IX. PROCESSING AND TRANSMISSION OF INFORMATION*

Prof. P. Elias
Prof. R. M. Fano
Prof. D. A. Huffman
Prof. C. E. Shannon
Dr. M. V. Cerrillo
W. G. Breckenridge
E. Ferretti
K. Joannou
R. M. Lerner
J. B. O'Loughlin
L. S. Onyshkevych
A. J. Osborne
W. W. Peterson
E. T. Schoen
F. F. Tung
S. H. Unger
M. L. Wetherell
J. M. Wozencraft
W. A. Youngblood

A. ROW ASSIGNMENTS IN SEQUENTIAL SWITCHING CIRUCITS

The terminal characteristics of asynchronous sequential switching circuits can be specified by means of flow tables (1). In an analogous manner, the external behavior of synchronous (or clocked) sequential circuits can be described by means of similar tables (2, 3), as shown in Fig. IX-1.

A general synthesis procedure for either circuit can be carried out as follows.

1. Construction and simplification of the flow table (1).

2. Assignment to each row of the table of one or more states of a set of binary-valued variables, which will be called "state variables." In the asynchronous case, these states must be so chosen that critical races never occur. That is, if any transition in the table calls for changing more than one state variable, then the order in which the changes occur must not affect the row that is ultimately reached. This requirement often necessitates the use of more than one state per row (4). No restriction of this kind applies in the case of synchronous systems; hence there is little reason to assign more than one state to a row.

3. Derivation from the flow table and row assignment of the specifications for a combinational circuit with feedback, as shown in reference 1; derivation by an analogous process for synchronous systems.

4. Synthesis of this combinational circuit by any convenient method.

This report will discuss step 2. Let us first consider the synchronous case, and assume that one state is to be assigned to each row; and, for the sake of simplicity, that m, the number of rows in the table, is an integral power of two. Thus, if $m = 2^n$, then n-state variables will yield the required number of states. Since any state can be assigned to any row, the number of possible arrangements is $m!$. Three of the 24 possible assignments are shown for the same table in Fig. IX-1. However, from a physical viewpoint, many of these assignments are essentially equivalent to one another, since they differ only in that some of the state variables have merely been relabelled. For example, the assignment in Fig. IX-1c can be obtained from the one in Fig. IX-1a by complementing y_2 and then interchanging y_1 and y_2.

It will be shown that the number of distinct assignments (those which, in general, may lead to different circuit specifications in step 3) is $(2^n - 1)!/n!$ for a 2^n-row synchronous flow table. In the case of asynchronous circuits, the problem of race

*This work was supported in part by Purchase Order DDL-B158. (See the Introduction.)

State y_1y_2 \ Input x_1x_2:	00	01	11	10	Row
00	1^1	1^0	1^0	2^0	1
01	1^0	2^1	2^0	3^1	2
11	1^0	3^1	2^1	4^0	3
10	1^0	4^0	3^0	1^0	4

(a)

State y_1y_2 \ Input x_1x_2:	00	01	11	10	Row
00	1^1	1^0	1^0	2^0	1
01	1^0	2^1	2^0	3^1	2
10	1^0	3^1	2^1	4^0	3
11	1^0	4^0	3^0	1^0	4

(b)

State y_1y_2 \ Input x_1x_2:	00	01	11	10	Row
10	1^1	1^0	1^0	2^0	1
00	1^0	2^1	2^0	3^1	2
01	1^0	3^1	2^1	4^0	3
11	1^0	4^0	3^0	1^0	4

(c)

Fig. IX-1. Synchronous flow tables. The numbers with superscripts indicate the next row; the superscripts correspond to the output. Row assignments in (a) and (b) are distinct; those in (a) and (c) are equivalent.

conditions restricts the allowable number of assignments to the extent that there are no nontrivial transformations that can always be made. In specific cases, however, several distinct assignments are possible.

These statements will be proved by using some elementary principles of group theory (see ref. 5). If r represents a particular row assignment for an m-row synchronous table (where $m = 2^n$), and if p represents one of the m! permutation transformations that can be applied to a set of m elements, then the expression rp can be used to designate the new row assignment that results from permuting assignment r in accordance with transformation p. To take an example: if the zeros and ones that describe each state are thought of as forming binary numbers, then the states can be compactly written as the decimal equivalents of these numbers, so that, in Fig. IX-1a, the internal states are

0, 1, 3, and 2, reading from the top down. If we apply the permutation (0)(1)(32), the assignment of Fig. IX-1b is obtained; the permutation (0132) transforms the same assignment into that of Fig. IX-1c. The set G of all permutations p (including the identity I) can easily be shown to be a noncomutative group with m! members.

A permutation s [such as (0132)] that results when the state variables are interchanged and/or complemented, will be called "symmetric." The set of all of these transformations (members of which will henceforth be referred to as s_i, $i = 1, 2, \ldots$) is a subgroup of G containing $n!\,2^n$ members, and it constitutes the set of all transformations, leaving distances on an n-dimensional hypercube invariant (6).

Two row assignments, r_1 and r_2, will be said to be equivalent (written $r_1 \sim r_2$), if $r_1 = r_2 s_i$. Similarly, two transformations t_1 and t_2 will be defined as being equivalent if $t_1 = t_2 s_i$. It follows that, if a row assignment is operated upon separately by two equivalent transformations, the two resultant assignments will be equivalent.

For each element p in G, form a subset of G that consists of the elements ps_i for every s_i in S. These subsets are called "left cosets of S."

Suppose that q_1 and q_2 belong to the same coset. Then, there are elements s_1 and s_2 in S, and an element p in G so that $q_1 = ps_1$, $q_2 = ps_2$ and $s_3 = s_2' s_1$ (s_2' is the inverse of s_2). Since $q_2 s_3 = (ps_2)(s_2' s_1) = p(s_2 s_2') s_1 = ps_1 = q_1$, it follows that $q_1 \sim q_2$.

Cosets possess the following properties (proved in sec. 9 of ref. 5):

1. Every member of G belongs to some coset of S.
2. Each coset contains the same number of elements as S.
3. Two cosets of S are either disjoint or identical.
4. S is a coset of itself.

We have shown that members of the same coset are equivalent. Now we shall demonstrate that the converse is true. Suppose that $q_1 \sim q_2$. Then, $q_1 = q_2 s_3$ and from property 1, $q_2 = ps_2$ for some p in G. If $s_1 = s_2 s_3$, then $q_1 = ps_2 s_3 = ps_1$ so that q_1 and q_2 belong to a common coset. Therefore, two transformations are distinct if and only if they belong to different cosets. But according to Lagrange's theorem (which can be derived from the first three properties of the cosets listed above) the number of distinct cosets of G is equal to the number of elements in G divided by the number of elements in S, or

$$\frac{(2^n)!}{2^n n!} = \frac{(2^n - 1)}{n!} \tag{1}$$

Hence, the number of distinct row assignment transformations and the number of distinct assignments are equal to term 1.

For the special case of the four-row table, the problem of finding a set of three distinct assignments is quite simple. If we start with any arbitrary assignment (as in Fig. IX-1a) and interchange the states assigned to the third and fourth rows, we have one distinct assignment (Fig. IX-1b). A third assignment, distinct from each of the first two, can then be found by interchanging the states of rows two and three in the first assignment. Symbolically, the two transformations can be written as (0)(1)(32) and (0)(13)(2), respectively. It might be well to note here that, in any particular problem, the number of row assignments that lead to physically different circuits may be less than the number of distinct transformations given in term 1, owing to symmetries within the particular flow table.

Now consider an asynchronous circuit in which transitions between all pairs of adjacent internal states (those states differing in the values of one variable only) occur at some point in the flow table. Any row assignment transformation that does not preserve distances on the n-dimensional hypercube whose vertices correspond to internal states of the system will introduce race conditions. Thus, only members of S can be used. This implies that, in general, no nontrivial transformations are possible, although they may exist for special examples.

In the special case of a four-row asynchronous flow table that is strongly connected (in the sense that there are input sequences connecting all pairs of internal states), similar reasoning indicates that no nontrivial row assignment transformations exist.

When nontrivial transformations are available, it would be highly desirable to have a method for ascertaining a priori which assignment is the best one – according to some criterion such as the minimization of the number of necessary combinational elements. The usefulness of a process of this kind can be appreciated, if it is realized that there are 840 distinct row assignments for any eight-row synchronous flow table. Unfortunately, this seems to be an exceedingly difficult problem and I have no suggestions as to how it can be approached.

S. H. Unger

References

1. D. A. Huffman, Technical Report 274, Research Laboratory of Electronics, M.I.T., Jan. 10, 1954.
2. D. A. Huffman, Proceedings of the Symposium on Information Networks, Polytechnic Institute of Brooklyn, New York, April 12-14, 1954.
3. E. F. Moore, Gedanken-experiments on Sequential Machines, Automata Studies (Princeton University Press, 1956).
4. D. A. Huffman, Technical Report 293, Research Laboratory of Electronics, M.I.T., March 14, 1955.
5. G. D. Birkhoff and S. MacLane, A Survey of Modern Algebra (Macmillan Company, New York, 1953), Chap. VI.
6. D. Slepian, Can. J. Math. 5, 185-193 (1954).

B. CODING FOR BINARY SYMMETRIC CHANNEL

Recent work by C. E. Shannon and P. Elias has established bounds on the exponential behavior of probability of error for finite-length messages transmitted over idealized noisy channels. They have also shown that random coding is exponentially equivalent to the best-possible coding, for transmission rates near to capacity (1, 2).

The physical implementation of a random-coding procedure is difficult because the number of possible messages increases exponentially with message length. Even with moderate message lengths, this number can become enormous for reasonable rates of transmission. Small message lengths, however, preclude the strong, large-sample, statistical assertions that are necessary to assure a small probability of error.

Research is in progress toward the determination of a physically realizable coding and decoding procedure for the idealized Binary Symmetric Channel. This procedure will be a compromise between the demands of reasonable equipment on the one hand, and acceptable performance on the other. A random-code message development, using a sliding parity-check generator, is envisioned at the transmitter. The transmitted message of length n is divided for coding and decoding purposes into several smaller sublengths $n_1 < n_2 = n_1 + \Delta_1 < n_3 = n_2 + \Delta_2 < \ldots < n_i = n_{i-1} + \Delta_{i-1} < \ldots n$. In going from any length n_i to n_{i+1}, the transmitter inserts a number $\delta_i < \Delta_i$ of completely arbitrary information digits, filling the rest of the increment Δ_i with "random" check digits generated as the mod 2 sum of the sliding check pattern and as much of the message as has already been determined.

Correspondingly, at each stage n_i of decoding, the receiver progressively compares the received message with the set of possible transmitted messages, and discards those members of the set that are beneath a certain threshold of probability. At each stage, a number of possible messages whose individual a posteriori probabilities sum to an acceptable aggregate is retained. In the next stage, then, the receiver need only compute those possible messages that have prefixes which are members of the stored subset.

In the end, the process is made to converge to the selection of a single message of high probability. The over-all probability of error is equal to one minus the cumulative probability of having retained the correct message at each stage of the procedure.

It has been shown that the number m_i of prefixes that should be retained at the i^{th} stage can be made to vary as $1/n_i$ by adopting suitable constraints on the incremental rate $R_i = \delta_i/\Delta_i$. As n_i increases, R_i can also increase, giving an effective average rate R reasonably close to the maximum rate that is permitted under ideal coding for the specified design probability of error and block-length n.

J. M. Wozencraft

References

1. C. E. Shannon, The rate of approach to ideal coding (Abstract), IRE Convention Record, Part 4, 1955.
2. P. Elias, Coding for noisy channel, IRE Convention Record, Part 4, 1955.