INFORMATION AND CONTROL 9, 521–530 (1966)

Testing and Generating Infinite Sequences by a Finite Automaton*

ROBERT MCNAUGHTON

Massachusetts Institute of Technology, Cambridge, Massachusetts

Büchi (1962) has given a decision procedure for a system of logic known as "the Sequential Calculus," by showing that each well formed formula of the system is equivalent to a formula that, roughly speaking, says something about the infinite input history of a finite automaton. In so doing he managed to answer an open question that was of concern to pure logicians, some of whom had no interest in the theory of automata.

Muller (1963) came upon quite similar concepts in studying a problem in asynchronous switching theory. The problem was to describe the behavior of an asynchronous circuit that does not reach any stability condition when starting from a certain state and subject to a certain input condition. Many different things can happen, since there is no control over how fast various parts of the circuit react with respect to each other. Since at no time during the presence of that input condition will the circuit reach a terminal condition, it will be possible to describe the total set of possibilities in an ideal fashion only if an infinite amount of time is assumed for that input condition.

Neither Büchi's Sequential Calculus nor Muller's problem of asynchronous circuitry will be described further here. It is interesting that two such apparently divergent areas of inquiry should give rise to the same problem, namely, that of describing the infinite history of finite automata. It is this problem to which the remainder of this paper will address itself.

It will be recalled that a well known basic theorem in the theory of

* This paper was sponsored in part by the Advanced Research Projects Agency, Department of Defense, through Office of Naval Research Contract Nonr-4102(01). It is closely related to a talk given by the author at the Harvard Colloquium on Computation and Control in October, 1964.

finite automata is that often referred to as the "Kleene-Myhill theorem" (because it was proved first by Kleene (1956) and re-exposited by Myhill (1957)). The theorem states that the class of regular events equals the class of finite-state events. An event is a set of words, and a word is simply a finite sequence of symbols from some input alphabet. A regular event is defined as one given by a regular expression, and a finite-state event is defined as one given by a state graph. (It will be assumed that the reader has some experience with regular expressions and state graphs.)

These two characterizations of the class of events processed by finite automata differ considerably. The first is in terms of a mechanism for generating the words in the event, while the second is in terms of a mechanism for testing a word for membership in the event. In each case the class of mechanisms are the finite-state mechanisms. Since the Kleene-Myhill theorem implies that events generated by finite-state mechanisms are the same as those tested by finite-state mechanisms, it is an important cornerstone of the theory of finite automata.

The bulk of the present paper is a proof of an analogue to the Kleene-Myhill theorem for ω-events. An ω-event is a set of infinite sequences from some finite input alphabet; in other words a set of sequences of ordinality ω. Regular expressions can be extended to describe ω-events by introducing a new operator: thus, where α is a nonempty event (set of finite words) not containing the null word, α^ω is a set of infinite sequences formed by concatenating infinitely many members of α; alternatively expressed, it is the result of an ω-concatenation of words from α. Thus $(0 \cup 1)^\omega$ is the set of all infinite sequences (ordinality ω) of 0's and 1's. If α is an event, and β is an ω-event then $\alpha\beta$ is an ω-event. But, since we regard sequences as going from left to right, $\beta\alpha$ will in general have sequences of ordinality greater than ω, which are not considered here. Thus 0^*1^ω is the set of all sequences having infinitely many 1's and no occurrence of a 0 following a 1. Similarly, the union of two ω-events is an ω-event.

An ω-event E is *regular* if there exist regular events $\alpha_1, \cdots, \alpha_n$, $\beta_1, \cdots, \beta_n$ such that $E = \alpha_1\beta_1^\omega \cup \cdots \cup \alpha_n\beta_n^\omega$. (Throughout this paper the word "event" when not preceded by "ω-" means a set of finite words.) It is clear here that since E is an ω-event no β_i can contain the null word.

On the other hand, an ω-event is *finite-state* if there is a finite automaton (as given, for example, by a state graph) and a subclass

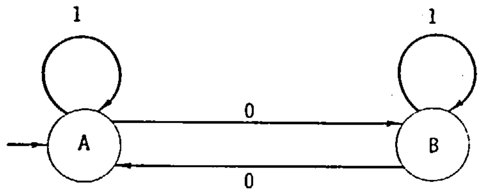

FIG. 1

$\{\pi_1, \cdots, \pi_m\}$ of the class of all nonempty subsets of states of the automaton such that, for any infinite sequence S whose terms are from Σ, S is in E if and only if the precise set of states that the automaton assumes infinitely often when given S as an input sequence (starting from the initial state) is one of the sets $\pi_1, \cdots, \pi_m$. This concept can be thought of as a definition in terms of the testing of an infinite sequence. The sense of the word "test" is rather peculiar here since the machine that is given an infinite sequence never stops.

As an example, consider the state graph of Fig. 1. (The state graphs of this paper will have a single short unlabeled arrow pointing to the initial state.) The event given by the class of subsets $\{\{A\}, \{B\}\}$ is the ω-event of all infinite sequences having only finitely many 0's. It could be given as a regular expression $(0 \cup 1)^*1^\omega$.

As another example, consider Fig. 2 and the ω-event given by the class $\{\{A\}, \{A, B, C\}\}$. To analyze this ω-event note that $\alpha = (11 \cup 0)^*100^*1$ is the set of all words which trace out a path in the graph starting from A hitting both B and C and then terminating the first time that it hits A after hitting both B and C. The ω-event given by the class $\{\{A\}\}$ is $\alpha^*(0 \cup 11)^*0^\omega$. The ω-event given by $\{\{A, B, C\}\}$ is α^ω. The given ω-event, therefore, is $\alpha^*(0 \cup 11)^*0^\omega \cup \alpha^\omega$.

The concept of regular ω-event is found in both (Büchi, 1962) and (Muller, 1963). However, both the concept of finite-state ω-event (or "machine regular" as Muller (1963) calls it) and the statement of the theorem equating the two concepts are Muller's contributions. Muller's proof of this theorem proceeds along different lines from the proof given in this paper; the version of his proof in (Muller, 1963) is not valid. The sequences in a regular ω-event can be generated by a graph; a precise description of one manner of this use of graphs as generators (the so-called "nondeterministic graphs") for infinite sequences is given in (Muller, 1963). Such graphs, however, will play no rôle in the present paper.

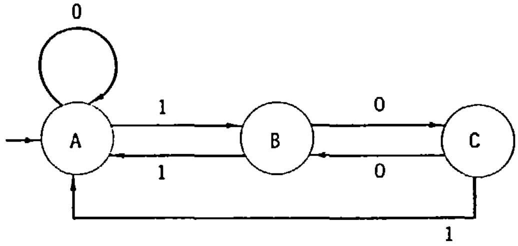

FIG. 2

THEOREM. *An ω-event is regular if and only if it is finite-state. (Also, given the event characterized in one way, the other kind of characterization is effectively determined.)*

The proof of this theorem occupies almost all of the remainder of this paper. Assume first that E is a finite-state ω-event. Then E is given by a class $\{\pi_1, \cdots, \pi_m\}$ where each π_i is a set of states of a state graph G. Since a finite union of regular ω-events is obviously regular it suffices to show that the ω-event E_i, which is the set of all infinite sequences S such that the set of states hit infinitely often by S in its path through G is just one of the sets π_i, is a regular ω-event.

Let $\pi_i = \{s_1, \cdots, s_k\}$. Let α be the set of all words tracing paths from the initial state to s_1. For $1 \leqq j \leqq k$, let β_j be the set of all words taking the automaton from s_j to s_{j+1} (or to s_1 if $j = k$) without hitting any of the states outside of π_i. The sets $\alpha, \beta_1, \cdots, \beta_k$ are all regular, as the reader familiar with the theory of regular events will verify. Now $E_i = \alpha(\beta_1\beta_2 \cdots \beta_k)^\omega$, which is proved as follows.

If $S \in E_i$, consider the path through G traced by S. Let t be the time after which no state other than those of π_i is assumed. Let $\{t_1, t_2, t_3, \cdots\}$ be an infinite set of the integers all greater than t and such that $t_j > t_h$ for $j > h$, where, for each x and y, $1 \leqq y \leqq k$, t_{kx+y} is a time when the device assumes state s_y. That such a set of times exists follows from the fact that the device assumes all states of π_i infinitely often. S parsed at $t_1, t_2, t_3, \cdots$ shows it to be in $\alpha(\beta_1\beta_2 \cdots \beta_k)^\omega$.

On the other hand, assume $S \in \alpha(\beta_1\beta_2 \cdots \beta_k)^\omega$. Let $S = S'X$, where $S' \in \alpha$ and $X \in (\beta_1\beta_2 \cdots \beta_k)^\omega$. S' takes the device to s_1, and from there on (by definition of the β's) the path traced by S never assumes a state outside of π_i. But all the states of π_i are assumed infinitely often, and so $S \in E_i$.

Thus all finite-state ω-events are regular. The more difficult converse is proved after several definitions and lemmas, by a construction.

Note first that the union of finitely many finite-state ω-events is a finite-state ω-event. It is easier to show this for the union of two, from which the proposition for the union of any finite number follows easily. Let E_1 and E_2 be such ω-events. Then E_1 is given by the state graph G_1 and a class $\{\pi_1^1, \cdots, \pi_{m_1}^1\}$, and E_2 by G_2 and $\{\pi_1^2, \cdots, \pi_{m_2}^2\}$. Take the Cartesian product of the two state graphs $G_1 \times G_2$, the initial state being $s_{01} \times s_{02}$ where s_{01} and s_{02} are the initial states of G_1 and G_2, respectively. For any set β of states of this graph, let $P_1(\beta) = \{s_1 : (\exists s_2) s_1 \times s_2 \in \beta\}$ and $P_2(\beta) = \{s_2 : (\exists s_1) s_1 \times s_2 \in \beta\}$. Note that $\{\beta: (\exists i)(1 \leqq i \leqq m_1 \,\&\, P_1(\beta) = \pi_i^1)\}$ is a class of sets for E_1. That is, if a sequence S is applied to the constructed state graph, then $S \in E_1$ if and only if $P_1(\beta) = \pi_i^1$ for some i, where β is the precise set of states hit infinitely by the path spelling out S. Similarly, $\{\beta: (\exists i)(1 \leqq i \leqq m_2 \,\&\, P_2(\beta) = \pi_i^2)\}$ is a class of sets for E_2. The union of these two classes or $\{\beta: (\exists i)[(1 \leqq i \leqq m_1 \,\&\, P_1(\beta) = \pi_i^1) \vee (1 \leqq i \leqq m_2 \,\&\, P_2(\beta) = \pi_i^2)]\}$ is a class of states for $E_1 \cup E_2$, showing that $E_1 \cup E_2$ is a finite state ω-event.

Thus we may henceforth assume that $E = \alpha\beta^\omega$ where α and β are regular sets of finite words. Let S be an arbitrary infinite sequence from the input alphabet Σ. Let S_t be the initial segment of S ending at time t, and $S_{t_1t_2}$ the segment from $t_1 + 1$ to t_2 inclusive. t_2 *favors* t_1 if $t_2 > t_1$, $S_{t_1t_2} \in \beta^*$, and $S_{t_1} \in \alpha\beta^*$. (This and the following concepts are relative to S.) $E(t_1, t_2, t_3)$, or t_1 is *equivalent* to t_2 as judged at time t_3, if $t_3 \geqq t_1$, $t_3 \geqq t_2$, $S_{t_1} \in \alpha\beta^*$, $S_{t_2} \in \alpha\beta^*$ and, for every word X on the input alphabet Σ, $S_{t_1t_3}X \in \beta^*$ if and only if $S_{t_2t_3}X \in \beta^*$. An easily proved law is that if $E(t_1, t_2, t_3)$ and $t_4 > t_3$ then $E(t_1, t_2, t_4)$. In other words, if t_1 and t_2 are ever judged to be equivalent then they will forever thereafter be judged to be equivalent. Moreover, if $E(t_1, t_2, t_3)$ and $t_4 \geqq t_3$ then t_4 favors t_2 if and only if t_4 favors t_1. The following definition is natural.

$E(t_1, t_2)$, or t_1 and t_2 are *equivalent*, if and only if there exists a t such that $E(t_1, t_2, t)$. Let p be the number of states in a reduced state graph for β^*.

LEMMA 1. *The number of equivalence classes given by $E(t_1, t_2, t)$ among the times $t_1, t_2 \leqq t$ such that S_{t_1} and $S_{t_2} \in \alpha\beta^*$ is no more than p; also the number of equivalence classes given by $E(t_1, t_2)$ is no more than p.*

Proof: If $S_{t_1}, S_{t_2} \in \alpha\beta^*$ then t_1 and t_2 will be in the same equivalence class if S_{t_1t} and S_{t_2t} both trace out paths from the initial state to the same state in the reduced state graph for β^*, thus proving the first assertion. To prove the second assertion, suppose there are $p + 1$ or more equivalence classes. There would then be times $t_1, t_2, \cdots, t_{p+1}$, no two of which are equivalent. For $t > \max(t_1, \cdots, t_{p+1})$ we would have, for each i and j, not $E(t_i, t_j, t)$. Thus there would be $p + 1$ equivalence classes, as judged at time t, contradicting the first assertion already proved.

LEMMA 2. *$S \in \alpha\beta^\omega$ if and only if there exists a τ such that there are infinitely many t equivalent to τ and favoring τ.*

Proof: Suppose first that $S \in \alpha\beta^\omega$. Then there exists a sequence $t_0, t_1, t_2, \cdots$ ($t_i > t_j$, for $i > j$) such that $S_{t_0} \in \alpha$ and for every $i \geqq 0$, $S_{t_i t_{i+1}} \in \beta$. For $i > j$, $S_{t_j t_i} \in \beta^*$ and so t_i favors t_j. But there are only finitely many equivalence classes among the t's by $E(t_i, t_j)$, and so there must be an infinite set of t's in at least one of these classes. Taking τ as the smallest member of this class, Q.E.D., one way.

Now suppose that there are infinitely many t's equivalent to τ and favoring it. $S_\tau \in \alpha\beta^*$. Put $t_0 = \tau$. Take $t_1 > t_0$ so that $E(t_1, t_0)$ and t_1 favors t_0. Then, for some $t_1' \geqq t_1$, $E(t_0, t_1, t_1')$. Take $t_2 > t_1'$ so that $E(t_2, t_0)$ and t_2 favors t_0. But then $S_{t_0 t_2} \in \beta^*$ and since $t_2 > t_1'$ we have, by definition of $E(t_0, t_1, t_1')$, $S_{t_1 t_2} \in \beta^*$. (Note that $S_{t_1 t_2} \in \beta^*$ would not follow from any weaker hypothesis about t_0, t_1, and t_2. Thus the need for both the concept of "favors" and the concept of "equivalence" in the proof.) In this manner the infinite sequence $t_0 = \tau, t_1, t_2, \cdots$ is constructed so that each t_i is equivalent to t_0 and favors it; but t_i is chosen as a time when t_0 is judged to be equivalent to t_{i-1}, so that $S_{t_{i-1} t_i}$ will be in β^*. From an obvious relationship between the star operator and the omega operator, $S \in \alpha\beta^\omega$, concluding the proof of Lemma 2.

The machine is now constructed to determine whether $S \in \alpha\beta^\omega$, in the light of Lemma 2, by determining whether there exists a τ such that there are infinitely many t equivalent to τ and favoring it. The machine will be such as to make it clear that it performs the appropriate function, although it will be only informally described. It will have a set of sets of states $\{\pi_1, \cdots, \pi_m\}$ such that, for any S, the set of states that the device assumes infinitely often is one of the π_i if and only if there exists such a τ.

The machine consists of $p + 2$ sequential machines, p being the number of states in the reduced state graph for β^*, with data links to a master control which has some additional memory. The first sequential machine (the $\alpha\beta^*$ machine) receives the inputs as they come and reports to the master control at any time t whether or not $S_t \in \alpha\beta^*$. The remaining $p + 1$ sequential machines (the β^* machines) are modeled after the reduced state graph for β^*. Each β^* machine at any time may be dormant, in which case it is oblivious to the input sequence coming in and simply remains in the initial state until activated by the master control. When a β^* machine is activated at time t it then becomes receptive to the input sequence and reports to the master control, at each time $t' > t$, precisely which of the p states it is in; this it does until it is made dormant by the master control, at which point it goes to and remains in the initial state until it is again activated.

There are two possibilities: either α contains the null word or not. If so, then just before the initial moment of time, i.e., the time of the first input, one of the β^* machines will start at its initial state by being active (i.e., receptive to the first input) and all the remaining β^* machines will be dormant. If α does not contain the null word then all the β^* machines are dormant just before the initial moment of time.

The master control keeps track of which of the β^* machines are active and also the order in which they last became active. At any time t, if $S_t \in \alpha\beta^*$ and none of the active β^* machines are in the initial state then one of the dormant machines is activated and made receptive to the input at time $t + 1$. (For the moment, note that if $S_t \in \alpha\beta^*$ and one of the active β^* machines M is in the initial state then $E(t, t', t)$, where t' is the time that M was activated.)

Suppose $t_1 < t_2$, M_1 and M_2 are β^* machines which were activated at times t_1 and t_2 respectively; the master control keeps track (for all such pairs M_1 and M_2) whether or not t_2 favors t_1 as a relationship between M_1 and M_2. (Since the master control has only finite memory it cannot keep track of the values of t_1 and t_2, which, fortunately, are not needed.) Now for any $t > t_2$, $E(t_1, t_2, t)$ if and only if M_1 and M_2 are in the same state at time t. If M_1 and M_2 go into the same state then M_2 goes dormant, justified by the fact that any $t' > t$ favoring t_2 will also favor t_1.

Note that there will never be more than p active β^* machines, since there are only p states in any such machine. Thus there is always at least one dormant β^* machine ready to become active. (As a matter of fact, there is no reason why a machine could not become dormant and be reactivated at the same time. Thus only p β^* machines are needed.)

The master control has one green light and one red light as outputs associated with each of the $p+1$ β^* machines. Whenever a machine goes from the active state to the dormant state, its red light flashes. Let

M_1 be any of the β^* machines. M_1's green light flashes at time t if and only if M_1 is active at time t having become active at time t_1 and either (1) t favors t_1 and M_1 is in the initial state at time t, and thus $E(t_1, t, t)$, or (2) for some M_2 activated at t_2, where $t_1 < t_2 < t$, t_2 favors t_1, and t is the earliest time at which $E(t_1, t_2, t)$.

LEMMA 3. *If there is a time equivalent to infinitely many times that favor it and τ is the earliest such time, then there is a β^* machine M that is activated at τ, remains activated forever, and flashes its green light infinitely many times. (After τ its red light never flashes; thus its red light flashes only finitely many times.)*

Proof: If some machine M' has been active before τ and goes into the initial state at time τ, then let τ' be the time when M' was activated. $\tau' < \tau$ and any t equivalent to τ and favoring it would also be equivalent to and would favor τ', contradicting the hypothesis that τ is the earliest time equivalent to infinitely many times that favor it. Thus no M' that is active is in the initial state at τ, and thus some M is activated at time τ. Again, if for some M' that was activated at $\tau' < \tau$, $E(\tau, \tau', t)$ where $t > \tau$ then the same contradiction could be inferred. Thus M never goes into the dormant state after time τ. Since infinitely many t's are equivalent to and favor τ, M's green light will flash infinitely many times, by construction.

LEMMA 4. *Conversely, if there is a β^* machine M whose green light flashes infinitely often and whose red light only finitely often then there are infinitely many times equivalent to and favoring the last time τ at which M becomes active.*

Proof: After τ, M would remain active forever. Since its green light flashes infinitely many times, there are infinitely many times that are equivalent to τ and favor it.

It should be obvious to the experienced reader that the entire system so constructed is a finite-state machine although the number of states for medium-sized values of p is large. Lemmas 2, 3, and 4 show that $S \in \alpha\beta^\omega$ if and only if, for some M, M's green light flashes infinitely often and M's red light flashes finitely often. For each M_i, let μ_i be the set of all states in which M_i's green light flashes and M_i's red light does not flash. Let ν_i be the set of all states in which M_i's red light does not flash. Let $\{\pi_{i1}, \cdots, \pi_{iq_i}\}$ be the set of all sets π such that $\mu_i \subseteqq \pi \subseteqq \nu_i$. If M_i's green light flashes infinitely often and M_i's red light flashes only finitely often then the precise set of states assumed by the system infinitely often is one of $\pi_{i1}, \cdots, \pi_{iq_i}$. The set of sets of states $\{\pi_{11}, \cdots,$

$\pi_{1q_1}, \cdots, \pi_{(p+1)1}, \cdots, \pi_{(p+1)q_{p+1}}\}$ is therefore precisely the set of sets of states to establish that $\alpha\beta^\omega$ is a finite-state ω-event according to the definition.

This concludes the proof of the theorem. Let us consider two examples. A machine for the ω-event $(0 \cup 1 \cup 2)^*(0^*1)^\omega$ has one green light and one red light. The green light flashes at every occurrence of a 1. The red light flashes at every occurrence of a 2. It is easy to see that a sequence is in the given ω-event if and only if the green light of this machine flashes infinitely often and the red light finitely often. This machine is actually a simplification of the one that would result from the construction given above. The example shows that in general both red and green lights are necessary to represent ω-events.

For the second example, let Σ_i be $(0 \cup 1 \cup \cdots \cup i)$, and consider the regular ω-event $E = \Sigma_4{}^*[\Sigma_1{}^*0\Sigma_1{}^*1 \cup \Sigma_3{}^*0\Sigma_3{}^*1\Sigma_3{}^*2\Sigma_3{}^*3]^\omega$. A machine with two sets of lights suffices for this ω-event. The first red light flashes at any occurrence of a 2, 3, or 4, and the first green light flashes at a completion of a word in $\Sigma_1{}^*0\Sigma_1{}^*1$ since the last time the first green light or the first red light flashed whichever was later. The second red light flashes at any occurrence of a 4, and the second green light flashes at the completion of a word in $\Sigma_3{}^*0\Sigma_3{}^*1\Sigma_3{}^*2\Sigma_3{}^*3$ since the last flash of either the second green light or the second red light. It is not difficult to see that a sequence is in E if and only if either (1) the first red light of this machine flashes finitely often and the first green light infinitely often, or (2) the second red light flashes finitely often and the second green light infinitely often. No machine for this ω-event has just one green and one red light, but a proof of this fact is left for the reader. This example shows it is not the case that all ω-events of the form $\alpha\beta^\omega$ can be represented by machines with one set of lights, which would have been a natural conjecture to make.

A final comment is directed to those interested in Büchi's paper (1962). By far the most difficult part of Büchi's proof is the proof of Lemma 9 which states that the negation of every formula in the class $\Sigma_1{}^\omega$ has an equivalent formula in $\Sigma_1{}^\omega$. (From this it is relatively simple to show that every formula of the Sequential Calculus is equivalent to some formula of $\Sigma_1{}^\omega$, from which the decidability of the system follows.) The theorem proved in this paper gives an alternative proof to Büchi's Lemma 9. For the regular ω-events are exactly the events describable by formulas of $\Sigma_1{}^\omega$ (Lemma 10 of (Büchi, 1962)). Finite-state ω-events are closed under complementation, which is clear from the definition. From the last two sentences and the main theorem of this paper it follows that the events describable by formulas of Σ_1^ω are closed under complementation, and thus Lemma 9 is proved.

RECEIVED: September 14, 1965

REFERENCES

BÜCHI, J. R., (1962), On a decision method in restricted second order arithmetic. *Logic, Methodology, and Philosophy of Science: Proc. 1960 Intern. Congr.*, pp. 1–11 (Stanford Univ. Press, 1962).

MULLER, D. E., (1963), Infinite sequences and finite machines. *Switching Circuit Theory and Logical Design: Proc. Fourth Ann. Symp.* pp. 3–16 (Inst. of Electrical and Electronic Engineers, New York).

KLEENE, S. C., (1956), Representation of events in nerve nets and finite automata. *In* "Automata Studies," C. E. Shannon and J. McCarthy, eds., pp. 3–42. Princeton Univ. Press, Princeton, New Jersey.

MYHILL, J., NERODE, A. AND TENNENBAUM, S., (1957), "Fundamental Concepts in the Theory of Systems," Tech. Report No. 57-624 (Wright Air Development Center, Cincinnati).