References

[1] G. C. Bacon, "The decomposition of stochastic automata," *Inform. Contr.*, vol. 7, 1964, pp. 320–339.
[2] S. Fujimoto and T. Fukao, "The decomposition of probabilistic automata," *Bull. Electrotech. Lab.* (Tokyo), vol. 30, 1966, pp. 688–698.
[3] A. Paz, "Some aspects of probabilistic automata," *Inform. Contr.*, vol. 9, 1966, pp. 26–60.

On the Bounds for State-Set Size in the Proofs of Equivalence Between Deterministic, Nondeterministic, and Two-Way Finite Automata

FRANK R. MOORE, MEMBER, IEEE

Abstract—The bounds on state-set size in the proofs of the equivalence between nondeterministic and deterministic finite automata and between two-way and one-way deterministic finite automata are considered. It is shown that the number of states in the subset machine in the first construction cannot be reduced for certain cases. It is also shown that the number of states in the one-way automation constructed in the second proof may be reduced only slightly.

Index Terms—Automata theory, equivalence proofs, finite automata, nondeterministic automata, two-way automata, upperbound.

Introduction

In this note we consider the deterministic finite automaton (DFA) as presented by Moore [1]. This idea was generalized by Rabin and Scott to allow nondeterministic operation and two-way motion [2]. Rabin and Scott proved that the nondeterministic finite automaton (NFA) accepts the same class of tapes as the DFA. In addition, Shepherdson showed that two-way deterministic finite automata (2DFA) accept the same class of tapes as the DFA [3]. Hopcroft and Ullman give a slightly different and more explicit proof [4].

In both of these proofs an upper bound on the number of states in the constructed DFA is given. This means that the constructed machine will be finite. However, it has been speculated that at least one of these bounds is not precise. In commenting on the NFA to DFA construction, Rabin states in [5], "It is not known whether the bound of 2^n on the number of states . . . may be considerably improved." It will be shown that the NFA bound cannot be improved, in general, and the 2DFA bound has room for only slight improvement.

The Subset Construction Bound

In the subset construction of Rabin and Scott [2], we see that the constructed DFA, D(A) has 2^n states, the subsets of S, which is the state set of A. However, if we reduce equivalent states in D(A) and only take those states in D(A) which are connected to the initial state, it is clear that an equivalent DFA which may have less than 2^n states can be constructed. We now show that this upper bound may be reached by displaying an NFA, B_n for each n, which, when the subset construction is applied, is connected, reduced and has 2^n states. This machine's state table is given in Fig. 1. Thus

B_n	a	b
→1	2	1
2	3	3
3	4	4
4	5	5
⋮		
n-1	n	n
(n)	1, 2	∅

Fig. 1. The nondeterministic automaton B_n. (The initial state is shown by an arrow and the final state is circled.)

$$B_n = \langle \{1, 2, \cdots, n\}, M, \{1\}, \{n\} \rangle$$

where $S=\{1, 2, \cdots, n\}$ is the state set with $S_0=\{1\}$ the initial and $F=\{n\}$ the final subsets and where

$$\begin{aligned} M(i, a) &= \{i+1\}, \qquad i = 1, 2, \cdots, n-1 \\ M(n, a) &= \{1, 2\} \\ M(1, b) &= \{1\} \\ M(i, b) &= \{i+1\}, \qquad i = 2, 3, \cdots, n-1 \\ M(n, b) &= \varnothing. \end{aligned}$$

It will be shown by two lemmas that $D(B_n)$ is reduced and connected. We first need a definition. In a DFA, two states q and p are *equivalent* ($q \equiv p$), if for all $x \in \Sigma^*$, $M(q, x) \in F$ if and only if $M(p, x) \in F$, where F is the final subset.

Lemma 1: In $D(B_n)$, $Q \equiv P$ if and only if $Q=P$, for Q, $P \in 2^S$.

Proof: Since $S=\{1, 2, \cdots, n\}$, we write

$$\begin{aligned} Q &= \{i_1, i_2, \cdots, i_k\} \\ P &= \{j_1, j_2, \cdots, j_l\}. \end{aligned}$$

Obviously $Q \equiv P$ if $Q=P$. Assume $Q \neq P$. Then $Q \not\equiv P$ if there is a tape $x \in \{a, b\}^*$ such that $n \in M(Q, x)$ but $n \notin M(P, x)$ or vice versa.

Then choose i_r to be an integer such that $i_r \notin P \cap Q$ but $i_r \in P$ or $i_r \in Q$. Assume $i_r \in Q$. If $i_r \geq 2$, $n \in M(Q, a^{n-i_r})$, but $n \notin M(P, a^{n-i_r})$. If $i_r = 1$, then $n \in M(Q, b^n a^{n-1})$ but $n \notin M(P, b^n a^{n-1})$. In any case $Q \not\equiv P$.

As an example, let $n=5$ and $Q=\{1, 2\}$, $P=\{2\}$. Then we would choose $i_r=1$, and $M(Q, b^5a^4)=\{5\}$ and $M(P, b^5a^4) = \varnothing$.

Lemma 2: For every $Q \in 2^S$ in $D(B_n)$ there is a tape $x \in \Sigma^*$ such that $M(S_0, x)=Q$. Thus, $D(B_n)$ is connected.

Proof: Let $Q=\{i_1, i_2, \cdots, i_k\}$, $1 \leq i_1 < i_2 < \cdots < i_k \leq n$. We will now show how to connect Q to a subset P such that P has one less state. Then, since all the singleton states

Manuscript received September 5, 1970; revised January 9, 1971.
The author is with the Systems Development Division, IBM Corporation, Poughkeepsie, N. Y. 12602.

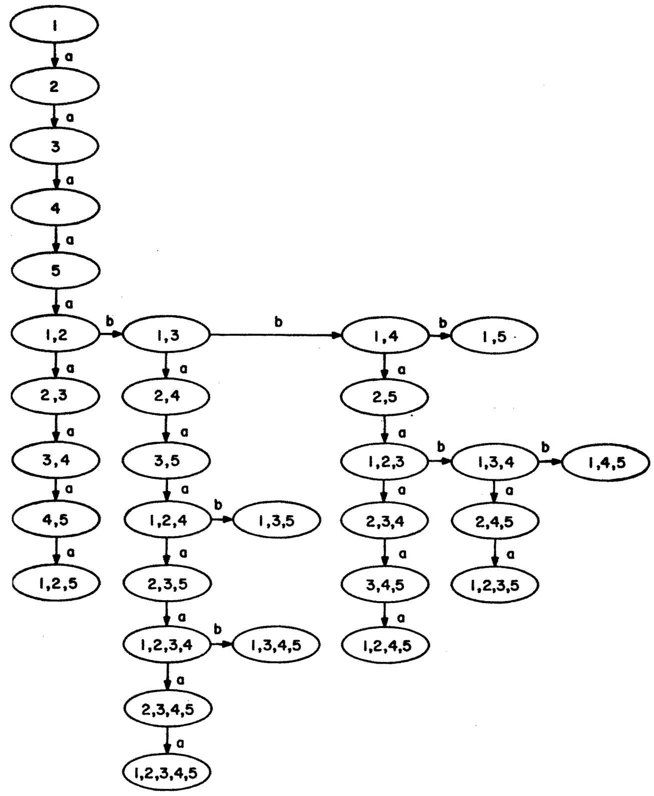

Fig. 2. Part of the state table for $D(B_5)$.

are connected to state 1 by $M(1, a^{i-1}) = \{i\}$, we will have proved the lemma by induction. If $i_2 - i_1 = 1$, then let $P = \{i_3', i_4', \cdots, i_k', n\}$, where $i_r' = i_r - i_1$ and $M(P, a^{i_1}) = Q$. If $i_2 - i_1 \neq 1$, let $P = \{i_3'', i_4'', \cdots, i_k'', n\}$, where $i_r'' = i_r - i_2 + 1$ and $M(P, ab^{i_2-(i_1+1)}a^{i_1-1}) = Q$. In either case P has one less state and the lemma is proved.

To illustrate this the relevant parts of the state table for $D(B_5)$ are shown in (Fig. 2). Thus we have the following theorem.

Theorem 1: There is a two-input n-state NFA for each n, for which the reduced and connected DFA obtained from the subset construction has 2^n states.

Now, we get the immediate corollary if we note that if two subsets are not equivalent over a two-letter alphabet, then increasing the size of the alphabet cannot make them equivalent.

Corollary 1: For each $k \geq 2$ there is a k-input n-state NFA for which the corresponding reduced DFA has 2^n states.

It is interesting to note that there are only two nondeterministic transitions in B_n, both from state n. It seems that this is the minimum required for Theorem 1. Further, using input a alone, we can reach $(n-1)^2+2$ of the subsets [8, p. 340, prob. 1]. This forms the basis for the next observation.

In light of the above theorem, we can ask ourselves whether there are any one-input NFA such that the subset construction gives a reduced, connected DFA with 2^n states. But if the subset machine is to be connected, each of the n states must map to a distinct singleton subset except one (since the initial state may always be reached), which must map to a subset with at least two states. If two-state subsets are to be reached, this state must map to a two-state subset. But now we can only reach $n-1$ of the $(1/2)n(n-1)$ possible two-state subsets. Hence the machine cannot be connected. (Use B_n with only the a input as an NDA which fits all the arguments.) Thus, we find that a one-input NFA has a reduced, connected subset machine with less than 2^n states.

Two-Way and One-Way Finite Automata

We now consider another generalization by Rabin and Scott, the two-way finite automaton (2DFA). Rabin and Scott as well as Shepherdson show that this modification is no more powerful than the one-way finite automaton [2], [3]. However, the construction to show this involves constructing a DFA in which the number of states is increased from n states to $(n+1)^{(n+1)}$ states. This establishes an upper bound on the number of states. The question now is whether this increase is always necessary, or whether the 2DFA may be simulated by a smaller state DFA.

We will now show that the upper bound may be approached. We will construct a 2DFA which uses $2k+5$ states (k an arbitrary parameter) while the same set can be accepted by a DFA which uses $k^k + k(2^k-2)+2$ states.

While $(2k+6)^{(2k+6)}$, which is of the same order as $(2k)^{2k}$, grows more rapidly than $k^k+k(2^k-2)+2$, which is of the same order as k^k, we will have constructed a 2DFA for which the equivalent DFA has a number of states of the same complexity as that given by the upper bound construction. That is $(2k)^{2k}$ is of the same complexity as k^k.

We assume that a 2DFA is a system $C = \langle S, \Sigma, M, s_0, F\rangle$, where S, Σ, s_0, and F are as for a DFA, and M is given by

$$M: S \times (\sum \cup \{¢, \$\}) \rightarrow \} -1, +1\} \times S.$$

That is, the input is $¢y\$$ where $y \in \Sigma^*$. ¢ and \$ are the left and right end markers, and M maps state and symbol into direction and new state.

The 2DFA accepts if it goes off the right end in an accepting state and rejects in all other cases.

The construction of the DFA proceeds by considering the states of the new DFA to be a pair, the first element of which is a mapping selected from the set of all possible mappings of S into $S \cup \{R\}$ (R a symbol not in S), and the second element of which is a state selected from the set of all states and the R symbol. This means, since we have $(n+1)^n$ possible choices of the first element and $n+1$ for the second, there will be $(n+1)^n(n+1) = (n+1)^{(n+1)}$ possible states. The DFA, as it moves right, keeps track of which mapping τ corresponds to the left portion of the tape in the first coordinate of its state. That is, if the 2DFA moved left into the left portion of the tape in state s, it would move right off of this portion of tape in $\tau(s)$ if it is a state and would reject by cycling or going off of the left end if $\tau(s) = R$. In the

$\tilde{A}$	a	b	c
→ 1	2	2	1
2	3	1	1
3	4	3	3
⋮			
k-1	k	k-1	k-1
(k)	1	k	k

Fig. 3. The finite automaton $\tilde{A}$.

C	a	b	c	d	¢	$
p	+p	+p	+p	+q	+p	+r
q	+q	+q	+q	+r		-s
s	-s	-s	-s	+1		
1	+2	+2	+1	+r		-1'
2	+3	+1	+1	+r		-2'
⋮						
k	+1	+k	+k	+f		+k'
1'	-1'	-1'	-1'	-1'	+1	-k'
2'	-2'	-2'	-2'	-2'	+2	
⋮						
k'	-k'	-k'	-k'	-k'	+k	
f	+f	+f	+f			+f
r	+r	+r	+r	+r		+r

Fig. 4. 2DFA to accept α.

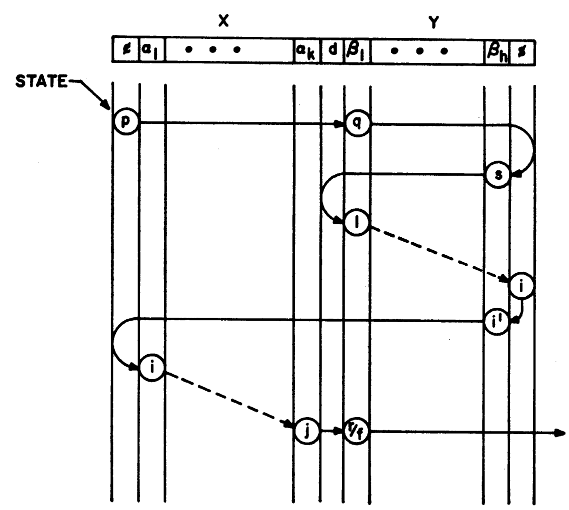

Fig. 5. A typical computation of C.

second coordinate of its state it keeps track of the state of C. Every possible mapping may not be necessary, however, since we want the DFA to be reduced and connected, so it is possible that the number of states may be less than $(n+1)^{(n+1)}$.

Now if $\tilde{A}$ is the k-state DFA with the state table shown in Fig. 3, then there is an input in $\{a, b, c\}^*$ which maps a k-tuple of states into another k-tuple of states with all k-tuples accessible from the identity k-tuple [6]. For every transformation of states there exists some input which will perform that transformation.

Note that input a causes a great permutation, input b causes a transposition, and input c causes a contraction. Thus, the semigroup of functions of $\{1, \cdots, k\}$ into itself is generated by the inputs a, b, c.

Now, consider the set

$$\alpha = \{xdy \mid x, y \in \{a, b, c\}^* \text{ and } yx \in T(\tilde{A})\}.$$

That is, α is the set of all tapes, of two parts x and y which are in the free semigroup generated by a, b, and c, and separated by symbol d, different from a, b, and c. In addition, it must be possible to take the two parts separated by the d, concatenate them together in the reverse order, yx, and have the resultant tape be in the set of tapes accepted by $\tilde{A}$.

First we consider how a 2DFA might accept α (or more precisely, the set of tapes ¢xdy\$). It would have a next-state table as shown in Fig. 4 (where unspecified entries will not occur).

The 2DFA, when in states p, q, r, checks to verify that only one d occurs. States $1, 2, \cdots, k$ then find to what state y takes $\tilde{A}$. States $1', 2', \cdots, k'$ are used to move left to the beginning of x, retaining the final state information of y. Finally, states $1, 2, \cdots, k$ find to what state x takes $\tilde{A}$. State f is a final accepting state and r is a final rejecting state. Thus $2k+5$ states are sufficient. A typical computation for a tape in the correct format is shown in Fig. 5.

State i is the result of feeding y to $\tilde{A}$ when started in state 1, and j is the result of feeding x to $\tilde{A}$ when started in state i.

Now we would like to construct a DFA to recognize α, and show that this DFA is the smallest state DFA that could recognize it. This will be done by building a DFA and showing that no two states are equivalent. The DFA, A', that we construct, has a state set $S' = S^S \cup \{(2^S - \{\varnothing, U\}) \times S\} \cup \{\varnothing, U\}$, where S is the state set of $\tilde{A}$, S^S is the set of all mappings of S into S, 2^S is the set of all subsets of S, U is the universal subset, $\varnothing$ is the null subset, and $2^S - \{\varnothing, U\}$ is the set of subsets of S without including $\varnothing$ and U, and $A \times B$ is the set of ordered pairs of elements from A and B. We take an element of S^S as $\tau = \langle i_1, i_2, \cdots, i_k \rangle$ where the jth coordinate of τ, i_j, is the state that j maps to under τ, i.e., $\tau(j) = i_j$. A typical element of $(2^S - \{\varnothing, U\}) \times S$ will be a pair $\langle Q, i \rangle$, where Q is a subset of S which is not U or $\varnothing$ and i is an element of S.

The next-state function M', will be given by the following, where M is the next-state function of $\tilde{A}$:

$$
\begin{aligned}
M'(\tau, \sigma) &= M'(\langle i_1, i_2, \cdots, i_k\rangle, \sigma), \\
&\qquad\qquad \text{for } \sigma \in \{a, b, c\} \\
&= \langle M(i_1, \sigma), \cdots, M(i_k, \sigma)\rangle \qquad (1) \\
M'(\tau, d) &= M'(\langle i_1, i_2, \cdots, i_k\rangle, d) \\
&= \langle Q, 1\rangle \qquad (2)
\end{aligned}
$$

where $j \in Q$ if and only if $i_j = k$, and $M'(\tau, d) = \varnothing$ if and only if for all j, $i_j = k$ and $M'(\tau, d) = U$ if and only if for all j, $i_j = k$.

$$
\begin{aligned}
&M'(\langle Q, i\rangle, \sigma) = \langle Q, M(i, \sigma)\rangle, \qquad \text{for } \sigma \in \{a, b, c\} \\
&M'(\langle Q, i\rangle, d) = \varnothing \qquad (3) \\
&M'(\varnothing, \sigma) = \varnothing, \qquad \text{for } \sigma \in \{a, b, c, d\} \\
&M'(U, \sigma) = U, \qquad \text{for } \sigma \in \{a, b, c\} \\
&M'(U, d) = \varnothing. \qquad (4)
\end{aligned}
$$

Finally, the initial state is the identity mapping $\langle 1, 2, \cdots, k\rangle$ and the final states are U and all those pairs $\langle Q, i\rangle$ where $i \in Q$.

It remains to be shown that there are no two equivalent states in A'. We first note that every mapping τ may be reached by some combination of inputs, hence any subset Q in $\langle Q, i\rangle$ is reachable. Thus A' is connected. It will be shown that no two states are equivalent by giving a tape which takes one of the pair to a final state but not the other.

1) For two distinct states $\tau, \eta \in S^S$ we select some coordinate in which they differ. That is, choose j so that $\tau(j) \neq \eta(j)$. Assume, without loss of generality, $\tau(j) > \eta(j)$, then $a^{k-\tau(j)} d\, a^j$ takes τ to a final state but not η.

2) For two states $\langle Q, i\rangle, \langle P, j\rangle \in (2^S - \{\varnothing, U\}) \times S$ we recognize two cases.

a) If $Q \neq P$, select $m \in Q$ and $m \notin P$, which is always possible, then $(ca)^k a^{m-1}$ takes $\langle Q, i\rangle$ to a final state and $\langle P, j\rangle$ does not go to a final state.

b) If $Q = P$, then we must have $i \neq j$. Assume $i > j$. Now select $m \in Q$, $l \notin Q$ which is possible since $Q \neq \varnothing$, $Q \neq U$. Assume $m > l$, the other case will follow by a similar argument. If $m - l \geq i - j$ then $a^{k-j+2}(ca)^{m-l-(i-j)} a^{l-2}$ takes state i to state m and j to state l. If $i - j > m - l$, then $a^{k-i+2}(ca)^{i-j-(m-l)} a^{m-2}$ produces the desired result.

3) Finally, for states τ and $\langle Q, i\rangle$, take $m \in Q$ and then a^{m-1} or a^{m-1+k} takes $\langle Q, i\rangle$ to a final state, but not τ.

Thus we have a reduced machine, and we have established that the bound in the construction may be approached.

Acknowledgment

The author would like to thank his advisor Prof. M. K. Hu of Syracuse University for his encouragement and advice, and Prof. R. Prather of the University of Vermont and Prof. G. Foster of Syracuse University for their many technical suggestions and improvements to this note.

References

[1] E. F. Moore, "Gedanken-experiments of sequential machines," in *Automata Studies* (Ann. of Math. Studies, no. 34). Princeton, N. J.: Princeton Univ. Press, 1956, pp. 129–153.

[2] M. O. Rabin and D. Scott, "Finite automata and their decision problems," *IBM J. Res. Develop.*, vol. 3, 1959, pp. 114–125.

[3] J. C. Shepherdson, "The reduction of two-way automata to one-way automata," *IBM J. Res. Develop.*, vol. 3, 1959, pp. 198–200.

[4] J. E. Hopcroft and J. D. Ullman, *Formal Languages and Their Relation to Automata.* Reading, Mass.: Addison-Wesley, 1969.

[5] M. O. Rabin, "Mathematical theory of automata," *Proc. Symp. Appl. Math.*, J. T. Schwartz, Ed., American Mathematical Society, 1967, vol. 19.

[6] R. J. Nelson, *Introduction to Automata.* New York: Wiley, 1968.

[7] F. R. Moore, "Deterministic realization and simulation of nondeterministic automata," Ph.D. dissertation, Syracuse University, Dep. Elec. Eng., Sept. 1969. (*Note:* An uncirculated technical report by G. Ott, "On multipath automata I," Sperry Rand Res. Rep. SRRC-RR-64-69, which contains some of the results of the first part of this paper, has come to the attention of the author subsequent to the notification of these results in [7].)

[8] M. A. Harrison, *Introduction to Switching and Automata Theory.* New York: McGraw-Hill, 1965.

Recognition of Monotonic and Unate Cascade Realizable Functions Using an Informational Model of Switching Circuits

W. S. MATHESON, MEMBER, IEEE

Abstract—A model of combinational switching circuits used as information processors is described. A set of entropies (in the information theory sense) can be associated with each completely specified function, and can be easily computed from the truth table representation for the function. It is shown that simple arithmetic relations between the magnitudes of these entropies are sufficient to identify monotonic and unate functions and functions realizable as a unate cascade. In the latter case, a simple test identifies unate cascade realizable functions and gives the set of possible orderings of variables in the realization.

Index Terms—Information theory, joint entropy, monotonic functions, unate cascades, unate functions, switching circuits.

Introduction

A single-output combinational switching circuit may be considered as a box with N input terminals and one output terminal. The signals on the terminals are binary and the output signal is known when the input signals are specified. Since the reverse is not generally true (that is, we do not know the input signals, given the output), then it is reasonable to consider the box as an "information processor," where some of the input information is lost in the box, the remainder being the output information. Such a device is called a "deterministic channel" in information theory [1].

In order to make the concept of "information" quantitive, we use the accepted definition of "joint information con-

Manuscript received July 27, 1970; revised December 17, 1970. This work was developed from the author's Ph.D. dissertation, University of British Columbia, Vancouver, B. C., Canada, and was supported in part by the Commonwealth Scholarship and Fellowship Plan.

The author is with the Department of Electrical Engineering Science, University of Essex, Wivenhoe Park, Colchester, Essex, England.