A Theory of Asynchronous Circuits

DAVID E. MULLER
Research Associate Professor of Applied Mathematics
Universtiy of Illinois

and

W. S. BARTKY
University of Illinois

1. Introduction

Switching circuits are commonly classified as being either synchronous or asynchronous, depending upon whether or not the signals in the circuit are synchronized with some source of fundamental frequency (or clock) which regulates the entire circuit. Much of the mathematical theory of switching circuits and many design techniques have been limited to synchronous circuits, because it is possible to predict the state (or condition) of a synchronous circuit at the time of any given clock signal if one knows the initial state of the circuit and its logical characteristics. As a result, many design problems may be handled by logical algebra. However, in an asynchronous circuit it is not possible to predict the state immediately resulting from a previous state from a knowledge of the logical characteristics of the circuit alone. The resulting state may also depend upon the relative speeds of some of the logical elements which comprise the circuit. The possibility of such "races" in asynchronous circuits complicates the theory unless one is prepared to make definite assumptions concerning element speeds, and thus reduce the problem to the synchronous case, or else design one's circuits so that only one logical element is able to change at a time.

We shall not attempt here to extend the theory of synchronous circuits to cover the asynchronous case, but rather develop a comprehensive theory of asynchronous circuits which will differ from that of synchronous circuits in many fundamental respects. One of our main objects will be to describe the properties of circuits which are speed-independent in the sense that their ultimate behavior does not depend upon the relative speeds of their elements. What is meant by "ultimate behavior" will be set down precisely in the later discussion, and techniques for designing speed-independent circuits will be described toward the end.

Existing theories of asynchronous circuits have been mostly concerned with what might be called the "black-box" model of a circuit. One deals with a "black box" or circuit having a number of inputs, a number of outputs, and a number of internal states. When the input signals are changed, the circuit proceeds from its existing internal state to another uniquely determined internal state and the outputs change accordingly. One must always assume that no further change is made in the inputs until this second internal state has actually been achieved, for otherwise the behavior of the circuit would be indeterminate. The theory treats the way the states and outputs change as a result of manipulating the inputs and in most respects is similar to the corresponding theory of synchronous circuits.

The theory presented here is not a revision of the "black-box" theories but may be regarded as a supplement to them, since it is concerned with the changes which the circuit undergoes if the inputs, if any, are held fixed. It therefore deals with those transitions which occur between input changes. It might also be used to describe the action of a circuit which has no inputs of the type referred to above, for example, an automatic computer. Since the inputs, if they exist, are regarded as fixed in the present theory, they need not appear explicitly in our description of a circuit and may be regarded as parameters affecting the circuit's logical properties.

2. *Description of a Circuit*

In an idealized switching circuit the physical signal present at any point within the circuit may assume one of a discrete set of values. This physical signal may take the form of a voltage, current, position, or other measurable quantity. Let us assume that n such measurements are sufficient to specify the state of the circuit so that any other measurements may be uniquely determined from the given n. These n signals will be denoted by symbols such as $z_1, z_2, \ldots, z_n$, and the n-tuple $z = (z_1, z_2, \ldots, z_n)$ will be taken as representing the state of the circuit.

Each signal z_i may assume one of a discrete set of values S_i, where the elements of S_i are finite in number and totally ordered. They may therefore be set into correspondence with the integers $0, 1, \ldots, k_i - 1$, where it is assumed that S_i contains k_i elements. The set S of states is, thus, also finite and contains all n-tuples z whose components z_i are taken from the sets S_i.

An important special case is that of the binary switching circuit in which a signal may take one of but two possible values so that $k_i = 2$ for each $i = 1, 2, \ldots, n$. Thus, in the binary case the signal z_i may be either 0 or 1, while in the general case it may be any member of the ordered set of values $0, 1, \ldots, k_i - 1$. The binary case is so important that it would hardly be worth while treating the more general case were it not possible to do so with very little additional difficulty.

In a relay switching circuit the signal z_i may conveniently be taken as describing the position of the ith relay. If this relay is of the usual two-position (open or closed) type, the signal will be binary, while a relay having k_i standard positions could be described by the more general type of signal.

In an electronic switching circuit the signals are usually interpreted as voltages, and, although it is true that voltages in a circuit change in a continuous fashion, one may assume that each signal value merely specifies a range of voltage rather than an exact voltage. Naturally, we may use this simplified treatment of the signals only if the behavior of the circuit is adequately described by the discrete signals.

The switching properties of an idealized switching circuit can be expressed as a set of functions

$$z_i' = f_i(z_1, z_2, \ldots, z_n), \qquad i = 1, 2, \ldots, n,$$

where the dependent variables z_i' lie in the sets S_i. Each z_i' is assumed to be uniquely determined by the state $z = (z_1, z_2, \ldots, z_n)$. In a binary circuit these functions will be Boolean functions since all signals are assumed to be either 0 or 1. In an electronic circuit these functions represent the individual logical elements which form the circuit, and serve to describe their interconnections; in a relay circuit these functions express the behavior of the networks of contacts.

Our theory will therefore be concerned with the following concepts:

n signals z_i, $i = 1, 2, \ldots, n$, each taken from a set S_i of k_i ordered elements, which will be written $0, 1, \ldots, k_i - 1$. (2.1)

The set S of n-tuples of signals $z = (z_1, z_2, \ldots, z_n)$, called states. (2.2)

n functions $z_i' = f_i(z_1, z_2, \ldots, z_n)$ which define a mapping of S onto itself. (2.3)

A more general switching circuit will also be influenced by outside parameters or "inputs" which should properly be included in (2.3) above. Since the present theory is concerned only with the behavior of circuits during the time that such inputs (if present at all) are held fixed, we need not include them explicitly in the functions (2.3).

3. *Circuit Behavior*

We now wish to set down a mathematical description of the behavior of an asynchronous, or nonclocked, switching circuit. If the circuit is placed in a state $a = (a_1, a_2, \ldots, a_n)$, some of the signals will generally tend to change and the circuit will pass to another state $b = (b_1, b_2, \ldots, b_n)$. If the circuit is synchronous this "next" state b will occur just one clock interval later and will be uniquely determined by the functions (2.3). In fact, b will be just $a' = (a_1', a_2', \ldots, a_n')$. In an asynchronous circuit, on the other hand, there is no clock, or source of fundamental frequency, and the relative times which the various signals take to change will depend on physical properties of the circuit elements and will be unrelated to the logical properties expressed in (2.3). The state b is, thus, not always uniquely determined by the functions (2.3) in the asynchronous case and, in general, may be any one of several states depending on these relative speeds.

We wish to make no specific assumptions concerning relative speeds of circuit elements in the asynchronous case and we shall try to describe all possible states b into which the circuit may pass from a given state a. This concept is expressed in terms of a relation $\mathscr{R}$:

$a \mathrel{\mathscr{R}} b$ means that each signal b_i of b satisfies either $a_i \leq b_i \leq a_i'$ or $a_i \geq b_i \geq a_i'$, depending upon whether $a_i \leq a_i'$ or $a_i \geq a_i'$. (3.1)

Clearly $a \mathrel{\mathscr{R}} a$ and $a \mathrel{\mathscr{R}} a'$, but, in general, there may be other states b as well which satisfy $a \mathrel{\mathscr{R}} b$, and in asynchronous-circuit theory all such "next" states will be regarded as possible. If one thinks of a_i as the existing signal and a_i' as a new signal toward which point i is tending, then (3.1) may be thought of intuitively as saying that in the "next" state b the signal b_i at point i may have changed so that it lies anywhere in the closed interval a_i to a_i'.

A partial allowed sequence of k states $a(1)$, $a(2)$, . . . , $a(k)$ is any sequence of $k \geq 1$ states which, whenever $k \geq 2$, satisfies $a(j) \mathscr{R} a(j+1)$ and $a(j) \neq a(j+1)$ for all $j = 1, 2, \ldots, k-1$. (3.2)

A partial allowed sequence is a sequence of states which is intended to describe the possible behavior of a circuit which starts in state $a(1)$ and passes through succeeding states $a(2), \ldots, a(k)$. The circuit may go on to other states after reaching $a(k)$ and so to complete the description of the circuit's behavior we require:

An allowed sequence of states $a(1)$, $a(2)$, . . . (which may be either finite or infinite) is any sequence such that:

$a(j) \mathscr{R} a(j+1)$ and $a(j) \neq a(j+1)$ for all consecutive pairs of states $a(j)$, $a(j+1)$ in the sequence; and (3.3a)

there exists no signal $a_i(j)$ with $a_i(j) = a_i(k) < a_i'(k)$ or $a_i(j) = a_i(k) > a_i'(k)$ for all signals $a_i(k)$ with $k \geq j$. (3.3b)

An allowed sequence may be regarded as a possible sequence of states through which an asynchronous circuit might pass if placed initially in state $a(1)$. This definition (3.3) was chosen because it was thought to best represent asynchronous-circuit behavior. Other possible definitions may be more convenient from a mathematical standpoint but would fail to yield a realistic theory. Condition (3.3b) requires that no point i in the circuit may retain a signal $a_i(j)$ indefinitely if it is tending toward some other value $a_i'(k)$ which remains either greater than $a_i(j)$ or less than $a_i(j)$ for the rest of the sequence. We note that (3.3b) permits $a_i(j)$ to remain fixed indefinitely if $a_i'(j)$ is alternately greater and less than $a_i(j)$.

Any finite, consecutive set of states in an allowed sequence forms a partial allowed sequence. (3.4)

If both $a(1)$, $a(2)$, . . . , $a(k)$ and $a(k)$, $a(k+1)$, . . . , $a(m)$ are partial allowed sequences, then $a(1)$, $a(2)$, . . . , $a(k)$, . . . , $a(m)$ is a partial allowed sequence. (3.5a)

If the sequence $a(k)$, $a(k+1)$, . . . is an allowed sequence and $a(1)$, $a(2)$, . . . , $a(k)$ is a partial allowed sequence, then the composite sequence $a(1)$, $a(2)$, . . . , $a(k)$, . . . is an allowed sequence. (3.5b)

Allowed sequences may be either finite or infinite, but if a finite sequence $a(1)$, $a(2)$, . . . , $a(m)$ is allowed, then the terminal state $a(m)$ must be an equilibrium state, that is, one for which $a(m) = a'(m)$. (3.6)

The statements above follow from the definitions of allowed and of partial allowed sequences. Statement (3.6) must hold in order to avoid a violation of (3.3b); (3.3b) also restricts infinite allowed sequences, but in a more subtle way, as will be demonstrated later.

If an allowed sequence does indeed represent a possible sequence of states through which the circuit might pass, then it should be possible to show that at least one allowed sequence exists which starts with any state $a(1)$ as the initial state. If no allowed sequence exists, then we must seek some other way of describing the behavior of the circuit when placed in state $a(1)$.

Theorem 1: Given any state $a(1)$, there must exist at least one allowed sequence $a(1), a(2), \ldots$ having $a(1)$ as its initial state.

Proof: Form the sequence $a(1), a(2), \ldots\ldots$ by the following rules:

(1) let $a(j+1) = a'(j)$ if $a'(j) \neq a(j)$;

(2) let the sequence terminate with $a(j)$ if $a'(j) = a(j)$. That this sequence satisfies (3.3a) may be seen from the property $a(j) \mathscr{R} a'(j)$; (3.3b) may also be seen to hold if one notes that either $a_i(j) = a_i'(j)$ or else $a_i(j) \neq a_i'(j) = a_i(j+1)$ so that either $a_i(k) = a_i'(k)$, with $k = j$, or else $a_i(j) \neq a_i(k)$, with $k = j + 1$.

In the relation $a \mathscr{R} b$ we have expressed the notion that state b may come after state a with no intervening states. We now go on to define a new relation $a \mathscr{F} b$ which will indicate that b may come after a but that intervening states may separate them.

$a \mathscr{F} b$, read a is followed by b, means that a partial allowed sequence exists having a as its first and b as its last state. (3.7)

Two properties of the $\mathscr{F}$ relation may be immediately noted.

$$a \mathscr{F} a \text{ for all states } a. \tag{3.8a}$$

We note that any state a by itself forms a partial allowed sequence.

$$a \mathscr{F} b \text{ and } b \mathscr{F} c \text{ implies } a \mathscr{F} c. \tag{3.8b}$$

The composite sequence $a, \ldots, b, \ldots, c$ is a partial allowed sequence.

Unfortunately, the $\mathscr{F}$ relation does not produce a partial ordering of the states, since we may have $a \mathscr{F} b$ and $b \mathscr{F} a$ and yet $a \neq b$. A partial ordering may be constructed between sets of states rather than states, in a manner described in the following definition:

$$a \mathscr{E} b \text{ means } a \mathscr{F} b \text{ and } b \mathscr{F} a. \tag{3.9}$$

Theorem 2: $\mathscr{E}$ is an equivalence relation.

Proof: We need only note that

$$a \mathscr{E} a \text{ for all } a, \tag{3.10a}$$

$$a \mathscr{E} b \text{ implies } b \mathscr{E} a, \tag{3.10b}$$

$$a \mathscr{E} b \text{ and } b \mathscr{E} c \text{ imply } a \mathscr{E} c, \tag{3.10c}$$

which follow from the properties of $\mathscr{F}$.

Since the states are finite in number, by construction, we see that the $\mathscr{E}$ relation breaks the set of states S into a finite number of nonvoid equivalence sets A, B, C, ...

Two states a and b lie in the same equivalence set C if and only if $a \mathscr{E} b$. (3.11)

$A \mathscr{F} B$, read A is followed by B, means that there is a state a in A and a state b in B such that $a \mathscr{F} b$. (3.12)

Theorem 3: If a is in A and b is in B, and if $A \mathscr{F} B$, then $a \mathscr{F} b$.

Proof: By (3.12) we can find a state a^* in A and a state b^* in B such that $a^* \mathscr{F} b^*$. Then since $a \mathscr{F} a^*$, $a^* \mathscr{F} b^*$, $b^* \mathscr{F} b$, we have $a \mathscr{F} b$.

Theorem 4: The $\mathscr{F}$ relation defines a partial ordering between equivalence sets.

Proof: We must show that

$$A \mathscr{F} A \text{ for all } A. \tag{3.13a}$$

$$A \mathscr{F} B \text{ and } B \mathscr{F} C \text{ implies } A \mathscr{F} C. \tag{3.13b}$$

$$A \mathscr{F} B \text{ and } B \mathscr{F} A \text{ implies } A = B. \tag{3.13c}$$

These three properties may be easily deduced from (3.12) and Theorem 3.

Since the number of equivalence sets is finite and partially ordered, there must exist at least one maximum or final set.

M is a final set if and only if there is no set M^* different from M, such that $M \mathscr{F} M^*$. (3.14)

Given any equivalence set A there must exist at least one final set M such that $A \mathscr{F} M$. (3.15)

If we deny (3.15) we may construct a sequence of sets A, $A(1)$, $A(2)$, . . . of indefinite length such that $A(j) \mathscr{F} A(j + 1)$ and $A(j) \neq A(j + 1)$, and involving no repetitions because of partial ordering. This requires an infinite number of sets. Similarly, a minimum set may be shown to exist, but such sets will have little importance in the present theory.

Theorem 5: $a = a'$ (that is, a is an equilibrium state) if and only if its equivalence set A is a final set containing just one state.

Proof: If $a = a'$, then $a \mathscr{R} b$ implies $a = b$. Hence A is a set containing just one state, and consequently is a final set since $A \mathscr{F} B$ would imply $a \mathscr{F} b$ for a state b in B. If A is a final set containing just one state a, then, since $a \mathscr{R} a'$, we have either a' in B with $A \mathscr{F} B$, which is impossible, or else a' in A, which means $a = a'$.

A pseudo-final set P is an equivalence set of states $p(1), \ldots, p(r)$ which is not final and for which there is no signal index i such that $p_i(j)$ is constant over all $j = 1, \ldots, r$, and either $p_i(j) < a_i'(j)$ for all $j = 1, \ldots, r$, or $p_i(j) > a_i'(j)$ for all $j = 1, \ldots, r$. (3.16)

We note that a pseudo-final set must contain more than one state.

Theorem 6: Any allowed sequence $a(1)$, $a(2)$, . . . must contain a state $a(m)$ such that all states $a(m)$, $a(m + 1)$, . . . lie in the same equivalence set T (called the terminal set of the sequence), which is either final or pseudo-final.

Proof: Since the number of equivalence sets is finite, we see that the number of sets which are represented in any allowed sequence is also finite. Hence there must be a state $a(m)$ such that all equivalence sets in the entire allowed sequence are represented in the partial allowed sequence $a(1)$, $a(2)$, . . . , $a(m)$. Now if $a(m)$ is in T, then all states following $a(m)$ must also be in T. Otherwise, partial ordering of the sets would be violated.

We must now show that T is either final or pseudo-final. Assume that T is neither. In this case we have either $a_i(m) = a_i(k) < a_i'(k)$ for some i and all $k \geq m$, or $a_i(m) = a_i(k) > a_i'(k)$ for some i and all $k \geq m$, and consequently we have violated (3.3*b*).

In view of (3.15) we note that, if any initial state u is chosen, we may always form an allowed sequence starting with u, whose terminal set is final. A somewhat stronger result may be proved, however.

Theorem 7: If u is any state and U is its equivalence set, then, if T is any final or pseudo-final set such that $U \mathcal{F} T$, an allowed sequence may be constructed starting with u whose terminal set is T.

Proof: If T is a final set and $t(0)$ is any state in T, we may form a partial allowed sequence u, . . . , $t(0)$ by (3.7) and Theorem 3. An allowed sequence starting with t may now be formed by the method of Theorem 1. Since T is final, the sequence must be entirely in T; for if some member of the sequence lies in another set T, we would have $T \mathcal{F} T^*$. Now if we combine these two sequences by (3.5*b*), we obtain the desired sequence u, . . . , $t(0)$, ...

If T is a pseudo-final set, the same proof may be used provided we may form an allowed sequence starting with $t(0)$ and lying entirely in T. This is done in the following paragraph.

Let $t(0)$, $t(1)$, . . . , $t(k)$ be the states in the pseudo-final set T. Construct $k + 1$ partial allowed sequences $t(0)$, . . . , $t(1)$; $t(1)$, . . . , $t(2)$; $t(2)$, . . . , $t(3)$; . . . ; $t(k - 1)$, . . . , $t(k)$; $t(k)$, . . . , $t(0)$; by use of (3.7). Since the states at the ends of these partial allowed sequences match, they may be combined by (3.5*a*) into a single partial allowed sequence $t(0)$, . . . , $t(1)$, . . . , $t(2)$, . . . , . . . , $t(k)$, . . . , $t(0)$ containing all states in T. Let us now repeat this partial allowed sequence indefinitely, always letting the last member of the previous partial allowed sequence be the first member of the next. This resulting sequence is allowed since all states in T are present and (3.16) gives us (3.3*b*).

4. *An Example of a Circuit*

As an example, consider the binary circuit whose defining equations (2.3) are the Boolean equations:

$$\begin{aligned} z_1' &= z_2 \vee z_3, & z_3' &= \bar{z}_4(z_1 \vee \bar{z}_2), \\ z_2' &= \bar{z}_1, & z_4' &= \bar{z}_3. \end{aligned} \tag{4.1}$$

This circuit, if represented by a logical diagram, would consist of two "not" elements, an "or" element, and a special element for producing the function $\bar{z}_4(z_1 \vee \bar{z}_2)$. They are to be connected as in Fig. 1, where E represents the special element.

If one writes the $\mathscr{R}$ relations between the sixteen states, and the corresponding $\mathscr{F}$ relations, it can be shown that there are four equivalence sets. They may be designated by A, B, C, and D as follows:

A contains (0000), (0010), (0011), (0100), (0110), (0111), (1000), (1011), (1100), (1111);
B contains (0001), (0101), (1001), (1101);
C contains (1110);
D contains (1010).

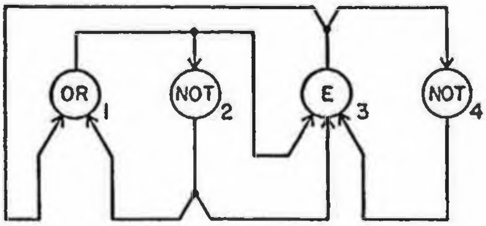

FIG. 1. Logical diagram defined by Eqs. (4.1).

We have $A \mathscr{F} B$, $A \mathscr{F} C$, $A \mathscr{F} D$, and $C \mathscr{F} D$. We note also that B and D are final sets, while A is pseudo-final and C is neither final nor pseudo-final. Since (1010) is an equilibrium state, we see by Theorem 5 that its set contains no other state and must be final.

If we start with the initial state (1111) we may illustrate some of the possible allowed sequences:

(1) (1111), (1010);
(2) (1111), (1110), (1010);
(3) (1111), (1101), (1001), (0001), (0101), (1101), (1001), . . . ;
(4) (1111), (0111), (0110), (0100), (1100), (1000), (0000),
(0010), (0110), (0100), ...

The last two allowed sequences are infinite, having cycles of four and six states, respectively.

Sequences (1) and (2) have the final set D as their terminal set. Since this set contains just the equilibrium state (1010) we see that both these allowed sequences are finite. The sequence (1) proceeds directly from A to D while (2) goes through the intermediate set C before terminating in D.

Sequence (3) goes from A to B, and since B is final this must be its terminal set. This sequence enters a cycle of states in B and does not terminate.

Sequence (4) remains, indefinitely, in the pseudo-final set A. It may appear as if condition (3.3b) is violated in the cycle because the fourth signal never changes after the first two states; but since $a_4'(k) = a_4(k)$ for states (0110) and (0010) we see that no violation has occurred.

5. *Speed Independence*

In the previous discussion we have sought to describe the behavior of a circuit by means of the concept of an allowed sequence. In Theorem 6 we saw that the circuit eventually passes into a final or pseudo-final set of states, and stays in this set from then on. If the terminal set consists of one state, this means that the circuit goes to equilibrium and the allowed sequence terminates. Otherwise the circuit may never reach equilibrium; but one may regard the final or pseudo-final set, which perpetuates itself, as a sort of dynamic equilibrium.

Of special interest are those circuits in which the ultimate behavior of the circuit does not depend on the relative speeds of the elements. Such circuits, which will be called speed-independent, may be designed without regard to time tolerances and capacities of elements and wiring. Hence they should be easier to design and more reliable than asynchronous circuits which require time tolerances on the elements for proper operation.

There remains the problem of selecting a suitable definition for speed-independence in asynchronous circuits. One might choose the requirement that all allowed sequences starting with a given initial state u shall terminate in an equilibrium state m. This requirement has been expressed before in slightly different terms by another author,[1] and it has the advantage that it ensures a unique final condition for the circuit. On the other hand, it precludes the possibility of having speed-independent circuits which "cycle" indefinitely (within a final or pseudo-final set), and for this reason we shall use a somewhat broader definition for speed independence.

A circuit is said to be speed-independent with respect to an initial state u if there exists a final set M such that every allowed sequence beginning with u contains a state in M. (5.1)

Theorem 8: If a circuit is speed-independent with respect to u, then the terminal set of every allowed sequence starting with u must be M.

Proof: Let an allowed sequence under consideration be $u, a(1), a(2), \ldots$, and let $a(j)$ be a state of the sequence which is in M. Then $a(j), a(j+1), \ldots$ must all lie in M; for if $a(k)$ with $k > j$ is in M^*, then $M \mathscr{F} M^*$, which is impossible. Thus M is the terminal set of all allowed sequences starting with u.

Theorem 8 shows that the ultimate behavior of the circuit, when placed in state u, will not depend upon the relative speeds of the elements. That is, we interpret the rather loose concept of ultimate behavior as meaning a specification of which terminal set is attained by an allowed sequence. Thus if all allowed sequences starting with u have the same terminal set we mean that the circuit will always arrive, ultimately, at a unique static or dynamic condition.

Theorem 9: A circuit is speed-independent with respect to u if and only if U, the set of u, is followed by just one final set and no pseudo-final sets.

Proof: Assume that $U \mathscr{F} M$, where M is final, and that U is followed by no other final set and no pseudo-final sets. Then any allowed sequence $u, a(1), a(2), \ldots$ must have M as its terminal set, for if the terminal set T of the sequence is not equal to M then $U \mathscr{F} T$ in contradiction of the hypothesis.

Assume that the circuit is speed-independent with respect to u. Now if $U \mathscr{F} T$, where T is either final or pseudo-final but not equal to M, we may construct an allowed sequence whose initial state is u and whose terminal set is T by Theorem 7. Since by hypothesis this sequence contains a state m of M, we have $M \mathscr{F} T$ which contradicts the assumption that M is final.

When we face the involved problem of circuit design it becomes apparent that (5.1) is not a convenient definition for speed-independence from the point of view of applications. It is usually difficult to determine whether or not a given circuit is speed-independent since the number of states, sets, and allowed sequences starting with an initial state u may be very great. Therefore, in the following paragraphs we shall discuss other conditions which do not have this disadvantage yet imply speed independence.

One such condition which has been used by other authors[1,2] is:

A circuit is totally sequential with respect to an initial state u if and only if there is only one allowed sequence starting with u. (5.2)

This condition does imply speed-independence since U, the set of u, is followed by some final set M. Hence, by Theorem 7, the single allowed sequence starting with u must have terminal set M.

If we assume that $u, a(1), a(2), \ldots$ is the only allowed sequence starting with u, then we must have $u \mathscr{R} a(1), \ldots, a(j) \mathscr{R} a(j+1), \ldots$, but there can be no other state $b(j+1)$ such that $a(j) \mathscr{R} b(j+1)$. Thus $a(j+1) = a'(j)$, and by (3.1) we see that there is at most one signal $a_i(j)$ of $a(j)$ for which $a_i(j) \neq a_i'(j)$. For this signal we must have either $a_i(j) = a_i'(j) + 1$ or $a_i(j) = a_i'(j) - 1$. Thus, only one signal tends to change at a time in a totally sequential circuit, so that no circuits can be totally sequential and have parallel changes occur in them. Many modern computers use just such parallel changes to achieve their extraordinary speeds. Therefore we seek some other condition to impose on our circuits which is less restrictive than that they be totally sequential.

A circuit is semimodular with respect to an initial state u if and only if for all states b and c such that $u \mathscr{F} b$ and $b \mathscr{R} c$ the relation $c \mathscr{R} b'$ also holds. (5.3)

The name "semimodular" was given to this condition because of its connection with a semimodular lattice, which will be discussed later. An immediate consequence of (5.3) is the property that for any three states a, b, and c such that $u \mathscr{F} a$, $a \mathscr{R} b$, and $a \mathscr{R} c$ there must be a fourth state d such that $b \mathscr{R} d$ and $c \mathscr{R} d$. We see that $d = a'$ has these properties.

A more useful state d of this type is defined as follows:

If a circuit is semimodular with respect to u and $u \mathscr{F} a$, $a \mathscr{R} b$, and $a \mathscr{R} c$, then the state $d = M[a;b,c]$ is defined componentwise by

$$d_i = \max(b_i, c_i) \quad \text{if} \quad a_i \leq a_i', \tag{5.4a}$$

and

$$d_i = \min(b_i, c_i) \quad \text{if} \quad a_i \geq a_i'. \tag{5.4b}$$

This definition is not inconsistent in case $a_i = a_i'$, since then $a_i = b_i = c_i$.

Theorem 10: In (5.4*a*,*b*), $a \mathscr{R} d$, $b \mathscr{R} d$, and $c \mathscr{R} d$.

Proof: Since b_i and c_i both satisfy the conditions of (3.1), we see that d_i must also and hence $a \mathscr{R} d$. Now, if $a_i \leq b_i < a_i'$, we have $b_i \leq d_i \leq a_i' \leq b_i'$ by (5.3) and (3.1). Similarly, if $a_i \geq b_i > a_i'$, we have $b_i \geq d_i \geq a_i' \geq b_i'$. However, if $b_i = a_i'$, then we have $b_i = d_i$. Hence in any case we satisfy (3.1), giving $b \mathscr{R} d$. Similarly, $c \mathscr{R} d$.

Theorem 11: In a circuit semimodular with respect to u, let $u \mathscr{F} a(0)$ and let $a(0), a(1), \ldots, a(k)$ be a partial allowed sequence. If $a(0) \mathscr{R} b(0)$, then we may define a sequence $b(0), b(1), \ldots, b(k)$ where $b(j) = M[a(j-1);\ a(j), b(j-1)]$ when $j = 1, 2, \ldots, k$.

Proof: Since $u \mathscr{F} a(0)$, $a(0) \mathscr{R} a(1)$, and $a(0) \mathscr{R} b(0)$, we may form $b(1)$ and by Theorem 10 we have $a(1) \mathscr{R} b(1)$. Assume that $b(j)$ may be defined as in Theorem 11 and that $a(j) \mathscr{R} b(j)$. Then, since $u \mathscr{F} a(j)$ by (3.8*b*) and $a(j) \mathscr{R} a(j+1)$, we may define $b(j+1)$ and by Theorem 10 we have $a(j+1) \mathscr{R} b(j+1)$. Hence by induction we may define $b(j)$ for $j = 1, 2, \ldots, k$.

Theorem 12: A circuit which is semimodular with respect to u is speed-independent with respect to u.

Proof: We shall make use of Theorem 9 and show that U, the set of u, is followed by just one final and no pseudo-final sets.

To show that U is followed by just one final set let us assume that there are two distinct final sets M and M^* such that $U \mathscr{F} M$ and $U \mathscr{F} M^*$. By (3.7) and Theorem 3 we form a partial allowed sequence $u, a(1), a(2), \ldots, a(k), m$, where m is a state in M. Let m^* be some state in M^*. Now $u \mathscr{F} m^*$ by Theorem 3 but $m \mathscr{F} m^*$ (m^* does not follow m), since M is a final set. Let $a(j+1)$ be the first state in the sequence for which $a(j+1) \mathscr{F} m^*$. (Take $a(0) = u$ and $a(k+1) = m$ for notational convenience.) Thus $a(j) \mathscr{F} m^*$. Construct a partial allowed sequence $a(j), b(1), b(2), \ldots, b(h), m^*$. (Again let $b(0) = a(j)$ and $b(h+1) = m^*$ for notational convenience.) By Theorem 11 we may define $c(1) = M[a(j);\ a(j+1), b(1)]$ and $c(p) = M[b(p-1);\ b(p), c(p-1)]$ for $p = 2, 3, \ldots, h+1$. Also, by Theorem 10 we have $a(j+1) \mathscr{R} c(1) \mathscr{R} c(2) \mathscr{R} \cdots \mathscr{R} c(h+1)$. Now we obtain $a(j+1) \mathscr{F} c(h+1)$ by (3.8*b*). Also $c(h+1) \neq m^*$ since $a(j+1) \mathscr{F} m^*$ and, by Theorem 10, $m^* = b(h+1)$ and $b(h+1) \mathscr{F} c(h+1)$. Thus M^* cannot be final, in contradiction of our hypothesis.

Next assume that U is followed by a pseudo-final set T composed of states $t(0), t(1), \ldots, t(k)$. Since T is not final there must be some set $D \neq T$ such that $T \mathscr{F} D$. Construct a partial allowed sequence $t(0), \ldots, d$, where d is a state in D. Let $q(0)$ be the first state in this sequence which is not in T. Thus, we have $t(j) \mathscr{R} q(0)$ for some state $t(j)$ in T which directly precedes q in the sequence. We lose no generality by making $j = 0$, since the numbering of the states in T is arbitrary. Thus we take $t(0) \mathscr{R} q(0)$.

Construct a partial allowed sequence $t(0), \ldots, t(1), \ldots, t(k), \ldots, t(0)$ in the manner of the proof of Theorem 7, so that all states in T appear in the sequence. States in this partial allowed sequence may be renamed $p(0), p(1), p(2), \ldots, p(r), p(0)$, where $p(0) = t(0)$ and all the other k states have been renamed as one or more of the states $p(j)$. Since $u \mathscr{F} p(0)$ by Theorem 3, we may define $q(j) = M[p(j-1); p(j), q(j-1)]$ for $j = 1, 2, \ldots, r$ and $q(r+1) = M[p(r); p(0), q(r)]$ by use of Theorem 11. By Theorem 10 we have $q(0) \mathscr{R} q(1) \mathscr{R} \cdots \mathscr{R} q(r+1)$. By (3.8b) we have $q(0) \mathscr{F} q(r+1)$. Now $q(r+1)$ cannot lie in T, for if so we would have $p(0) \mathscr{R} q(0) \mathscr{F} q(r+1)$ and $q(0)$ would also lie in T. Thus $p(0) \neq q(r+1)$, so that $p(0)$ and $q(r+1)$ must differ in at least one signal, say $p_i(0) \neq q_i(r+1)$. This implies $p_i(j) \neq q_i(j)$ for all $j = 0, 1, \ldots, r$, for if $p_i(j) = q_i(j)$ then $p_i(j+1) = q_i(j+1)$ by (5.4a,b) and hence by induction $p_i(0) = q_i(r+1)$, which violates our assumption.

We assume now that $p_i(0) < q_i(0)$. Then it follows that $p_i(j) < q_i(j) \leq p_i'(j)$ for all $j = 0, 1, \ldots, r$. For assume that it is true for $j = 0, 1, \ldots, s$. Then, since $p(s) \mathscr{R} q(s)$ and $p_i(s) < q_i(s) \leq p_i'(s)$, we have $q_i(s+1) = \max[p_i(s+1), q_i(s)]$. But $q_i(s+1) \neq p_i(s+1)$ and $p(s+1) \mathscr{R} q(s+1)$ so $p_i(s+1) < q_i(s+1) \leq p_i'(s+1)$. Since $p_i(j) < p_i'(j)$ for all $j = 0, 1, \ldots, r$, we have $p_i(0) \leq p_i(1) \leq \cdots \leq p_i(r) \leq p_i(0)$. Hence $p_i(0) = p_i(j) < p_i'(j)$ for all $j = 0, 1, \ldots, r$, so that $t_i(0) = t_i(j) < t_i'(j)$ for all $j = 0, 1, \ldots, k$. This contradicts the assumption (3.16) that T is pseudo-final.

If, on the other hand, we assume that $p_i(0) > q_i(0)$, we may make a similar argument with the sense of the inequalities reversed and giving $t_i(0) = t_i(j) > t_i'(j)$ for all $j = 0, 1, \ldots, k$. This also contradicts assumption (3.16).

The condition (5.3) for semimodularity is a convenient one to use, since it is defined with respect to individual transitions which may occur between states and does not refer to allowed sequences and the system of states as a whole. These transitions may be examined individually to see if they satisfy $b \mathscr{R} a'$ whenever $a \mathscr{R} b$, but no such method seems possible if (5.1) is used. It is true that (5.3) is more restrictive than (5.1) but, in practice, no useful circuits have been found which satisfy the weaker and not the stronger condition. Parallel changes, for example, may occur under (5.3), and common computer circuits such as counters, parallel adders, and shifting registers have been designed subject to it. Although circuit design techniques will be discussed in a future paper, we should note that all these techniques require at least the assumption of semimodularity.

6. *Length of an $\mathscr{R}$-Sequence*

Partial allowed sequences in circuits which are semimodular with respect to an initial state u (such a circuit will be abbreviated sm $[u]$) exhibit important length properties. In order to study these properties, however, it is convenient to treat a somewhat more general sequence, called an $\mathscr{R}$-sequence.

An $\mathscr{R}$-sequence $a(1), a(2), \dots, a(k)$ is any finite sequence of states in which $a(i) \mathrel{\mathscr{R}} a(i+1)$ for all $i = 1, 2, \dots, k-1$. (6.1)

We note that this definition is more general than the definition of a partial allowed sequence (3.2), since the restriction $a(i) \neq a(i+1)$ has been removed. Therefore, any partial allowed sequence is an $\mathscr{R}$-sequence. Also, for any $\mathscr{R}$-sequence we can find a corresponding partial allowed sequence if subsequences consisting of equal states are replaced by single states.

In an $\mathscr{R}$-sequence $a(1), a(2), \dots, a(k)$ we say that a consecutive pair of states $a(i), a(i+1)$ is redundant if and only if $a(i) = a(i+1)$. (6.2)

Thus, a partial allowed sequence is an $\mathscr{R}$-sequence having no redundant pairs.

Given any $\mathscr{R}$-sequence $a(1), a(2), \dots, a(k)$, we define an n-dimensional "length" vector $L[a(1), a(2), \dots, a(k)]$ recursively by:

$$L[a(1)] = (0, 0, \dots, 0); \tag{6.3a}$$

$$L[a(i), a(i+1)] = (l_1, l_2, \dots, l_n), \quad \text{where} \quad l_j = |a_j(i+1) - a_j(i)|; \tag{6.3b}$$

$$L[a(1), a(2), \dots, a(i+1)] = L[a(1), a(2), \dots, a(i)] + L[a(i), a(i+1)]. \tag{6.3c}$$

Componentwise vector addition is assumed in (6.3c). One may interpret the ith component of $L[a(1), a(2), \dots, a(k)]$ as the sum of the magnitudes of the changes that have occurred in the ith signal while passing through the $\mathscr{R}$-sequence $a(1), a(2), \dots, a(k)$.

In the succeeding discussion the following vector operations will be needed:

$L[a(1), a(2), \dots, a(k)] \leq L[b(1), b(2), \dots, b(t)]$ means that each component of $L[a(1), a(2), \dots, a(k)]$ is less than or equal to the corresponding component of $L[b(1), b(2), \dots, b(t)]$. (6.4)

$L[a(1), a(2), \dots, a(k)] \vee L[b(1), b(2), \dots, b(t)]$ is a vector whose components are the pairwise maxima of the corresponding components of $L[a(1), a(2), \dots, a(k)]$ and $L[b(1), b(2), \dots, b(t)]$. (6.5)

$L[a(1), a(2), \dots, a(k)] \wedge L[b(1), b(2), \dots, b(t)]$ is a vector whose components are the pairwise minima of the corresponding components of $L[a(1), a(2), \dots, a(k)]$ and $L[b(1), b(2), \dots, b(t)]$. (6.6)

Several properties of such vectors may be readily verified. They are:

$$L[a(1), a(2), \dots, a(j), \dots, a(k)] = L[a(1), a(2), \dots, a(j)] + L[a(j), a(j+1), \dots, a(k)]; \tag{6.7}$$

$$L[a(1), a(2), \dots, a(j)] \leq L[a(1), a(2), \dots, a(k)] \quad \text{whenever} \quad j \leq k; \tag{6.8}$$

$$L[a(1), a(2), \dots, a(k)] = 0 \text{ if and only if } a(j) = a(1) \text{ for all } j = 1, 2, \dots, k. \tag{6.9}$$

As a consequence of (6.7) and (6.9) the length of an $\mathscr{R}$-sequence is unchanged if it is contracted to form a partial allowed sequence as described in the first part of this section.

Some properties of the state $M[a;b,c]$ were developed in the discussion following (5.2). Further properties concerned with length vectors may now be described.

Theorem 13: In an sm $[u]$ circuit let $u \mathscr{F} a$, $a \mathscr{R} b$, and $a \mathscr{R} c$. If we write $d = M[a;b,c]$, then $L[a,d] = L[a,b,d] = L[a,c,d] = L[a,b] \vee L[a,c]$.

Proof: By Theorem 10, $a \mathscr{R} d$, $b \mathscr{R} d$, and $c \mathscr{R} d$, so that expressions for $L[a,d]$, $L[a,b,d]$, and $L[a,c,d]$ may be written. Now by the definition of $M[a;b,c]$ given in (5.4a,b), if $a_i \leq a_i'$ we have either $a_i \leq b_i \leq c_i = d_i$ or $a_i \leq c_i \leq b_i = d_i$ or both. In either case

$$|d_i - a_i| = |d_i - b_i| + |b_i - a_i| = |d_i - c_i| + |c_i - a_i| = \max\,[|b_i - a_i|, |c_i - a_i|]. \quad (6.10)$$

Similarly, if $a_i \geq a_i'$ we have either $a_i \geq b_i \geq c_i = d_i$ or $a_i \geq c_i \geq b_i = d_i$ or both, and (6.10) still holds.

Since any $\mathscr{R}$-sequence can be contracted to a partial allowed sequence, we note that if $u \mathscr{F} a(1)$ and if $a(1), a(2), \ldots, a(k)$ is an $\mathscr{R}$-sequence then $u \mathscr{F} a(i)$ for all $i = 1, 2, \ldots, k$. We may therefore extend Theorem 11 to yield:

> Let $u \mathscr{F} a(1,1)$ in an sm $[u]$ circuit and let $a(1,1), a(1,2), \ldots, a(1,j)$ and $a(1,1), a(2,1), \ldots, a(i,1)$ be two $\mathscr{R}$-sequences. We may then define $a(r,s) = M[a(r-1, s-1); a(r-1, s), a(r, s-1)]$ recursively for $r = 2, 3, \ldots, i$ and $s = 2, 3, \ldots, j$. (6.11)

The results given in Theorem 13 and (6.11) may now be used to generalize Theorem 13 to:

Theorem 14: Under the assumptions of (6.11),

$$\begin{aligned} &L[a(1,1), a(1,2), \ldots, a(1,j), a(2,j), \ldots, a(i,j)] \\ &\qquad = L[a(1,1), a(2,1), \ldots, a(i,1), a(i,2), \ldots, a(i,j)] \\ &\qquad = L[a(1,1), a(1,2), \ldots, a(1,j)] \vee L[a(1,1), a(2,1), \ldots, a(i,1)]. \end{aligned}$$

Proof: The theorem holds trivially when either $i = 1$ or $j = 1$. Let us assume that it holds if indices (i,j) are replaced by $(i-1, j-1)$, $(i-1, j)$, or $(i, j-1)$ and prove the result by induction. By Theorem 13 we have:

$$\begin{aligned} &L[a(i-1, j-1), a(i, j-1), a(i,j)] \\ &\qquad = L[a(i-1, j-1), a(i-1, j), a(i,j)] \qquad (6.12) \\ &\qquad = L[a(i-1, j-1), a(i, j-1)] \vee L[a(i-1, j-1), a(i-1, j)]. \end{aligned}$$

We have assumed that

$$\begin{aligned} &L[a(1,1), a(1,2), \ldots, a(1, j-1); a(2, j-1), \ldots, a(i-1, j-1)] \\ &\qquad = L[a(1,1), a(2,1), \ldots, a(i-1, 1), a(i-1, 2), \ldots, a(i-1, j-1)]. \quad (6.13) \end{aligned}$$

Use is now made of the following property of numerical vectors:

If w, x, y, and z are numerical vectors and $x \vee y = z$, then $(x + w) \vee (y + w) = z + w$. (6.14)

Using properties (6.14) and (6.7) we suitably add terms of (6.13) to (6.12) and obtain:

$$\begin{aligned} &L[a(1,1), a(1,2), \ldots, a(1, j-1), a(2, j-1), \ldots, a(i, j-1)] + L[a(i, j-1), a(i,j)] \\ &\quad = L[a(1,1), a(2,1), \ldots, a(i-1, 1), a(i-1, 2), \ldots, a(i-1, j)] \\ &\quad\quad + L[a(i-1, j), a(i,j)] \\ &\quad = L[a(1,1), a(1,2), \ldots, n(1, j-1), a(2, j-1), \ldots, a(i, j-1)] \\ &\quad\quad \vee L[a(1,1), a(2,1), \ldots, a(i-1, 1), a(i-1, 2), \ldots, a(i-1, j)]. \end{aligned} \tag{6.15}$$

But by the induction hypothesis on $(i, j-1)$ we have

$$\begin{aligned} &L[a(1,1), a(1,2), \ldots, a(1, j-1), a(2, j-1), \ldots, a(i, j-1)] \\ &\quad = L[a(1,1), a(2,1), \ldots, a(i,1), a(i,2), \ldots, a(i, j-1)] \\ &\quad = L[a(1,1), a(1,2), \ldots, a(i, j-1)] \vee L[a(1,1), a(2,1), \ldots, a(i,1)]; \end{aligned} \tag{6.16}$$

and on $(i-1, j)$,

$$\begin{aligned} &L[a(1,1), a(1,2), \ldots, a(1,j), a(2,j), \ldots, a(i-1, j)] \\ &\quad = L[a(1,1), a(2,1), \ldots, a(i-1, 1), a(i-1, 2), \ldots, a(i-1, j)] \\ &\quad = L[a(1,1), a(1,2), \ldots, a(1,j)] \vee L[a(1,1), a(2,1), \ldots, a(i-1, 1)]. \end{aligned} \tag{6.17}$$

Substituting (6.16) and (6.17) in (6.15) we obtain:

$$\begin{aligned} &L[a(1,1), a(2,1), \ldots, a(i,1), a(i,2), \ldots, a(i, j-1)] + L[a(i, j-1), a(i,j)] \\ &\quad = L[a(1,1), a(1,2), \ldots, a(i,j), a(2,j), \ldots, a(i-1, j)] + L[a(i-1, j), a(i,j)] \\ &\quad = L[a(1,1), a(1,2), \ldots, a(1, j-1)] \vee L[a(1,1), a(2,1), \ldots, a(i,1)] \\ &\quad\quad \vee L[a(1,1), a(1,2), \ldots, a(1,j)] \vee L[a(1,1), a(2,1), \ldots, a(i-1, 1)]. \end{aligned} \tag{6.18}$$

In this expression we make use of a further property of numerical vectors.

If x and y are numerical vectors and if $x \leq y$, then $x \vee y = y$. (6.19)

The first and fourth terms in the last expression of (6.18) are respectively less than the third and second terms, so that (6.18) may be reduced to the equations of Theorem 14 by use of (6.7) and (6.8). Thus, by induction, Theorem 14 holds for all i and j, and the theorem is proved.

7. *Cumulative States*

The result contained in Theorem 14 may be used to simplify the theory of semimodular circuits and express it in a new form which permits many of the properties of such circuits to be easily demonstrated. This reformulation involves introducing the notion of a cumulative state (to be abbreviated C-state), which not only determines the state of the circuit but also the important features of the partial allowed sequence through which the circuit passed in reaching this state.

A cumulative state (or C-state) $\mathbf{a}$ of a partial allowed sequence $u, a(1), a(2), \ldots, a(k), a$ in an sm[u] circuit is defined as $L[u, a(1), a(2), \ldots, a(k), a]$. (7.1)

A C-state, thus, is an n-dimensional vector having nonnegative integral components, since it is equal to the length of a partial allowed sequence. Although a partial allowed sequence whose length is $\mathbf{a}$ must exist in order to define the C-state $\mathbf{a}$, we note that more than one such sequence may exist, as was demonstrated in Theorem 13. The state u in (7.1) is called the initial state and a the terminal state corresponding to $\mathbf{a}$ and its partial allowed sequence.

Theorem 15: In an sm [u] circuit if $\mathbf{a}$ is a C-state having initial state u, then the terminal state of $\mathbf{a}$ is uniquely determined independently of which partial allowed sequence is used to define $\mathbf{a}$.

Proof: This result is proved trivially in the binary case, because the components of $\mathbf{a}$ are simply the numbers of changes which have occurred in the signals while passing from u to the terminal state. Thus the respective signals of this terminal state will either agree or disagree with those of u, depending upon whether an even or an odd number of changes have occurred and consequently upon whether the corresponding components of $\mathbf{a}$ are even or odd.

In the general case we must use Theorem 14 to prove uniqueness. Let us assume two partial allowed sequences correspond to $\mathbf{a}$ so that

$$\begin{aligned}\mathbf{a} &= L[u, a(1,2), a(1,3), \ldots, a(1,j)]\\ &= L[u, a(2,1), a(3,1), \ldots, a(i,1)].\end{aligned}$$

Then by Theorem 14 we may form $\mathscr{R}$-sequences such that

$$\begin{aligned}&L[u, a(1,2), a(1,3), \ldots, a(1,j), a(2,j), \ldots, a(i,j)]\\ &\quad = L[u, a(1,2), a(1,3), \ldots, a(1,j)] \vee L[u, a(2,1), a(3,1), \ldots, a(i,1)] = \mathbf{a} \vee \mathbf{a} = \mathbf{a}.\end{aligned}$$

Thus we have

$$\mathbf{a} + L[a(1,j), a(2,j), \ldots, a(i,j)] = \mathbf{a};$$

hence

$$L[a(1,j), a(2,j), \ldots, a(i,j)] = 0$$

by (6.7), and (6.9) yields $a(1,j) = a(i,j)$. A similar argument gives us $a(j,1) = a(i,j)$, and the two terminal states are identical.

Since the terminal state is determined by the C-state (and the initial state u) we shall use the notation $t(\mathbf{a})$ to represent the terminal state corresponding to $\mathbf{a}$ or, when convenient, use the same letter designation (in this case $a = t(\mathbf{a})$) for it.

Of particular interest are the relations between the C-states which have a particular state u as their initial state. The set of such C-states (which may be infinite) will be called $C[u]$. Such a set of C-states will be shown to form a semimodular lattice under a suitable ordering. It is for this reason that we have used the term semimodular in the description of circuits.

The set $C[u]$ will be used to display the properties of semimodular circuits more easily and completely than is possible merely using the notion of allowed sequences.

We begin by defining the $\mathscr{F}$ relation with respect to C-states:

If $\mathbf{a}$ and $\mathbf{b}$ are in $C[u]$, with terminal states a and b respectively, we define $\mathbf{a} \mathscr{F} \mathbf{b}$ to mean that there exists a partial allowed sequence $a, a(1), a(2), \ldots, a(k), b$ such that $L[a, a(1), a(2), \ldots, a(k), b] + \mathbf{a} = \mathbf{b}$. (7.2)

Using this definition and (7.1) we may restate Theorem 14 as follows.

If $\mathbf{a}$ and $\mathbf{b}$ are in $C[u]$, then $\mathbf{c} = \mathbf{a} \vee \mathbf{b}$ is in $C[u]$, and $\mathbf{a} \mathscr{F} \mathbf{c}$ and $\mathbf{b} \mathscr{F} \mathbf{c}$. (7.3)

This theorem in the form given above is now used to show that $C[u]$ is a lattice under the $\mathscr{F}$ relation.

Theorem 16: Given $\mathbf{a}$ and $\mathbf{b}$ in $C[u]$, then $\mathbf{a} \mathscr{F} \mathbf{b}$ if and only if $\mathbf{a} \leq \mathbf{b}$.

Proof: Assume $\mathbf{a} \mathscr{F} \mathbf{b}$ so that by (7.2) there is a partial allowed sequence $a, a(1), a(2), \ldots, a(k), b$ such that $L[a, a(1), a(2), \ldots, a(k), b] + \mathbf{a} = \mathbf{b}$. Since the length vector has nonnegative components we have $\mathbf{a} \leq \mathbf{b}$.

Assume $\mathbf{a} \leq \mathbf{b}$. Then $\mathbf{a} \vee \mathbf{b} = \mathbf{b}$ and, by (7.3), $\mathbf{a} \mathscr{F} \mathbf{a} \vee \mathbf{b} = \mathbf{b}$, and the theorem is proved.

We see from Theorem 16 that the elements of $C[u]$ are partially ordered under the relation, since it is equivalent to the $\leq$ relation of numerical vectors, which defines a partial ordering.

By combining (7.3) and Theorem 16 we may extend Theorem 14 further, to another form. This form of Theorem 14, given in Theorem 17, provides a simpler and more natural way of stating this basic concept.

Theorem 17: If $\mathbf{a}$ and $\mathbf{b}$ are in $C[u]$, then $\mathbf{a} \vee \mathbf{b}$ is in $C[u]$ and is their least upper bound under the $\mathscr{F}$ relation.

Proof: That $\mathbf{a} \vee \mathbf{b}$ is an upper bound in $C[u]$ follows from (7.3). It is also a least upper bound since it is a numerical least upper bound, and by Theorem 16 this is equivalent to its being a least upper bound under the $\mathscr{F}$ relation. Hence, we shall use the notation $\mathbf{a} \cup \mathbf{b}$ (the least upper bound of $\mathbf{a}$ and $\mathbf{b}$) interchangeably with $\mathbf{a} \vee \mathbf{b}$.

Theorem 18: If a and b are in $C[u]$, then their greatest lower bound (written $\mathbf{a} \cap \mathbf{b}$) in $C[u]$ exists.

Proof: The set of all C-states $\mathbf{m}$ such that $\mathbf{m} \mathscr{F} \mathbf{a}$ and $\mathbf{m} \mathscr{F} \mathbf{b}$ is finite since all such $\mathbf{m}$ must have nonnegative integral components which are all less than or equal to the corresponding components of $\mathbf{a}$. Let us designate these C-states as $\mathbf{m}(1), \mathbf{m}(2), \ldots, \mathbf{m}(j)$. This set is nonempty since we may form a C-state $\mathbf{0}$, whose components are all zero, from the partial allowed sequence consisting only of the initial state u. By Theorem 16 $\mathbf{0} \mathscr{F} \mathbf{x}$ for all $\mathbf{x}$ in $C[u]$ and, therefore, is a lower bound of a and b. Now form $\mathbf{m}(1) \cup \mathbf{m}(2) \cup \cdots \cup \mathbf{m}(j) = \mathbf{c}$. By Theorem 17 we have $\mathbf{c} \mathscr{F} \mathbf{a}$ and $\mathbf{c} \mathscr{F} \mathbf{b}$, and yet $\mathbf{m}(i) \mathscr{F} \mathbf{c}$ for all $\mathbf{m}(i)$. Hence $\mathbf{c} = \mathbf{a} \cap \mathbf{b}$.

Combining the results, Theorems 16, 17, and 18, and the discussion of $\mathbf{0}$ in the foregoing proof we have:

Theorem 19: $C[u]$ is a lattice with a zero under the partial ordering relation $\mathscr{F}$.

It should be observed at this point that $\mathbf{a} \cap \mathbf{b}$, while the greatest lower bound of a and b in $C[u]$ is not necessarily the numerical intersection $\mathbf{a} \wedge \mathbf{b}$. This latter vector may not be a C-state in $C[u]$, although, if it is, the two intersections are equal by Theorem 16.

We now wish to show that the lattice of Theorem 19 is a semimodular lattice. This is done most easily by introducing an $\mathscr{R}$ relation among the C-states in $C[u]$:

$$\mathbf{a} \mathscr{R} \mathbf{b} \text{ means } a \mathscr{R} b \text{ and } \mathbf{b} = L[a,b] + \mathbf{a}. \tag{7.4}$$

Here it is understood that $a = t(\mathbf{a})$ and $b = t(\mathbf{b})$. By (7.1), we note that if a is in $C[u]$ and $a \mathscr{R} b$ we may always form b in $C[u]$ so that $\mathbf{a} \mathscr{R} \mathbf{b}$. Thus we may go on to define

$$\mathbf{a}' = L[a,a'] + \mathbf{a}, \tag{7.5}$$

for any a in $C[u]$, since $a \mathscr{R} a'$ by (3.1). By (7.4) we see that $\mathbf{a} \mathscr{R} \mathbf{a}'$ for all a. Using these definitions we may parallel some of the results in Secs. 3 and 5, with the C-states in $C[u]$ replacing the states of S. The following theorem is analogous to (3.1):

Theorem 20: $\mathbf{a} \mathscr{R} \mathbf{b}$ if and only if $\mathbf{a} \leq \mathbf{b} \leq \mathbf{a}'$. (Note that by Theorem 16 this condition is equivalent to $\mathbf{a} \mathscr{F} \mathbf{b} \mathscr{F} \mathbf{a}'$.)

Proof: If $\mathbf{a} \mathscr{R} \mathbf{b}$ we have $a \mathscr{R} b$, so that for each signal we have either $a_i \leq b_i \leq a_i'$ or $a_i \geq b_i \geq a_i'$ and in either case $|b_i - a_i| \leq |a_i' - a_i|$; but since $a \mathscr{R} b$ and $a \mathscr{R} a'$ this implies $|b_i - a_i| = \mathrm{b}_i - \mathrm{a}_i$ and $|a_i - a_i'| = \mathrm{a}_i - \mathrm{a}_i'$, where a_i, b_i, and a_i' are the ith components of a, b, and a′. Thus $\mathbf{b} \leq \mathbf{a}'$ and, since $|b_i - a_i| \geq 0$, we have $\mathbf{a} \leq \mathbf{b}$.

Assume next that $\mathbf{a} \leq \mathbf{b} \leq \mathbf{a}'$. Construct a state b^* as follows: Let $b_i^* = a_i + (\mathrm{b}_i - \mathrm{a}_i)$ if $a_i \leq a_i'$ and let $b_i^* = a_i - (\mathrm{b}_i - \mathrm{a}_i)$ if $a_i > a_i'$. Then, since $|a_i' - a_i| = \mathrm{a}_i' - \mathrm{a}_i$, we have $a_i \leq b_i^* \leq a_i'$ if $a_i \leq a_i'$, and $a_i \geq b_i^* \geq a_i'$ if $a_i > a_i'$. Hence $a \mathscr{R} b^*$. But $b^* = b$ since $L[a,b^*] = \mathbf{b} - \mathbf{a}$, and (7.4) is therefore satisfied.

Theorem 21: If $\mathrm{a}\ \mathscr{R}\ \mathrm{b}$ then $\mathrm{b}\ \mathscr{R}\ \mathrm{a}'$.

Proof: This result is analogous to (5.3). From (5.3) we have $b\ \mathscr{R}\ a'$. We need only show that $L[b,a'] + \mathrm{b} = \mathrm{a}'$. Since $|a_i' - b_i| + |b_i - a_i| = |a_i' - a_i|$ by (3.1), we have

$$L[a,b] + L[b,a'] = L[a,a']$$

and

$$\begin{aligned} L[b,a'] &= L[a,a'] - L[a,b] = (\mathrm{a}' - \mathrm{a}) - (\mathrm{b} - \mathrm{a}) \\ &= \mathrm{a}' - \mathrm{b}. \end{aligned}$$

Theorem 22: If $\mathrm{a}\ \mathscr{R}\ \mathrm{c}$ and $\mathrm{a} \leq \mathrm{b} \leq \mathrm{c}$, then $\mathrm{a}\ \mathscr{R}\ \mathrm{b}\ \mathscr{R}\ \mathrm{c}$.

Proof: By Theorem 20, $\mathrm{c} \leq \mathrm{a}'$, so $\mathrm{a} \leq \mathrm{b} \leq \mathrm{a}'$ and hence $\mathrm{a}\ \mathscr{R}\ \mathrm{b}$. Also, by Theorem 21, $\mathrm{b}\ \mathscr{R}\ \mathrm{a}'$, so $\mathrm{a}' \leq \mathrm{b}'$ and hence $\mathrm{b} \leq \mathrm{c} \leq \mathrm{a}' \leq \mathrm{b}'$ and $\mathrm{b}\ \mathscr{R}\ \mathrm{c}$.

Theorem 23: If $\mathrm{a}\ \mathscr{R}\ \mathrm{b}$ and $\mathrm{a}\ \mathscr{R}\ \mathrm{c}$ then $\mathrm{a}\ \mathscr{R}\ (\mathrm{b} \cup \mathrm{c})$.

Proof: Since $\mathrm{a} \leq \mathrm{b} \leq \mathrm{a}'$ and $\mathrm{a} \leq \mathrm{c} \leq \mathrm{a}'$, we have $\mathrm{a} \leq \mathrm{b} \cup \mathrm{c} \leq \mathrm{a}'$; hence $\mathrm{a}\ \mathscr{R}\ (\mathrm{b} \cup \mathrm{c})$ by Theorem 20.

Theorem 24: If $\mathrm{a}\ \mathscr{R}\ \mathrm{b}$ and $\mathrm{a}\ \mathscr{R}\ \mathrm{c}$, then $\mathrm{b} \cap \mathrm{c} = \mathrm{b} \wedge \mathrm{c}$.

Proof: While Theorems 21, 22, and 23 are analogous to properties of the states of S which were given in Secs. 3 and 5, the result, Theorem 24, is not. Since $a\ \mathscr{R}\ b$ and $a\ \mathscr{R}\ c$ we may define a state d as follows:

$$\begin{aligned} d_i &= \min\,[b_i,c_i], &\text{if}\quad a_i &\leq a_i'; \\ d_i &= \max\,[b_i,c_i], &\text{if}\quad a_i &\geq a_i'. \end{aligned}$$

Since b_i and c_i both satisfy the conditions of (3.1), we see that d_i does too and $a\ \mathscr{R}\ d$. Also $|d_i - a_i| = \min\,[|b_i - a_i|, |c_i - a_i|]$, so $L[a,d] = L[a,b] \wedge L[a,c]$ and, if we let $\mathrm{d} = \mathrm{a} + L[a,d]$, then, by (6.14), $\mathrm{d} = \mathrm{b} \wedge \mathrm{c}$. Thus $\mathrm{b} \wedge \mathrm{c}$ is in $C[u]$, and since it is a numerical greatest lower bound we see that $\mathrm{b} \cap \mathrm{c} = \mathrm{b} \wedge \mathrm{c}$.

It is now possible to prove:

Theorem 25: The lattice $C[u]$ is semimodular.

Proof: A lattice is said to be semimodular if the following condition is satisfied:

> If x, y, and a are three elements such that x and y cover a and $\mathrm{x} \neq \mathrm{y}$, then $\mathrm{x} \cup \mathrm{y}$ covers x and y.[3] (7.6)

In the present lattice $C[u]$ we express the "covers" relation as follows:

> If r and s are in $C[u]$, then s covers r if and only if $\mathrm{r}\ \mathscr{F}\ \mathrm{s}$, $\mathrm{r} \neq \mathrm{s}$, and $\mathrm{r}\ \mathscr{F}\ \mathrm{t}\ \mathscr{F}\ \mathrm{s}$ implies either $\mathrm{r} = \mathrm{t}$ or $\mathrm{t} = \mathrm{s}$.[4] (7.7)

We now seek to prove (7.6). First we show that x covers a implies $\mathrm{a}\ \mathscr{R}\ \mathrm{x}$. Since $\mathrm{a}\ \mathscr{F}\ \mathrm{x}$, there is a partial allowed sequence from a to x such that $L[a, a(1), \ldots, a(k), x] = \mathbf{x} - \mathbf{a}$. But this implies that $\mathbf{a}(1) = \mathbf{a} + L[a, a(1)]$ is such that $\mathbf{a}\,\mathscr{R}\,\mathbf{a}(1)\,\mathscr{F}\,\mathbf{x}$, and by (7.7) this means that $\mathbf{a}(1) = \mathbf{x}$, so that the partial allowed sequence contains only two members, a and x. Hence $\mathbf{a}\,\mathscr{R}\,\mathbf{x}$. Similarly $\mathbf{a}\,\mathscr{R}\,\mathbf{y}$, and, by Theorem 23, $\mathbf{a}\,\mathscr{R}\,\mathbf{x} \cup \mathbf{y}$.

Secondly, we show that $\mathbf{x} \cup \mathbf{y}$ covers $\mathbf{x}$. Let $\mathbf{b}$ be any C-state such that $\mathbf{x}\,\mathscr{F}\,\mathbf{b}\,\mathscr{F}\,\mathbf{x} \cup \mathbf{y}$. Now, by Theorem 22 we have $a\,\mathscr{R}\,b$ and by Theorem 24, $\mathbf{y} \cap \mathbf{b} = \mathbf{y} \wedge \mathbf{b}$. Using the distributive properties of numerical vectors,

$$\mathbf{x} \vee (\mathbf{y} \wedge \mathbf{b}) = (\mathbf{x} \vee \mathbf{y}) \wedge (\mathbf{x} \vee \mathbf{b}) = (\mathbf{x} \vee \mathbf{y}) \wedge \mathbf{b} = \mathbf{b}.$$

Since $\mathbf{a}\,\mathscr{F}\,\mathbf{y} \wedge \mathbf{b}\,\mathscr{F}\,\mathbf{y}$, by (7.7), either $\mathbf{y} \wedge \mathbf{b} = \mathbf{a}$ or $\mathbf{y} \wedge \mathbf{b} = \mathbf{y}$, so in the former case $\mathbf{x} = \mathbf{x} \vee \mathbf{a} = \mathbf{x} \vee (\mathbf{y} \wedge \mathbf{b}) = \mathbf{b}$, and in the latter, $\mathbf{x} \vee \mathbf{y} = \mathbf{x} \vee (\mathbf{y} \wedge \mathbf{b}) = \mathbf{b}$. Hence $\mathbf{x} \vee \mathbf{y}$ covers $\mathbf{x}$ by (7.7), and similarly $\mathbf{x} \vee \mathbf{y}$ covers $\mathbf{y}$.

An alternative proof of Theorem 25 may be obtained if a closer investigation is made into the nature of the "covers" relation.

Theorem 26: $\mathbf{b}$ covers $\mathbf{a}$ if and only if there is one component index i such that $\mathbf{b}_i = \mathbf{a}_i + 1$ and $\mathbf{b}_j = \mathbf{a}_j$ whenever $j \neq i$.

Proof: If $\mathbf{b}_i = \mathbf{a}_i + 1$ and $\mathbf{b}_j = \mathbf{a}_j$ whenever $j \neq i$, then $\mathbf{a}\,\mathscr{F}\,\mathbf{b}$ by Theorem 16 and, since the C-states must have integral components, (7.7) is satisfied so that $\mathbf{b}$ covers $\mathbf{a}$.

If, on the other hand, $\mathbf{b}$ covers $\mathbf{a}$, then, by the proof of Theorem 19, $\mathbf{a}\,\mathscr{R}\,\mathbf{b}$ and $a\,\mathscr{R}\,b$. Since $\mathbf{a} \neq \mathbf{b}$ there must be some signal index i such that $\mathbf{a}_i < \mathbf{b}_i$. Thus $\mathbf{b}_i - \mathbf{a}_i = |b_i - a_i| > 0$, and either $a_i < b_i \leq a_i'$ or $a_i > b_i \geq a_i'$. Define a state b^* in S by letting $b_j^* = a_j$ for $j \neq i$ and $b_i^* = a_i + 1$ if $a_i < a_i'$ but $b_i^* = a_i - 1$ if $a_i > a_i'$. To show that b^* is in S we note that b_j^* is in S_j, since a_j is in S_j, and b_i^* is in S_i, since either $a_i < b_i^* \leq a_i'$ or $a_i > b_i \geq a_i'$ and both a_i and a_i' are in S_i. Thus we may write $a\,\mathscr{R}\,b^*$, and, if we let $\mathbf{b}^* = \mathbf{a} + L[a,b^*]$, then $\mathbf{a}\,\mathscr{R}\,\mathbf{b}^*$. But $\mathbf{b}^* \leq \mathbf{b}$, so $\mathbf{a}\,\mathscr{F}\,\mathbf{b}^*\,\mathscr{F}\,\mathbf{b}$, and since $\mathbf{a} \neq \mathbf{b}$ we must have $\mathbf{b}^* = \mathbf{b}$ by (7.7). However, $\mathbf{b}^*$ has the properties required of $\mathbf{b}$ in Theorem 26.

The proof of Theorem 26 is unique in that it requires the construction of a state b^* in S, and thus makes use of the assumption (2.2) that S is the set of all n-tuples of signals taken from the sets S_i. It is true that constructions have been used before; specifically they have been used in (5.4) and Theorem 24. In these two constructions somewhat weaker assumptions were involved, as we shall see.

In the original choice of signals (2.1) and functions (2.3) the assumption (2.2) amounts to assuming that these signals are independent of each other, so that not only do they describe the state of the circuit, but this description is not redundant. This puts the burden on the circuit designer to make certain that the signals he uses to describe the circuit are independent in the sense that he is not using two or more signals to measure some quantity which could be measured by one signal. If two signals were not independent in this sense, the effect would be to make the value of one signal uniquely dependent upon the value of the other, and the states of S would be correspondingly limited. Now in the constructions of (5.4) and Theorem 24 such dependence between signals is not violated, while in Theorem 26 it is. Thus the assumption of independence of the signals has not been used except in the proof of Theorem 26.

A further assumption is also involved in Theorem 26 which is not used elsewhere; it is that all the signal levels z_i in the sets S_i may actually occur. This means that the designer must be sure that the k_i signal levels in each set S_i are realizable in the actual circuit. In (5.4) and Theorem 24 only signal levels in existing states are used in the construction of new states, while in Theorem 26 a new signal level may be introduced.

Thus we see that new assumptions which were not used in the proofs of previous results occur in the proof of Theorem 26. It is for this reason that the proof of Theorem 25 was made independently of Theorem 26. A simpler proof that $C[u]$ is semimodular may be obtained if we use Theorem 26.

Alternative proof of Theorem 25: We wish to show that, if $\mathbf{x}$ and $\mathbf{y}$ cover $\mathbf{a}$, then $\mathbf{x} \cup \mathbf{y}$ covers $\mathbf{x}$ and $\mathbf{y}$. By Theorem 26 there are two signal indices i and j such that $\mathbf{x}_i = \mathbf{a}_i + 1$ and $\mathbf{x}_k = \mathbf{a}_k$ if $k \neq i$, and $\mathbf{y}_j = \mathbf{a}_j + 1$ and $\mathbf{y}_k = \mathbf{a}_k$ if $k \neq j$. We see that $i \neq j$, since in the hypothesis of Theorem 25 $\mathbf{x} \neq \mathbf{y}$. Thus if $\mathbf{x} \cup \mathbf{y} = \mathbf{b}$ we have $\mathbf{b}_i = \mathbf{a}_i + 1$ and $\mathbf{b}_j = \mathbf{a}_j + 1$, $\mathbf{b}_k = \mathbf{a}_k$ if $k \neq i$ and $k \neq j$. Therefore, by Theorem 26, $\mathbf{b}$ covers $\mathbf{x}$ and $\mathbf{y}$.

Another theorem that involves the construction of a state, and will be needed later on, is the following:

Theorem 27: Let $\mathbf{a}$ be a C-state in $C[u]$ for which $\mathbf{a}_i \neq \mathbf{a}_i'$. Then there exists a C-state $\mathbf{b}$ in $C[u]$ such that $\mathbf{b}_j = \mathbf{a}_j$ for $j \neq i$, and $\mathbf{b}_i = \mathbf{a}_i + 1$.

Proof: Let a be the terminal state of $\mathbf{a}$. Since $\mathbf{a}_i \neq \mathbf{a}_i'$, then either $a_i < a_i'$ or $a_i > a_i'$. In the former case define the state b by $b_j = a_j$ for $j \neq i$ and $b_i = a_i + 1$. Then b is a state in S, since $a \mathscr{R} b$, and the C-state $\mathbf{b} = \mathbf{a} + L[a,b]$ satisfies the theorem. If, on the other hand, $a_j > a_i'$, then the state b would be defined as $b_j = a_j$ for $j \neq i$ and $b_i = a_i - 1$.

We note that under the hypothesis of Theorem 27 $\mathbf{b}$ covers $\mathbf{a}$ as a consequence of Theorem 26.

To illustrate the relation between states and C-states, consider the example of the following binary circuit:

$$\begin{aligned} z_1' &= z_2z_3 \vee z_1z_2 \vee z_1z_3, \\ z_2' &= \bar{z}_1, \\ z_3' &= \bar{z}_1. \end{aligned} \tag{7.8}$$

This circuit, if represented by a logical diagram, would consist of two "not" elements and a special element C for producing the function $z_2z_3 \vee z_1z_2 \vee z_1z_3$. This element has the property that its output z_1 tends to agree with the two inputs z_2 and z_3 if they agree with each other, but it retains its old value if they disagree. This circuit is illustrated in Fig. 2.

Let us assume that the circuit is placed in the state (0,1,1). It must then pass to the state (1,1,1). This state may lead to either of the states (1,0,1) or (1,1,0). Whichever of these occurs, the circuit will then pass to (1,0,0) and then to (0,0,0). This state may change so as to become either (0,1,0) or (0,0,1), but either of these leads back to the initial state (0,1,1). We may check that (5.3) is satisfied in each transition, but that (5.2) is not, so the circuit is semimodular but not totally sequential. Since the circuit never reaches equilibrium, its lattice $C[u]$ of C-states is infinite. This lattice is partly illustrated in Fig. 3 for $u = (0,1,1)$. In this figure the terminal state corresponding to any C-state may be obtained by adding $u = (0,1,1)$ to the C-state and taking residues of each component modulo 2.

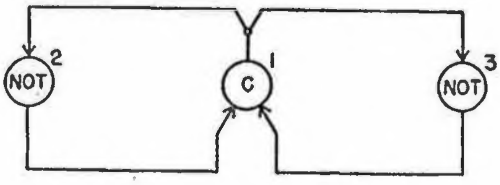

FIG. 2. Logical diagram defined by Eqs. (7.8).

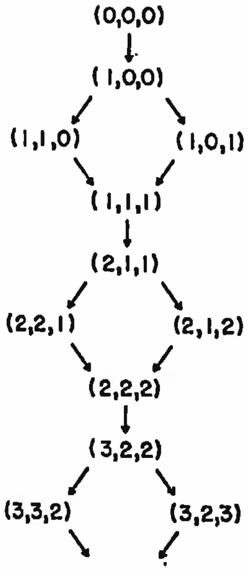

FIG. 3. Partial lattice diagram of C-states for $u = (0,1,1)$.

8. *Cycling Theory*

It was observed that it is possible for a state to recur in a partial allowed sequence. Since the behavior of the circuit depends only on the state, we should expect a repetitive behavior when states may recur. In the present section we shall study this repetitive behavior when it occurs in semimodular circuits.

Let v be in $C[u]$; then make the following definitions:

D[v] is the set of all C-states a in $C[u]$ such that v $\mathscr{F}$ a, and (8.1*a*)

E[v] is the set of all C-states a in D[v] such that t[v] $=$ t[a]. (8.1*b*)

We note that $E[\mathbf{v}]$ contains only $\mathbf{v}$ unless the state $t(\mathbf{v})$ may recur. Also it is easily verified that $D[\mathbf{v}]$ is a sublattice of $C[u]$.

Theorem 28: If $\mathbf{v}$ is in $C[u]$, then the lattice $C[v]$ and the sublattice $D[\mathbf{v}]$ are isomorphic under the transformation $\mathbf{a}^* = \mathbf{v} + \mathbf{a}$, where $\mathbf{a}^*$ is in $D[\mathbf{v}]$ and $\mathbf{a}$ is in $C[v]$.

Proof: Let $\mathbf{a}$ be a C-state in $C[v]$. Then there is a partial allowed sequence from v to a such that $L[v, a(1), \ldots, a(k), a] = \mathbf{a}$. Then since $\mathbf{v}$ is in $C[u]$ we also have a partial allowed sequence from u to v such that $L[u, v(1), \ldots, v(l), v] = \mathbf{v}$. Thus $\mathbf{a}^* = L[u, v(1), \ldots, v(l), v, a(1), \ldots, a(k), a]$ is a C-state in $C[u]$. Also, $\mathbf{a}^*$ is in $D[\mathbf{v}]$ since $\mathbf{v} \mathscr{F} \mathbf{a}^*$ and $\mathbf{a}^* = \mathbf{v} + \mathbf{a}$. Hence for every $\mathbf{a}$ in $C[v]$ there is a corresponding $\mathbf{a}^*$ in $D[\mathbf{v}]$. Similarly, for every $\mathbf{a}^*$ in $D[\mathbf{v}]$, since $\mathbf{v} \mathscr{F} \mathbf{a}^*$, we have a partial allowed sequence from v to a such that $L[v, a(1), \ldots, a(k), a] + \mathbf{v} = \mathbf{a}^*$. Thus there is one-to-one correspondence between the C-states.

We note also that ordering relations in the two lattices $C[v]$ and $D[\mathbf{v}]$ are identical since, by Theorem 16, the ordering is numerical and numerical ordering is preserved under the transformation $\mathbf{a}^* = \mathbf{v} + \mathbf{a}$ between corresponding elements in $C[v]$ and $D[\mathbf{v}]$. Hence the lattices are isomorphic.

A corollary to Theorem 28 is:

Corollary: In a circuit which is sm $[u]$ and sm $[u^*]$, if $\mathbf{v}$ is in $C[u]$ and $\mathbf{v}^*$ is in $C[u^*]$ and $t(\mathbf{v}) = t(\mathbf{v}^*) = v$, then $D[\mathbf{v}]$ is isomorphic with $D[\mathbf{v}^*]$ under the transformation $\mathbf{v}^* + \mathbf{a} = \mathbf{v} + \mathbf{a}^*$, where $\mathbf{a}$ is in $D[\mathbf{v}]$ and $\mathbf{a}^*$ is in $D[\mathbf{v}^*]$.

This result follows from Theorem 28, since $D[\mathbf{v}]$ and $D[\mathbf{v}^*]$ are both isomorphic with $C[v]$.

Theorem 28 and the corollary show that the lattice properties of $D[\mathbf{v}]$ are independent of the initial state u, provided, of course, that $u \mathscr{F} v$. In other words, the behavior of the circuit after having passed through state v is independent of the initial state u of the circuit and depends only on v. The fact that the numerical components of the vectors in $D(\mathbf{v})$ have their fiducial values altered (by $\mathbf{v}^* - \mathbf{v}$) when the initial state is altered is merely a consequence of the way the C-states are defined and does not reflect a physical property of the circuit. The lattice relations $\mathscr{F}$, $\cup$, and $\cap$, as well as the $\mathscr{R}$ relation, are invariant under such translations, as is the circuit behavior which we are seeking to describe with them.

Two properties of recurring states will now be developed.

Theorem 29: If $\mathbf{a}$ and $\mathbf{b}$ are in $C[u]$ and $t(\mathbf{a}) = t(\mathbf{b})$, then $t(\mathbf{a} \cup \mathbf{b}) = t(\mathbf{a}) = t(\mathbf{b})$.

Proof: Let $\mathbf{c} = \mathbf{a} \cup \mathbf{b}$ and let $c = t(\mathbf{c})$. Then for any component $\mathbf{c}_i = \max\{\mathbf{a}_i, \mathbf{b}_i\}$. Assume $\mathbf{a}_i \geq \mathbf{b}_i$, so $\mathbf{c}_i = \mathbf{a}_i$. Then, since $\mathbf{a} \mathscr{F} \mathbf{c}$, we may form a partial allowed sequence from $a = t(\mathbf{a})$ to c, such that $L[a, c(1), \ldots, c(k), c] = \mathbf{c} - \mathbf{a}$. Since the ith component of this vector is zero, the ith signal has not changed in going from a to c, and $a_i = c_i$. Similarly, if $\mathbf{b}_i \geq \mathbf{a}_i$, we have $b_i = c_i$. But $a_i = b_i = t(\mathbf{a})_i = t(\mathbf{b})_i$, so in any case $t(\mathbf{c})_i = t(\mathbf{a})_i = t(\mathbf{b})_i$ for all components, and $t(\mathbf{a} \cup \mathbf{b}) = t(\mathbf{a}) = t(\mathbf{b})$.

Theorem 30: If $\mathbf{a}$ and $\mathbf{b}$ are in $C[u]$ and $a = t(\mathbf{a})$, $b = t(\mathbf{b})$ are in two equivalence sets A and B, where $A \mathscr{F} B$, then $t(\mathbf{a} \cup \mathbf{b})$ is in B.

Proof: By Theorem 3, $a \mathscr{F} b$, so we may form a partial allowed sequence from a to b. Define $\mathbf{b}^* = \mathbf{a} + L[a, b(1), \ldots, b(k), b]$, and $t(\mathbf{b}^*) = b$. Also $\mathbf{a} \mathscr{F} \mathbf{b}^*$. Let $\mathbf{b}^{**} = \mathbf{b} \cup \mathbf{b}^*$. Thus $\mathbf{a} \mathscr{F} \mathbf{b}^{**}$ and $\mathbf{b} \mathscr{F} \mathbf{b}^{**}$, so $\mathbf{a} \cup \mathbf{b} \mathscr{F} \mathbf{b}^{**}$ and hence $t(\mathbf{a} \cup \mathbf{b}) \mathscr{F} b$. But, since $\mathbf{b} \mathscr{F} \mathbf{a} \cup \mathbf{b}$, we have $b \mathscr{F} t(\mathbf{a} \cup \mathbf{b})$, and $t(\mathbf{a} \cup \mathbf{b})$ must be in B.

We now define a set of numerical vectors associated with any C-state which will serve to describe the cycling properties of the circuit.

Given $\mathbf{v}$ in $C[u]$, we define a set $W[\mathbf{v}]$ of numerical vectors $w(1), w(2), \ldots, w(k)$, having nonnegative integral components, by the following rule: $W[\mathbf{v}]$ contains all nonzero vectors $w(i)$ such that $\mathbf{v} + w(i)$ is in $E[\mathbf{v}]$ and if $\mathbf{a}$ is in $E[\mathbf{v}]$ with $\mathbf{v} \mathscr{F} \mathbf{a} \mathscr{F} \mathbf{v} + w(i)$ then either $\mathbf{a} = \mathbf{v}$ or $\mathbf{a} = \mathbf{v} + w(i)$. (8.2*a*)

The statement (8.2*a*) involves the "covers" concept and, in fact, may be restated as:

$w(i)$ is in $W[\mathbf{v}]$ if and only if $\mathbf{v} + w(i)$ covers $\mathbf{v}$ in $E[\mathbf{v}]$. (8.2*b*)

The set $W[\mathbf{v}]$ may, of course, be empty, in which case we shall say that $k = 0$. No limit is set on k by the definition but it will appear later that k cannot be greater than n.

Incidentally, it may be noted that the components of the vectors $w(i)$ are always even integers, since they represent a number of changes in the signals which bring them back to their initial values, and the number of negative changes must equal the number of positive changes.

Theorem 31: If $W[\mathbf{v}]$ is a set of vectors as defined above, $w(i) \vee w(j) = w(i) + w(j)$, when $i \neq j$.

Proof: We must not have $w(i) < w(j)$, for then $\mathbf{v} < \mathbf{v} + w(i) < \mathbf{v} + w(j)$, in violation of (8.2). Hence $w(j) < w(i) \vee w(j)$. By the numerical properties of vectors, and using (6.14), $w(i) \vee w(j) \leq w(i) + w(j)$ and hence $\mathbf{v} + w(j) < \mathbf{v} + [w(i) \vee w(j)] = [\mathbf{v} + w(i)] \vee [\mathbf{v} + w(j)] \leq \mathbf{v} + w(i) + w(j)$. Let $\mathbf{v}^* = \mathbf{v} + w(j)$. We now show that all expressions in this inequality are in $E[\mathbf{v}^*]$. The expression $[\mathbf{v} + w(i)] \vee [\mathbf{v} + w(j)]$ is in $E[\mathbf{v}]$ by Theorem 29; but it exceeds $\mathbf{v}^*$ so it is in $E[\mathbf{v}^*]$. Also $\mathbf{v} + w(i) + w(j) = \mathbf{v}^* + w(i)$, and is in $E[\mathbf{v}^*]$ by the corollary to Theorem 28 with $u = u^*$.

We now write the isomorphic expressions by the corollary to Theorem 28 with $u^* = u$. They are $\mathbf{v} < \mathbf{v} + [w(i) \vee w(j)] - w(j) \leq \mathbf{v} + w(i)$, and all expressions are now in $E[\mathbf{v}]$. Then by (8.2*b*) we obtain $[w(i) \vee w(j)] - w(j) = w(i)$.

In order for the relation $w(i) \vee w(j) = w(i) + w(j)$ to hold for vectors having nonnegative components, the nonzero components of $w(i)$ and $w(j)$ must have distinct component indices. Since this is true for all pairs of vectors in $W[\mathbf{v}]$ we have:

Corollary: The vectors $w(1), w(2), \ldots, w(k)$ of $W[\mathbf{v}]$ all have distinct indices for their nonzero components.

In other words, if $w_m(i) > 0$, then $w_m(j) = 0$ for all $j \neq i$. This also means that the vectors of W[v] are orthogonal in the vector sense, that is, the inner product of $w(i)$ and $w(j)$ is zero if and only if $i \neq j$.

A consequence of this corollary is the restriction $k \leq n$ which was mentioned earlier. In case $k = n$ each $w(i)$ has just one nonzero component and one $w(i)$ would correspond to each component index.

We shall describe the component indices of the nonzero components of $w(i)$ as the set of component indices *spanned* by $w(i)$. Furthermore, we shall designate the set of component indices spanned by any of the k vectors of W[v] as the set of component indices spanned by W[v].

Theorem 32: The set E[v] is precisely the set of vectors x which may be expressed in the form

$$\mathbf{x} = \mathbf{v} + \sum_{i=1}^{k} a_i w(i), \tag{8.3}$$

where the coefficients a_i are allowed to run over the nonnegative integers.

Proof: If

$$\mathbf{x} = \mathbf{v} + \sum_{i=1}^{k} a_i w(i),$$

then we show that x is in E[v] by induction. Certainly x = v is in E[v], which is the case in which the coefficients a_i are all zero. Assume next that

$$\mathbf{x} = \mathbf{v} + \sum_{i=1}^{k} a_i w(i)$$

is in E[v] for a given set of coefficients a_i. Since t(v) = t(x) then, by the corollary to Theorem 28, with $u = u^*$, we have x + $w(j)$ is in E[x] since v + $w(j)$ is in E[v]. Hence x + $w(j)$ is in E[v], and we see that any coefficient a_j may be increased by 1 (and hence by any integer) to yield a new x in E[v].

Next assume that x is in E[v]. Induction is used to show that x may be expressed in the form (8.3). Form a covering sequence of C-states in E[v] from v to x. (This is shown to be possible in reference 3, page 6.) Let us assume that some member y of this sequence may be expressed in the form (8.3). We note that v is such a member. Let z be the next member of the sequence after y so that z covers y in E[v]. Then by the corollary to Theorem 28, v + (z − y) covers v, and hence by (8.2b) we see that (z − y) is one of the vectors $w(i)$ in W[v]. Since z = y + $w(i)$ we see that z is also expressible in the form (8.3), and by induction so is x.

Cycling with respect to the set E[v] is completely described by Theorem 32, since we see that v has periodicity of multiplicity k.

We now turn to the investigation of the dependence of W[v] on v.

Theorem 33: If $\mathbf{v}$ is in $C[u]$ and $\mathbf{v}^*$ is in $C[u^*]$ and $v = t(\mathbf{v}) = t(\mathbf{v}^*)$, then $W[\mathbf{v}] = W[\mathbf{v}^*]$.

Proof: By the corollary to Theorem 28, $D[\mathbf{v}]$ is isomorphic with $D[\mathbf{v}^*]$ under the transformation $\mathbf{v}^* + \mathbf{a} = \mathbf{v} + \mathbf{a}^*$. We see that, since the $w(i)$ in $W[\mathbf{v}]$ are differences between members of $D[\mathbf{v}]$, they are invariant under the transformation.

We shall therefore be able to write $W[v]$ to represent $W[\mathbf{v}]$ for all $\mathbf{v}$ such that $t(\mathbf{v}) = v$.

Theorem 34: In an sm $[u]$ circuit, if $u \mathscr{F} a \mathscr{F} b$, then any member of $W[a]$ is a sum of one or more members of $W[b]$.

Proof: Since $u \mathscr{F} a \mathscr{F} b$ we may construct partial allowed sequences from u to a to b, and thereby define some C-states $\mathbf{a}$ and $\mathbf{b}$ as $\mathbf{a} = L[u, a(1), \ldots, a(p), a]$ and $\mathbf{b} = \mathbf{a} + L[a, b(1), \ldots, b(q), b]$. We have defined $\mathbf{a}$ and $\mathbf{b}$ so that $a = t(\mathbf{a})$ and $b = t(\mathbf{b})$ and $\mathbf{a} \mathscr{F} \mathbf{b}$. Thus $\mathbf{b}$ is in $D[\mathbf{a}]$. By the corollary to Theorem 28, if $w(j,a)$ is in $W[\mathbf{a}]$ then $D[\mathbf{a}]$ is isomorphic with $D[\mathbf{a} + w(j,a)]$, and thus we have a correspondence between $\mathbf{b}$ and $\mathbf{b} + w(j,a)$. Hence $\mathbf{b} + w(j,a)$ is in $E[\mathbf{b}]$ and must be expressible in the form (8.3), so that $w(j,a)$ may be written in the form

$$w(j,a) = \sum_{i=1}^{k} c_i w(i,b),$$

where the c_i's are nonnegative integers, not all zero, and the vectors $w(i,b)$ are the members of $W[\mathbf{b}]$. Now, since $W[a] = W[\mathbf{a}]$ and $W[b] = W[\mathbf{b}]$, we have proved Theorem 34.

A corollary to Theorem 34 is the result that the number k of vectors can never decrease while passing through an allowed sequence. Thus, k has in common with entropy the property of never decreasing with time. It is also apparent that indices once spanned by a vector $w(i)$ will remain spanned throughout the remainder of an allowed sequence.

Our picture of the behavior of a semimodular circuit as it passes through an allowed sequence now involves an increasing number of vectors $w(i)$ being introduced and increasingly more indices being spanned. Also, we may imagine old vectors $w(i)$ breaking up into several vectors, each one spanning fewer nodes than the old $w(i)$.

Theorem 35: In an sm $[u]$ circuit, if $u \mathscr{F} a$ and a and b are in the same equivalence set A, then $W[a] = W[b]$.

Proof: Since $a \mathscr{F} b$, if $w(i,a)$ is in $W[a]$, then, by Theorem 34, $w(i,a)$ is a sum of one or more members of $W[b]$, so if $w(j,b)$ is in this sum we have $w(i,a) \geq w(j,b)$, since the vectors have nonnegative components. Similarly, since $b \mathscr{F} a$, there is a $w(h,a)$ in $W[a]$ such that $w(j,b) \geq w(h,a)$. But by the corollary to Theorem 31, if $w(i,a) \geq w(h,a)$, we must have $h = i$ and $w(i,a) = w(h,a)$, and hence $w(i,a) = w(j,b)$. Hence, for every $w(i,a)$ in $W[a]$ there is an equal $w(j,b)$ in $W[b]$, and similarly for every $w(j,b)$ in $W[b]$ there is an equal $w(i,a)$ in $W[a]$. Thus the two sets contain exactly the same vectors, and $W[a] = W[b]$.

This means that we may write $W[A]$ to represent the set of vectors corresponding to the equivalence set A. The set of vectors $w(i)$ now appears as a function of equivalence sets where originally it was defined as a function of C-states. We shall also use the notation **a** contained in **A** to denote that $t(\mathbf{a})$ is an element of the equivalence set A. Finally we shall say that a component i is unspanned by $W[A]$ if and only if the ith component of a C-state in **A** is unspanned by any of the vectors $w(j)$ of $W[A]$.

Theorem 36: **a** and **b** both lie in **A** if and only if those components of **a** and **b** unspanned by $W[A]$ are identical.

Proof: Assume that a and b are in the same equivalence set A. Form $\mathbf{c} = \mathbf{a} \cup \mathbf{b}$. By Theorem 30 we have $c = t(\mathbf{c})$ also in A. Hence $c \mathscr{F} a$, and we may construct a partial allowed sequence from c to a, and define $\mathbf{a}^* = \mathbf{c} + L[\mathbf{c}, a(1), \ldots, a(r), a]$. Since $\mathbf{a} \mathscr{F} \mathbf{c} \mathscr{F} \mathbf{a}^*$, we have $\mathbf{a}_j \le \mathbf{c}_j \le \mathbf{a}_j^*$ for each component index j. Now

$$\mathbf{a}^* = \mathbf{a} + \sum_{i=1}^{k} q_i w(i)$$

by Theorem 32; so for those components $\mathbf{a}_j$ not spanned by the $w(i)$'s we have $\mathbf{a}_j = \mathbf{a}_j^*$, and hence $\mathbf{a}_j = \mathbf{c}_j$ for unspanned components. Similarly, $\mathbf{b}_j = \mathbf{c}_j$ for unspanned components, giving $\mathbf{a}_j = \mathbf{b}_j$.

Assume now that **a** and **b** have identical unspanned components. Let $\mathbf{b}_{i\,\max}$ be the largest spanned component of **b**. If no components are spanned, let $\mathbf{b}_{i\,\max} = 0$. Then form

$$\mathbf{a}^* = \mathbf{a} + \mathbf{b}_{i\,\max} \sum_{i=1}^{k} w(i),$$

where the $w(i)$ are taken from $W[\mathbf{a}]$. Then $\mathbf{b} \mathscr{F} \mathbf{a}^*$, so $b \mathscr{F} a$ by Theorem 32. Similarly we have $a \mathscr{F} b$.

Theorem 37: If **a** and **b** lie in **A** and index i is unspanned by $W[A]$, then $\mathbf{a}_i' = \mathbf{b}_i'$.

Proof: We begin by proving that $a_i' = b_i'$. Construct a partial allowed sequence $a, a(1), a(2), \ldots, a(p), a$, which contains all states in A, by the method given in the proof of Theorem 12. We notice that $a', a'(1), a'(2), \ldots, a'(p), a'$ is an $\mathscr{R}$-sequence, because, by (5.3), $a(j) \mathscr{R} a(j+1)$ implies $a(j+1) \mathscr{R} a'(j)$, and hence $a'(j) \mathscr{R} a'(j+1)$ for each $i = 1, 2, \ldots, p-1$ and similarly $a' \mathscr{R} a'(1)$ and $a'(p) \mathscr{R} a'$. (It may not be a partial allowed sequence since some consecutive pairs may be equal.) By our hypothesis index i is unspanned by $W[A]$, so that $a_i = a_i(1) = a_i(2) = \cdots = a_i(p)$. Assume that $a_i < a_i'$. Then $a_i = a_i(1) < a_i' \le a_i'(1)$, and in general $a_i(j+1) < a_i'(j) \le a_i'(j+1)$. Thus we have $a_i' \le a_i'(1) \le a_i'(2) \le \cdots \le a_i'(p) \le a_i'$, so that $a_i' = a_i'(j)$ for all $j = 1, 2, \ldots, p$. Similarly, $a_i' = a_i'(j)$ for all $j = 1, 2, \ldots, p$, if we assume $a_i > a_i'$.

In the remaining case $a_i = a_i'$, if j exists such that $a_i(j) \ne a_i'(j)$, then by the previous argument we have $a_i' = a_i'(j)$, giving the contradiction $a_i = a_i' = a_i'(j) \ne a_i(j) = a_i$. Therefore, in this case too we have $a_i' = a_i'(j)$ for all $j = 1, 2, \ldots, p$. But since all states of A are included in the sequence $a, a(1), a(2), \ldots, a(p), a$ we see that $a_i' = b_i'$ for any pair of states in A.

Now let $\mathbf{a}$ and $\mathbf{b}$ be any two C-states in $\mathbf{A}$. Then $\mathbf{a}' = \mathbf{a} + L[a,a']$ and $\mathbf{b}' = \mathbf{b} + L[b,b']$. But $\mathbf{a}_i = \mathbf{b}_i$ by Theorem 36, and $|a_i' - a_i| = |b_i' - b_i|$, so $\mathbf{a}_i' = \mathbf{b}_i'$.

Two corollaries are immediate. They are:

Corollary A: For any $\mathbf{a}$ in $\mathbf{A}$ there exists a unique $\mathbf{A}'$ for which $\mathbf{a}'$ is in $\mathbf{A}'$ and $A \mathscr{F} A'$.

Corollary B: If A is final and i is unspanned by $W[A]$, then $\mathbf{a}_i = \mathbf{a}_i'$ for any $\mathbf{a}$ in A.

Thus we see that the unspanned components of the C-states, and hence the unspanned signals of the states, characterize the equivalence sets. Within equivalence sets only spanned components and signals change, while in going from one equivalence set to another the unspanned components and signals must change. In such a transition the number of unspanned components may decrease, and, if it does, the number k of vectors must increase. It is possible, as we shall see later, for the number k of vectors to increase without having a decrease in the number of unspanned components.

It also should be observed that the unspanned signals of the states uniquely determine the unspanned components of the C-states, since these are fixed by the equivalence set.

As an example consider the circuit defined by the equations

$$\begin{aligned} z_1' &= 1, \\ \bar{z}_2' &= \bar{z}_1\bar{z}_3 \vee z_1\bar{z}_2, \\ z_3' &= \bar{z}_1 z_2 \vee z_1\bar{z}_3. \end{aligned} \tag{8.4}$$

If the circuit is started in the initial state $u = (0,0,0)$, it may be shown to be semimodular. Two equivalence sets occur. They may be designated A and B as follows: A contains (0,0,0), (0,1,0), (0,1,1), (0,0,1); B contains (1,0,0), (1,1,0), (1,1,1), (1,0,1). In the circuit $A \mathscr{F} B$, so B is a final set. The first signal is the only one unspanned by vectors $w(i)$ in either set. $W[A]$ contains just one vector (0,2,2). $W[B]$ contains [0,2,0] and [0,0,2]. Here we have an example of a single vector from $W[A]$ splitting into two in $W[B]$. In this case the same number of unspanned signals occurs in both A and B, but this will not be the case in general.

9. *Ideals of* $C[u]$

While investigating the behavior of asynchronous circuits one is often concerned with what happens if a signal fails to change when it is supposed to do so. Malfunctions of this type never lead to C-states which are not in $C[u]$, since no assumptions have been made about the relative speeds of the elements.

Another problem, which is of interest to the circuit designer, is to find a way of describing the apparent behavior of a circuit to an observer who is not aware of all the signals which are present, but "sees" only certain signals from among the entire set. This problem and the preceding one will be treated by investigating the ideals of $C[u]$.

In order to represent the ideals of $C[u]$, we introduce the notion of a C-signal. This concept will also be useful in the theory of distributive circuits, which are treated in Sec. 10.

For each pair of integers α and i, such that there exists at least one C-state $\mathbf{a}$ in $C[u]$ for which $\mathbf{a}_i = \alpha$, we define the C-signal (α,i) as the set of all C-states $\mathbf{b}$ in $C[u]$ having $\mathbf{b}_i \leq \alpha$. The C-state $\mathbf{a}$ is then said to induce the C-signal (α,i). (9.1)

The C-signal (α,i) thus refers to the αth change which has occurred at point i in the circuit and, more specifically, contains all C-states in $C[u]$ for which no more than α signal changes have occurred at point i. It therefore describes the possible C-states which may occur if point i is prevented from changing more than α times. To describe what may happen if several signals fail to change, we introduce the notion of a break set.

If a C-state $\mathbf{a}$ in $C[u]$ induces all the distinct C-signals (α_1,i_1), (α_2,i_2), . . . , (α_m,i_m), we define the break set $\boldsymbol{\alpha} = [(\alpha_1,i_1), (\alpha_2,i_2), \ldots, (\alpha_m,i_m)]$ as the set of all C-states $\mathbf{b}$ having $\mathbf{b}_{i_j} \leq \alpha_j$ for $j = 1, 2, \ldots, m$. The C-state $\mathbf{a}$ is then said to induce the break set $\boldsymbol{\alpha}$. (9.2)

It will appear later that m cannot be greater than n, since in Theorem 39 it is shown that the indices i_j are distinct. We shall, however, admit the possibility that $m = 0$ as a special case. This break set $\boldsymbol{\theta} = [\ ]$ will be taken equal to $C[u]$, and all C-states in $C[u]$ will be said to induce it.

We note that the C-signals are, themselves, break sets referring to single C-signals. In other words, $[(\alpha,i)] = (\alpha,i)$.

Theorem 38: If for each of the m C-signals (α_j,i_j), where $j = 1, 2, \ldots, m$, there is a C-state $\mathbf{a}(j)$ inducing (α_j,i_j) and contained in the other C-signals, then $\boldsymbol{\alpha} = [(\alpha_1,i_1), (\alpha_2,i_2), \ldots, (\alpha_m,i_m)]$ is a break set.

This follows from (9.2) if we let $\mathbf{a} = \mathbf{a}(1) \cup \mathbf{a}(2) \cup \cdots \cup \mathbf{a}(m)$.

Theorem 39: If $\boldsymbol{\alpha} = [(\alpha_1,i_1), (\alpha_2,i_2), \ldots, (\alpha_m,i_m)]$ is any break set, the signal indices $i_1, i_2, \ldots, i_m$ are distinct.

Proof: Let $\mathbf{a}$ induce $\boldsymbol{\alpha}$. If $i_p = i_q$, then, by (9.2), $\alpha_p = \mathbf{a}_{i_p} = \mathbf{a}_{i_q} = \alpha_q$, which conflicts with the assumption that the C-signals are distinct.

Theorem 40: Any break set is an ideal of $C[u]$.

Proof: Ideals of $C[u]$ are defined as nonempty subsets of $C[u]$ having the following two properties:

An ideal J contains $\mathbf{x} \cup \mathbf{y}$ if it contains $\mathbf{x}$ and $\mathbf{y}$. (9.3*a*)

If $\mathbf{x}$ and $\mathbf{y}$ are C-states in $C[u]$, and if $\mathbf{x}$ is in an ideal J, then $\mathbf{x} \cap \mathbf{y}$ is also in J. (9.3*b*)

Property (9.3*a*) also applies to break sets by Theorem 17. We may infer (9.3*b*) from Theorem 16 and the fact that $\mathbf{x} \cap \mathbf{y} \mathscr{F} \mathbf{x}$.

Theorem 41: Any ideal of $C[u]$ can be represented as a break set in at least one way.

Proof: Let J be an ideal of $C[u]$. It should be noted that since J is nonempty it must contain at least the C-state 0, whose components are all zero. List all C-signals (α_1,i_1), $(\alpha_2,i_2), \ldots, (\alpha_m,i_m)$ such that (α_j,i_j) is induced by some C-state $\mathbf{a}(j)$ in J, where there is no C-signal (β_j,i_j) with $\beta_j > \alpha_j$ which is induced by a C-state in J (that is, α_j is maximal). Our list may contain no more than n C-signals by virtue of its definition, and, if some index i_{m+1} is not represented in the list, then every C-signal (α_{m+1}, i_{m+1}) is induced by a C-state in J, since $(0, i_{m+1})$ is induced by $\mathbf{0}$ in J. Let the C-states in J inducing these C-signals be denoted by $\mathbf{a}(1), \mathbf{a}(2), \ldots, \mathbf{a}(m)$. If $m > 0$ we have $\mathbf{a} = \mathbf{a}(1) \cup \mathbf{a}(2) \cup \cdots \cup \mathbf{a}(m)$ in J by (9.3a), and from the construction of each $\mathbf{a}(j)$ we see that $\mathbf{a}$ induces a break set

$$\boldsymbol{\alpha} = [(\alpha_1,i_1), (\alpha_2,i_2), \ldots, (\alpha_m,i_m)].$$

By (9.2), $\boldsymbol{\alpha}$ contains J. If $m = 0$ we let $\boldsymbol{\alpha} = \boldsymbol{\theta} = C[u]$, which must contain J.

To show that J contains $\boldsymbol{\alpha}$, let $\mathbf{x}$ be a C-state in $\boldsymbol{\alpha}$. Now for each component $\mathbf{x}_p$ of $\mathbf{x}$ we can find a C-state $\mathbf{b}(p)$ in J such that $\mathbf{b}_p(p) \geq \mathbf{x}_p$. Let $\mathbf{b} = \mathbf{b}(1) \cup \mathbf{b}(2) \cup \cdots \cup \mathbf{b}(n)$. Then $\mathbf{b}$ is in J by (9.3a). But $\mathbf{x} \mathscr{F} \mathbf{b}$ so $\mathbf{x} = \mathbf{x} \cap \mathbf{b}$ is in J by (9.3b). Hence J contains $\boldsymbol{\alpha}$, so $J = \boldsymbol{\alpha}$.

We see from Theorems 40 and 41 that the break-set notation is simply a way of specifying ideals. It is well known that the ideals of $C[u]$ form a lattice. The relation of this lattice to $C[u]$ is expressed in (9.4).

The ideals of $C[u]$ form a lattice under set inclusion. In this lattice $\boldsymbol{\alpha} \cup \boldsymbol{\beta}$ is the set of all elements of the form $(\mathbf{a} \cup \mathbf{b}) \cap \mathbf{c}$, where $\mathbf{a}$ and $\mathbf{b}$ are in $\boldsymbol{\alpha}$ and $\boldsymbol{\beta}$ respectively, and $\mathbf{c}$ is any C-state. The ideal $\boldsymbol{\alpha} \cap \boldsymbol{\beta}$, on the other hand, is merely the set-theoretical meet, containing all elements in both $\boldsymbol{\alpha}$ and $\boldsymbol{\beta}$. (9.4)

Various subsets of the lattice of ideals are important from the point of view of circuit behavior. One such subset is defined thus:

$H[u; i_1, i_2, \ldots, i_m]$ is the set of ideals of $C[u]$ which may be represented in the form $\boldsymbol{\alpha} = [(\alpha_1,i_1), (\alpha_2,i_2), \ldots, (\alpha_m,i_m)]$, where the quantities α_j may range over all values permitted by (9.2). (9.5)

This set may be regarded as describing the behavior of the circuit to an observer who merely detected the signals at points $i_1, i_2, \ldots, i_m$. To such an observer the ideals of $H[u; i_1, i_2, \ldots, i_m]$ would correspond to the C-states of an ordinary observer. Such sets also provide the basis for a theory of equivalent circuits. Two circuits could be called equivalent if $H[u; i_1, i_2, \ldots, i_m]$ in the first circuit is the same as $H[v; j_1, j_2, \ldots, j_m]$ in the second circuit. This type of equivalence is defined with respect to initial states u and v and selected signal indices in the two circuits.

The set $H[u; 1,2, \ldots, n]$ is isomorphic with the lattice $C[u]$, where set inclusion replaces the $\mathscr{F}$ relation. Also, $H[u,i]$ is merely a chain. Our suspicion that $H[u; i_1, i_2, \ldots, i_m]$ is a lattice under set inclusion will be shown to be justified, but it is not necessarily a sublattice of the lattice of ideals. We begin with Theorem 42 which is analogous to Theorem 16.

Theorem 42: If $\boldsymbol{\alpha}$ and $\boldsymbol{\beta}$ are in $H[u; i_1, i_2, \ldots, i_m]$, then $\boldsymbol{\alpha} \subseteq \boldsymbol{\beta}$ if and only if $\alpha_j \leq \beta_j$ for $j = 1, 2, \ldots, m$.

Proof: If $\alpha_j \leq \beta_j$ for $j = 1, 2, \ldots, m$, we see by (9.2) that $\boldsymbol{\alpha} \subseteq \boldsymbol{\beta}$. If a induces $\boldsymbol{\alpha}$, we have $\mathbf{a}_{i_j} = \alpha_j$. If, now, $\boldsymbol{\alpha} \subseteq \boldsymbol{\beta}$, we also have a in $\boldsymbol{\beta}$; hence $\mathbf{a}_{i_j} \leq \beta_j$ for $j = 1, 2, \ldots, m$, and therefore $\alpha_j \leq \beta_j$ for $j = 1, 2, \ldots, m$.

Theorem 43: $H[u; i_1, i_2, \ldots, i_m]$ is a lattice under set inclusion.

Proof: Let $\boldsymbol{\alpha}$ and $\boldsymbol{\beta}$ be two ideals in $H[u; i_1, i_2, \ldots, i_m]$. Define $\boldsymbol{\gamma}$ by the relation $\gamma_j = \max\,[\alpha_j, \beta_j]$ for $j = 1, 2, \ldots, m$. We see that $\boldsymbol{\gamma}$ is an ideal in $H[a; i_1, i_2, \ldots, i_m]$, since if a and b induce $\boldsymbol{\alpha}$ and $\boldsymbol{\beta}$, respectively, a $\cup$ b must induce $\boldsymbol{\gamma}$ by Theorem 17. By Theorem 42, $\boldsymbol{\gamma}$ contains $\boldsymbol{\alpha}$ and $\boldsymbol{\beta}$. It is also a least upper bound in $H[u; i_1, i_2, \ldots, i_m]$, since any other upper bound must contain $\boldsymbol{\gamma}$ by Theorem 42.

To show that $\boldsymbol{\alpha}$ and $\boldsymbol{\beta}$ have a greatest lower bound in $H[u; i_1, i_2, \ldots, i_m]$, we follow an argument similar to that of Theorem 18. Let $\boldsymbol{\omega} = [(0,i_1), (0,i_2), \ldots, (0,i_m)]$ be the ideal in $H[u; i_1, i_2, \ldots, i_m]$ induced by the C-state 0. By Theorem 42 we see that $\boldsymbol{\omega}$ is a lower bound to $\boldsymbol{\alpha}$ and $\boldsymbol{\beta}$, and thus there is at least one lower bound. Now, if we form the least upper bound of all lower bounds to $\boldsymbol{\alpha}$ and $\boldsymbol{\beta}$, we see that the result must be the greatest lower bound by the construction of the previous paragraph and Theorem 42.

A result analogous to Theorem 25 may also be obtained for the set $H[u; i_1, i_2, \ldots, i_m]$.

Theorem 44: $\boldsymbol{\alpha}$ covers $\boldsymbol{\beta}$ in $H[u; i_1, i_2, \ldots, i_m]$ if and only if there is one index i_j such that $\alpha_j = \beta_j + 1$ and $\alpha_p = \beta_p$ whenever $i_p \neq i_j$.

Proof: If $\alpha_j = \beta_j + 1$ and $\alpha_p = \beta_p$ whenever $i_p \neq i_j$, then $\boldsymbol{\alpha}$ must cover $\boldsymbol{\beta}$ in $H[u; i_1, i_2, \ldots, i_m]$ by Theorem 42, since all the quantities involved are integers.

Next assume that $\boldsymbol{\alpha}$ covers $\boldsymbol{\beta}$. To complete the proof we require the following lemma, which is valid for any ideal $\boldsymbol{\alpha}$.

Lemma: If b is in $\boldsymbol{\alpha}$ and a induces $\boldsymbol{\alpha}$, then a $\cup$ b induces $\boldsymbol{\alpha}$.

Since $\alpha_j = \mathbf{a}_{i_j}$ and $\alpha_j \geq \mathbf{b}_{i_j}$ by (9.2), we have $\mathbf{b}_{i_j} \leq \mathbf{a}_i$ and $\mathbf{a}_{i_j} \vee \mathbf{b}_{i_j} = \alpha_j$, so a $\cup$ b induces $\boldsymbol{\alpha}$.

Returning to the original proof, we let a and b be two C-states inducing $\boldsymbol{\alpha}$ and $\boldsymbol{\beta}$ respectively, so by the lemma given above a $\cup$ b induces $\boldsymbol{\alpha}$. Since b $\mathscr{F}$ a $\cup$ b, we may form a covering sequence b, c(1), . . . , c(p), a $\cup$ b. Let c(i) be the last C-state in the sequence which induces $\boldsymbol{\beta}$. By Theorem 42 all previous C-states in the sequence induce $\boldsymbol{\beta}$ and all later C-states induce $\boldsymbol{\alpha}$, and no other ideals in $H[u; i_1, i_2, \ldots, i_m]$ may be induced by members of the sequence. Since c(i) and c($i + 1$) differ by 1 in just one component, by Theorem 25, we see that $\boldsymbol{\beta}$ and $\boldsymbol{\alpha}$ may differ in no more than one C-signal, and in that, by at most 1. But since $\boldsymbol{\beta}$ and $\boldsymbol{\alpha}$ are different ideals, we obtain Theorem 44.

A correspondence between equivalence sets and certain ideals will now be developed which permits us to predict the behavior of a circuit in which certain signal changes are arrested. In particular, we shall be interested in determining whether or not the circuit will stop if certain signal changes fail to occur when they are expected to do so.

These questions are treated by considering the subset of the ideals defined in (9.6).

> $K[u]$ is the set of all ideals $\boldsymbol{\alpha} = [(\alpha_1,i_1), (\alpha_2,i_2), \ldots, (\alpha_m,i_m)]$, such that there exists a C-state **a** inducing $\boldsymbol{\alpha}$ whose unspanned component indices are just $i_1, i_2, \ldots, i_m$. (9.6)

Again, if there is a C-state **a** having no unspanned component indices, we shall adopt the convention that $\boldsymbol{\theta} = [\ ]$ is a member of $K[u]$.

Theorem 45: The partially ordered set of equivalence sets $A, B, \ldots$ which follow U (the equivalence set of u) is isomorphic with $K[u]$, where the $\mathscr{F}$ relation corresponds to set inclusion.

Proof: Let **a** be in **A**, and let **a** induce $\boldsymbol{\alpha}$ in $K[u]$. By Theorem 36 we see that every other C-state in **A** also induces $\boldsymbol{\alpha}$. Thus for every equivalence set $A, B, \ldots$ there is a corresponding ideal in $K[u]$, and by definition (9.6) there is an equivalence set for every ideal in $K[u]$.

We now show the correspondence between the $\mathscr{F}$ relation over sets $A, B, \ldots$ and set inclusion over $K[u]$. Given $\boldsymbol{\beta} \subseteq \boldsymbol{\alpha}$ with $\boldsymbol{\alpha}$ and $\boldsymbol{\beta}$ in $K[u]$, then if **a** induces $\boldsymbol{\alpha}$ and **b** induces $\boldsymbol{\beta}$ we have $\mathbf{a} \cup \mathbf{b}$ induces $\boldsymbol{\alpha}$, by the lemma in the proof of Theorem 44. Since $\mathbf{b} \mathscr{F} \mathbf{a} \cup \mathbf{b}$, we have $B \mathscr{F} A$.

Assume next that $B \mathscr{F} A$, where $U \mathscr{F} B$. Let a be a state in A and b be a state in B. Form C-states $\mathbf{b} = L[u, \ldots, b]$ and $\mathbf{a} = \mathbf{b} + L[b, \ldots, a]$. We thus have **a** in **A** and **b** in **B**, with $\mathbf{b} \mathscr{F} \mathbf{a}$. Now, by Theorem 34, the unspanned indices of A are also unspanned in B, so each index i_j of $\boldsymbol{\alpha}$ is also present in $\boldsymbol{\beta}$. Since $\mathbf{b} \mathscr{F} \mathbf{a}$ with **b** inducing $\boldsymbol{\beta}$ and **a** inducing $\boldsymbol{\alpha}$ we have $\beta_j \leq \alpha_j$ for each α_j of $\boldsymbol{\alpha}$. Thus $\boldsymbol{\beta} \subseteq \boldsymbol{\alpha}$ by (9.2).

This latter argument may also be used in proving the next theorem.

Theorem 46: If **b** is in $\boldsymbol{\alpha}$ and induces $\boldsymbol{\beta}$, where $\boldsymbol{\alpha}$ and $\boldsymbol{\beta}$ are both in $K[u]$, then $\boldsymbol{\beta} \subseteq \boldsymbol{\alpha}$.

Proof: If **a** induces $\boldsymbol{\alpha}$, then $\mathbf{a} \cup \mathbf{b}$ induces $\boldsymbol{\beta}$ by the lemma in the proof of Theorem 44; and, since $\mathbf{b} \mathscr{F} \mathbf{a} \cup \mathbf{b}$, we see that $\boldsymbol{\alpha}$ and $\boldsymbol{\beta}$ are related as in the previous argument with $\mathbf{a} \cup \mathbf{b}$ replacing **a**.

Theorem 47: $K[u]$ is a lattice under set inclusion.

Proof: Let $\boldsymbol{\alpha}$ and $\boldsymbol{\beta}$ be two ideals in $K[u]$, and let $\boldsymbol{\gamma}$ be the ideal in $K[u]$ induced by $\mathbf{a} \cup \mathbf{b}$, where **a** and **b** induce $\boldsymbol{\alpha}$ and $\boldsymbol{\beta}$, respectively. By Theorem 34, the unspanned indices of $\mathbf{a} \cup \mathbf{b}$ are also unspanned in **a** and **b**, so $\boldsymbol{\gamma}$ is independent of which **a** and **b** are chosen. Also, since **a** and **b** are in $\boldsymbol{\gamma}$, we have $\boldsymbol{\alpha} \subseteq \boldsymbol{\gamma}$ and $\boldsymbol{\beta} \subseteq \boldsymbol{\gamma}$, by Theorem 46. Let $\boldsymbol{\delta}$ be any other ideal in $K[u]$ satisfying $\alpha \subseteq \delta$ and $\beta \subseteq \delta$. Then δ must contain $\mathrm{a} \cup \mathrm{b}$ by (9.3*a*), and hence $\gamma \subseteq \delta$ by Theorem 46. Thus γ is the least upper bound of α and β in $K[u]$.

Let μ be the ideal of $K[u]$ corresponding to U (the set of u). Thus $\mu \subseteq \alpha$ and $\mu \subseteq \beta$ by Theorem 45, and μ is a lower bound to α and β. The least upper bound of all lower bounds to α and β is their greatest lower bound by Theorem 46.

From the preceding discussion we see that the sets $K[u]$ and $H[u; i_1, i_2, \ldots, i_m]$ are similar in many of their characteristics. Theorems 42 and 46 may be regarded as analogous, and the proofs of Theorems 43 and 47 show that the rules for forming least upper bounds are the same. Nothing corresponding to Theorem 44 can be obtained for $K[u]$, however.

Let us now take an arbitrary ideal $\gamma = [(\gamma_1,i_1), (\gamma_2,i_2), \ldots, (\gamma_m,i_m)]$ of $C[u]$. We may regard γ as representing those C-states which may occur if the signals at points $i_1, i_2, \ldots, i_m$ in the circuit are prevented from undergoing more than $\gamma_1, \gamma_2, \ldots, \gamma_m$ changes. If γ is a principal ideal, and hence has a maximum C-state, the circuit will stop when this C-state is reached. We now wish to see what conditions must be placed on γ to require that it be a principal ideal.

$K[u;\gamma]$ is the set of all ideals α in $K[u]$ such that there is a C-state a in γ which induces α. (9.7)

This means that $K[u;\gamma]$ corresponds to the set of equivalence sets which have representative C-states in γ.

Theorem 48: If α and β are both in $K[u;\gamma]$, then their least upper bound in $K[u]$ is also in $K[u;\gamma]$.

Proof: Let a and b both lie in γ, where a induces α and b induces β. Then $\mathrm{a} \cup \mathrm{b}$ is also in γ; but $\mathrm{a} \cup \mathrm{b}$ induces the least upper bound of α and β, by the proof of Theorem 47, so it is also in $K[u;\gamma]$.

Since the number of equivalence sets is finite, we see that $K[u;\gamma]$ contains a finite number of ideals. This implies the following theorem:

Theorem 49: There is a maximum ideal ϕ in $K[u;\gamma]$.

Corresponding to this maximum ideal ϕ there is an equivalence set F which must follow all other equivalence sets represented in γ. Thus we see that, if the circuit is constrained to remain in γ, it will eventually reach F. Whether or not the circuit will stop when it reaches F will depend on whether or not cycling can occur in F.

Theorem 50: γ is a principal ideal if and only if each $w(j)$ in $W[F]$ has at least one component index of a nonzero component which is represented in γ.

Proof: Assume that γ is a principal ideal. Then its maximum element f is in F. If $w(j)$ has no nonzero component index represented in γ, then $\mathrm{f} + w(j)$ is also in γ, contradicting the assumption that f is maximal.

Assume next that each $w(j)$ has at least one nonzero component index i_j represented in γ. Let (γ_j, i_j) be the corresponding C-signal. Then, if **f** is any C-state in **F**, we see that no C-state in **F** and γ can exceed

$$\mathbf{f} + \sum_{j=1}^{k} \gamma_j \, w(j)$$

without violating (9.2). Thus a maximal C-state in γ exists, and since γ is an ideal, it is unique.

This result allows us to predict whether or not cycling may occur within γ, provided we know the unspanned indices and C-signal corresponding to each equivalence set and the vectors $w(j)$.

The following example of a binary, semimodular circuit shows that equivalence sets are not necessarily lattices of C-states and that $K[u]$ need not be a sublattice of the lattice of ideals.

This circuit is represented by the Boolean equations:

$$\begin{aligned} z_1' &= \bar{z}_3 \vee \bar{z}_1, \\ z_2' &= \bar{z}_3 \vee \bar{z}_2, \\ z_3' &= z_1 \vee z_2 \vee z_3. \end{aligned} \tag{9.8}$$

Let the initial state u be (0,0,0). A partial lattice diagram of C-states may be drawn as shown in Fig. 4. The diagram should be continued downward in an infinite, two-dimensional array of C-states. Five equivalence sets are present corresponding to the four individual states (0,0,0), (1,0,0), (0,1,0), (1,1,0) and the set of states (1,0,1), (0,1,1), (0,0,1), (1,1,1). The latter set has two minimal C-states inducing its ideal. Only index 3 is unspanned in this set which has the two vectors (2,0,0) and (0,2,0) corresponding to it.

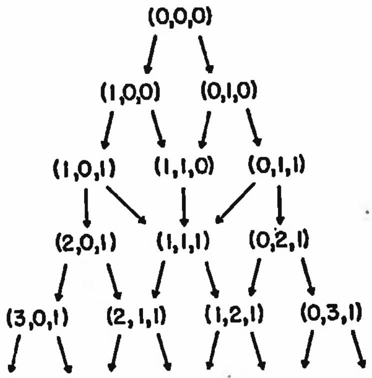

FIG. 4. Partial lattice diagram of C-states.

Another example of a totally sequential binary circuit shows that a circuit may have more than one equivalence set, and yet have no unspanned indices for one of its equivalence sets. This circuit has the equations

$$\begin{aligned} z_1' &= \bar{z}_3, \\ z_2' &= \bar{z}_1(z_2 \vee z_3), \\ z_3' &= \bar{z}_2(z_1 \vee z_3). \end{aligned} \tag{9.9}$$

Let the initial state u be (0,0,0). The sequence of C-states will then be (0,0,0), (1,0,0), (1,0,1), (2,0,1), (2,1,1), (2,1,2), (3,1,2), (3,2,2), etc. The initial state forms its own equivalence set, while the remaining six states which follow it form another equivalence set having the corresponding cycling vector (2,2,2). Hence, no indices are unspanned.

10. *Distributive Circuits*

In Sec. 5 it was pointed out that in some cases design and synthesis of circuits could be simplified by placing more restrictions upon them. Thus, semimodular circuits are easier to treat than more general speed-independent circuits, and totally sequential circuits exhibit still fewer peculiarities of behavior. Yet, as has been shown, totally sequential circuits are unsatisfactory for those applications in which parallel action is required, so that the less restrictive concept of semimodularity was used in the later analysis.

In this section we shall place a further restriction upon our circuits in order to simplify the problem of synthesis, but this restriction will not be so severe as to eliminate the possibility of parallel action within the circuit. This restriction is that the circuit shall be distributive.

The concept of a distributive circuit is related to that of a distributive lattice in the same way that the concept of a semimodular circuit is related to that of a semimodular lattice. We begin with the weaker restriction, however, that $C[u]$ be modular.

> The semimodular lattice $C[u]$ is said to be modular if for every three C-states a, x, and y in $C[u]$ such that a covers x and y and $\mathrm{x} \neq \mathrm{y}$ we have x and y covering $\mathrm{x} \cap \mathrm{y}$. (10.1)

This restriction combined with its dual (7.6) corresponds to the usual definition of modularity.[5] In the theory of general lattices, modularity is less restrictive than distributivity, but the lattice $C[u]$ has special properties which make these restrictions equivalent. This fact is demonstrated in the next two theorems.

Theorem 51: If p and q are any two C-states in $C[u]$, and $C[u]$ is modular, then $\mathrm{p} \cap \mathrm{q} = \mathrm{p} \wedge \mathrm{q}$.

Proof: Form two covering sequences in $C[u]$, $\mathrm{a}(r,0), \mathrm{a}(r,1), \ldots, \mathrm{a}(r,s)$, and $\mathrm{a}(0,s), \mathrm{a}(1,s), \ldots, \mathrm{a}(r,s)$, where we take $\mathrm{p} = \mathrm{a}(r,0)$, $\mathrm{q} = \mathrm{a}(0,s)$ and $\mathrm{p} \cup \mathrm{q} = a(r,s)$. As we have seen previously, we may construct such sequences because $\mathrm{p}\, \mathscr{F}\, \mathrm{p} \cup \mathrm{q}$ and $\mathrm{q}\, \mathscr{F}\, \mathrm{p} \cup \mathrm{q}$. The integers r and s are finite, and each is greater than or equal to 0.

Define $\mathrm{a}(i,j)$ recursively by the formula

$$\mathrm{a}(i,j) = \mathrm{a}(i, j + 1) \cap \mathrm{a}(i + 1, j)$$

for $0 \leq i < r$ and $0 \leq j < s$, starting with $i = r - 1$, $j = s - 1$ and proceeding to all other indices. Using induction with (10.1), we see that $\mathrm{a}(i,j)$ will be covered by $\mathrm{a}(i, j + 1)$ and by $\mathrm{a}(i + 1, j)$ for $0 \leq i < r$ and $0 \leq j < s$, provided we can show that $\mathrm{a}(i + 1, j) \neq \mathrm{a}(i, j + 1)$. But we may use induction to infer that $\mathrm{a}(i + 1, j) \neq \mathrm{a}(i + 1, j + 1)$ and $\mathrm{a}(i, j + 1) \neq \mathrm{a}(i + 1, j + 1)$, so that $\mathrm{a}(i + 1, j) \neq \mathrm{a}(i, j + 1)$.

It was pointed out in the proof of Theorem 25 that the "covers" relation implies the $\mathscr{R}$ relation, so that we may use Theorem 24 to get $\mathrm{a}(i,j) = \mathrm{a}(i, j + 1) \wedge \mathrm{a}(i + 1, j)$ for

$i = 0, 1, \ldots, r-1$ and $j = 0, 1, \ldots, s-1$. By induction we may replace this with the formula $\mathrm{a}(i,j) = \mathrm{a}(i,s) \wedge \mathrm{a}(r,j)$, since it holds for either $i = r$ or $j = s$, and if we assume it for $\mathrm{a}(i, j+1)$ and $\mathrm{a}(i+1, j)$ we obtain $\mathrm{a}(i,j) = \mathrm{a}(i,s) \wedge \mathrm{a}(r, j+1) \wedge \mathrm{a}(i+1, s) \wedge \mathrm{a}(r,j) = \mathrm{a}(i,s) \wedge \mathrm{a}(r,j)$. In the case $i = j = 0$ this formula becomes $\mathrm{a}(0,0) = \mathrm{a}(0,s) \wedge \mathrm{a}(r,0) = \mathrm{p} \wedge \mathrm{q}$. Thus $\mathrm{p} \wedge \mathrm{q}$ is a C-state, and by Theorem 16 is equal to $\mathrm{p} \cap \mathrm{q}$.

The statement of Theorem 51 is the dual of Theorem 17, and permits us to use the symbols $\wedge$ and $\cap$ interchangeably.

Theorem 52: If $C[u]$ is modular it is distributive.
Proof: We verify that the distributive laws

$$\mathrm{a} \cap (\mathrm{b} \cup \mathrm{c}) = (\mathrm{a} \cap \mathrm{b}) \cup (\mathrm{a} \cap \mathrm{c})$$
$$\mathrm{a} \cup (\mathrm{b} \cap \mathrm{c}) = (\mathrm{a} \cup \mathrm{b}) \cap (\mathrm{a} \cup \mathrm{c})$$

hold for numerical vectors if the operations $\wedge$ and $\vee$ are substituted for $\cap$ and $\cup$.

A complete equivalence between the three conditions has thus been established, since it is a well-known lattice theoretical result that distributivity implies modularity.[6]

A circuit is defined as distributive with respect to an initial state u if $C[u]$ is a distributive lattice. (10.2)

Our discussion of distributive circuits will also require a further property of $C[u]$.

Theorem 53: $C[u]$ satisfies the descending-chain condition.
Proof: The descending-chain condition[7] requires that all descending chains be finite. A descending chain in this case is a sequence of C-states $\mathrm{a}(1), \mathrm{a}(2), \ldots, \mathrm{a}(i), \ldots$ such that $\mathrm{a}(i+1) \mathscr{F} \mathrm{a}(i)$ and $\mathrm{a}(i+1) \neq \mathrm{a}(i)$ for $i = 1, 2, \ldots$. Since we are dealing with vectors whose components are nonnegative integers, and, since these vectors satisfy Theorem 16, we infer Theorem 53 immediately. $C[u]$ need not be distributive for Theorem 53.

A synthesis technique, which will be developed later, depends upon the properties of the join-irreducible elements of $C[u]$.

The notation $J[u]$ will be used to denote the set of join-irreducible elements of $C[u]$. A C-state a is join-irreducible if $\mathrm{a} = \mathrm{x} \cup \mathrm{y}$ implies either $\mathrm{a} = \mathrm{x}$ or $\mathrm{a} = \mathrm{y}$.[8] (10.3)

It has been shown by G. Birkhoff that each element in a distributive lattice satisfying the descending-chain condition has a unique representation as an irredundant join of join-irreducible elements, and that therefore there is a one-to-one correspondence between distributive lattices L satisfying the descending-chain condition and partially ordered sets p

satisfying the descending-chain condition, in which p is isomorphic to the subset of join-irreducible elements of L.[9] From these theorems we may state:

If $C[u]$ is distributive, each C-state may be represented as a unique irredundant join of elements of $J[u]$. (10.4)

An irredundant join is one from which no term may be removed without changing its value.

If $C[u]$ is distributive, the set of numerical vectors of the corresponding $J[u]$ determine the vectors of $C[u]$ uniquely. (10.5)

The importance of these results will appear in the later development of a synthesis technique which begins with the partially ordered set $J[u]$ and makes use of (10.4) and (10.5) to construct the distributive lattice $C[u]$.

The join-irreducible elements of $C[u]$ may be related to the C-signals in the following way.

Theorem 54: In a distributive $C[u]$ the set of nonzero join-irreducible elements is isomorphic with the set of C-signals (α,i) having $\alpha > 0$. Under this isomorphism, if (α,i) and (β,j) correspond to $\mathbf{a}$ and $\mathbf{b}$ respectively in $J[u]$, then $\mathbf{a} \mathscr{F} \mathbf{b}$ if and only if $(\alpha - 1, i) \subseteq (\beta - 1, j)$.

Proof: Let (α,i) be any C-signal. The set of all C-states inducing (α,i) must have at least one minimum C-state, since if $\mathbf{x}$ induces (α,i) there cannot be more than a finite number of C-states preceding $\mathbf{x}$ which induce (α,i). Also, there cannot be more than one minimum C-state, for if $\mathbf{a}$ and $\mathbf{b}$ are two minima then, by Theorem 51, $\mathbf{a} \cap \mathbf{b}$ also induces (α,i), and hence $\mathbf{a} \cap \mathbf{b} = \mathbf{a} = \mathbf{b}$. Thus $\mathbf{a}$ is unique.

The minimum C-state $\mathbf{a}$ which induces (α,i) is join-irreducible, for if $\mathbf{a} = \mathbf{x} \cup \mathbf{y}$ then either $\mathbf{x}$ induces (α,i) or $\mathbf{y}$ induces (α,i) by Theorem 17, so either $\mathbf{a} = \mathbf{x}$ or $\mathbf{a} = \mathbf{y}$. This means that each (α,i) determines a unique join-irreducible C-state $\mathbf{a}$, which is the minimum C-state inducing (α,i).

Now, let $\mathbf{b}$ be any join-irreducible C-state. We construct all C-signals induced by $\mathbf{b}$. They are $(\beta_1,1), (\beta_2,2), \ldots, (\beta_n,n)$, where $\beta_j = \mathrm{b}_j$ for $j = 1, 2, \ldots, n$. Let $\mathbf{c}(1), \mathbf{c}(2), \ldots, \mathbf{c}(n)$ be the join-irreducible C-states corresponding to these C-signals. Then, by construction, $\mathbf{c}(j) \mathscr{F} \mathbf{b}$ for each $j = 1, 2, \ldots, n$, so $\mathbf{b} = \mathbf{c}(1) \cup \mathbf{c}(2) \cup \cdots \cup \mathbf{c}(n)$. But $\mathbf{b}$ is join-irreducible, so that there is at least one $\mathbf{c}(j)$ such that $\mathbf{b} = \mathbf{c}(j)$. This shows that there is at least one C-signal corresponding to any join-irreducible element $\mathbf{b}$. We now wish to show that if $\mathbf{b} \neq 0$ this correspondence is one-to-one.

If $\alpha = 0$ in the C-signal (α,i), then 0 induces (α,i), and is clearly minimal. Thus all C-signals of the form $(0,i)$ have 0 for their corresponding join-irreducible C-state. Now take $\alpha > 0$ in (α,i), and let $\mathbf{a}$ be the corresponding join-irreducible element, as before. Let $0, \mathbf{a}(1), \mathbf{a}(2), \ldots, \mathbf{a}(r), \mathbf{a}$ be a covering sequence in $C[u]$ from 0 to $\mathbf{a}$. This sequence has at least two members because $\mathbf{a} \neq 0$. Since $\mathbf{a}(r)$ is covered by $\mathbf{a}$ it differs from $\mathbf{a}$ in just one component, by 1, according to Theorem 26. Thus $a_j(r) + 1 = a_j$ for just one index j, and $a_k(r) = a_k$ for all other indices k. But j must equal i, for otherwise $a(r)$ would induce (α,i), which is impossible because a is the minimum C-state inducing (α,i). Thus, i is uniquely j and α is uniquely a_i. This means that (α,i) is uniquely determined, and hence the mapping is one-to-one.

To demonstrate the second part of the theorem we require the lemma:

Lemma: If $C[u]$ is distributive and a is the join-irreducible element corresponding to (α,i), then for any x either $a \mathscr{F} x$, or else x is in $(\alpha - 1, i)$.

We begin by noting that if $\alpha > 0$ then $(\alpha - 1, i)$ exists. This may be seen by considering a covering sequence from 0 to a. By Theorem 26, some C-state in this sequence must induce $(\alpha - 1, i)$.

If x is not in $(\alpha - 1, i)$, then $a \cap x$ induces (α,i) by Theorem 51. By construction of a we have $a \mathscr{F} a \cap x$, so $a \mathscr{F} x$. Conversely, if $a \mathscr{F} x$ then $a \cap x = a$ is not in $(\alpha - 1, i)$, so x is not in $(\alpha - 1, i)$.

Let (α,i) and (β,j) correspond to the join-irreducible elements a and b respectively. Assume $a \mathscr{F} b$. If x is any C-state in $(\alpha - 1, i)$, we cannot have $b \mathscr{F} x$, for otherwise $a \mathscr{F} x$, which is impossible by the foregoing lemma. Hence x is in $(\beta - 1, j)$ by the lemma. Since x was arbitrary we have $(\alpha - 1, i) \subseteq (\beta - 1, j)$.

Next assume that $(\alpha - 1, i) \subseteq (\beta - 1, j)$. Since b is not in $(\beta - 1, j)$, it cannot be in $(\alpha - 1, i)$, and hence $a \mathscr{F} b$ by the lemma.

This completes the proof of Theorem 54, which, it should be noted, depends on Theorem 26 and, therefore, upon the assumption that the signals are independent.

Theorem 55: If two distributive lattices of C-states $C[u]$ and $C^*[u^*]$ determine identical partially ordered sets of C-signals, then $C[u]$ and $C^*[u^*]$ are identical.

Proof: Let us assume that $C[u]$ and $C^*[u^*]$ are not identical. By (10.5) we see that their corresponding sets $J[u]$ and $J^*[u^*]$ of join-irreducible elements are not identical. Hence there is at least one join-irreducible element a in $J[u]$ which differs from the corresponding element a^* in $J^*[u^*]$, but both correspond to C-signals having the same designation, say (α,i). Note that a and a^* may not be the zero elements in $J[u]$ and $J^*[u^*]$, since then they would be equal. Since $a_i = \alpha$ and $a_i^* = \alpha$, they must differ in some other component, say $a_j \neq a_j^*$. No loss of generality results from assuming $a_j < a_j^*$. Thus the C-signal (β,j) with $a_j^* = \beta > 0$ exists. Let b be the corresponding join-irreducible element in $J[u]$. Then a is in $(\beta - 1, j)$, so $b \mathscr{F} a$ by the lemma in the proof of Theorem 54; but a^* is not in $(\beta - 1, j)$, and $b^* \mathscr{F} a^*$. However, $J[u]$ and $J^*[u^*]$ are isomorphic by Theorem 54, giving a contradiction.

We shall take the set of C-signals and their ordering relations as the starting point for the synthesis procedure. It will be assumed, therefore, that some verbal description of the behavior of the circuit leads to a specification of this partially ordered set. In effect, we are specifying the signal changes which occur at points within the circuit and causation relations between these changes. Naturally, not every such specification will lead to a realizable circuit, but the theorems which follow will give us restrictions on the functions (2.3). If these restrictions are internally consistent, then any set of functions which satisfies them will represent a distributive (and hence speed-independent) circuit which behaves in the specified way.

There are two reasons for using the set of C-signals rather than the lattice $C[u]$ as our starting point. In the first place, the set of C-signals is not as numerous as the set of C-states, if parallel action takes place in the circuit. In fact, if r parallel changes occur in a binary circuit, we obtain r corresponding C-signals and 2^r C-states. Secondly, the C-signals are not subject to as many restrictions as the C-states, since the C-states must form a distributive (or at least semimodular) lattice while the C-signals merely need to be partially ordered, although in either case we must be able to obtain a consistent set of restrictions on the functions (2.3).

Theorem 56: If **a** induces (α,i) and (γ,j), and **b** is the join-irreducible C-state corresponding to $(\alpha + 1, i)$, then $\mathbf{a}_j < \mathbf{b}_j$ if and only if $(\gamma,j) \subseteq (\alpha,i)$.

Proof: Assume $\mathbf{a}_j < \mathbf{b}_j$. If **x** is any C-state not in (α,i), we have $\mathbf{b} \mathscr{F} \mathbf{x}$ by the lemma in the proof of Theorem 54. Hence $\gamma < \mathbf{b}_j \leq \mathbf{x}_j$, and **x** is not in (γ,j).

Next assume $(\gamma,j) \subseteq (\alpha,i)$. Since **b** is not in (α,i) it is not in (γ,j), and we have $\mathbf{a}_j = \gamma < \mathbf{b}_j$.

Theorem 57: If n is greater than 1 and **a** induces (α,i), then $\mathbf{a}_i = \mathbf{a}_i'$ if and only if there is a C-signal (γ,j) induced by **a** such that $(\gamma,j) \subseteq (\alpha,i)$ and $j \neq i$.

Proof: Assume that such a C-signal (γ,j) exists and yet that $\mathbf{a}_i \neq \mathbf{a}_i'$. Then by Theorem 27 we may construct a C-state **b** with $\mathbf{b}_i = \mathbf{a}_i + 1$ and $\mathbf{b}_j = \mathbf{a}_j$. Thus **b** is in (γ,j) and not in (α,i), and we cannot have $(\gamma,j) \subseteq (\alpha,i)$. Therefore $\mathbf{a}_i = \mathbf{a}_i'$.

Assume next that $\mathbf{a}_i = \mathbf{a}_i'$. If no C-signal (β,i) exists with $\beta > \alpha$, we see that $(\alpha,i) = C[u]$ and hence $(\gamma,j) \subseteq (\alpha,i)$ for every (γ,j). If (β,i) does exist and is induced by some C-state **c**, we may form a covering sequence from **a** to $\mathbf{a} \cup \mathbf{c}$ and by Theorem 26 obtain a C-state inducing $(\alpha + 1, i)$. Let **d** be the join-irreducible element corresponding to $(\alpha + 1, i)$. Assume that $\mathbf{a}_j \geq \mathbf{d}_j$ for all $j \neq i$. Then if we form $\mathbf{e} = \mathbf{a} \cup \mathbf{d}$ we see that $\mathbf{e}_j = \mathbf{a}_j$ for all $j \neq i$, and $\mathbf{e}_i = \mathbf{a}_i + 1$. Hence **e** covers **a**, so $\mathbf{a} \mathscr{R} \mathbf{e}$ and $\mathbf{e}_i \leq \mathbf{a}_i'$. This would mean $\mathbf{a}_i \neq \mathbf{a}_i'$, and hence we infer $\mathbf{a}_j < \mathbf{d}_j$ for some $j \neq i$. Therefore $(\gamma,j) \subseteq (\alpha,i)$ by Theorem 56, for some (γ,j) induced by **a**.

Theorem 58: Any vector **a** which, when regarded as a C-state, induces only existing C-signals, and does not violate any inclusion relations among the C-signals, does represent a member of $C[u]$.

Proof: Since **a**, regarded as a C-state, induces only existing C-signals we may attempt to write it as a join of the join-irreducible elements corresponding to these C-signals. Let this join be $\mathbf{a}^* = \mathbf{b}(1) \cup \mathbf{b}(2) \cup \cdots \cup \mathbf{b}(n)$. Let us assume $\mathbf{a}^* \neq \mathbf{a}$ so that $\mathbf{a}_i^* \neq \mathbf{a}_i$ for at least one i. Then there must be some $\mathbf{b}(j)$ such that $\mathbf{b}_i(j) > \mathbf{b}_i(i)$. Let $\mathbf{b}(i)$ induce (α,i) and $\mathbf{b}(j)$ induce (β,j). By the argument of the previous proof we have $(\alpha,i) \subseteq (\beta - 1, j)$. But this inclusion relation is violated by the assumption that $\mathbf{a}$ is in (α,i) but not in $(\beta - 1, j)$. Hence $\mathbf{a}^* = \mathbf{a}$ and $\mathbf{a}$ is in $C[u]$.

Theorems 57 and 58 may be used to obtain a synthesis method for binary circuits. A detailed presentation of this technique will appear in a future publication dealing with synthesis.

In a binary circuit the terminal state a of any C-state $\mathbf{a}$ is obtainable by summing u and $\mathbf{a}$, and taking the residues of the components modulo 2. Also, in the binary case, we see that $a_i \neq a_i'$ implies a_i' equals the complement of a_i. Thus we are able to determine explicitly whether $a_i' = a_i$ or $a_i' = \bar{a}_i$ from Theorem 57 with a knowledge of the ordering relations among the C-signals, provided we know what the other signals may be. But the other signals are subject only to the limitations described in Theorem 58. Thus, for each signal a_i we obtain a set of restrictions on the function f_i. If all these restrictions are applied to all f_i, we obtain a set of conditions which, if consistent, are necessary and sufficient to cause the circuit to behave in a way described by the lattice $C[u]$.

REFERENCES

1. D. A. Huffman, "The synthesis of sequential switching circuits," *J. Franklin Inst.* **257**, Nos. 3 and 4 (1954).

2. G. H. Mealy, "A method for synthesizing sequential circuits," *Bell System Tech. J.* (September 1955), 1045–1079.

3. G. Birkhoff, *Lattice theory*, American Mathematical Society Colloquium Publication, vol. 25 (1948), p. 100.

4. *Ibid.*, p. 5.

5. *Ibid.*, p. 66.

6. *Ibid.*, p. 134.

7. *Ibid.*, p. 37.

8. *Ibid.*, p. 20.

9. *Ibid.*, p. 142.