address.

13. ABSTRACT: Enter an abstract giving a brief and factual summary of the document indicative of the report, even though it may also appear elsewhere in the body of the technical report. If additional space is required, a continuation sheet shall be attached.

It is highly desirable that the abstract of classified reports be unclassified. Each paragraph of the abstract shall end with an indication of the military security classification of the information in the paragraph, represented as (TS), (S), (C), or (U).

There is no limitation on the length of the abstract. However, the suggested length is from 150 to 225 words.

14. KEY WORDS: Key words are technically meaningful terms or short phrases that characterize a report and may be used as index entries for cataloging the report. Key words must be selected so that no security classification is required. Identifiers, such as equipment model designation, trade name, military project code name, geographic location, may be used as key words but will be followed by an indication of technical context. The assignment of links, roles, and weights is optional.