DISTINGUISHABILITY OF A SEMI-GROUP BY A MACHINE

SEYMOUR GINSBURG AND E. H. SPANIER[1]

1. **Introduction.** In this note we consider whether or not an arbitrary semi-group W can serve as the input semi-group of a machine which distinguishes among the elements of W. It is shown (Theorem 1) that the answer is in the affirmative. However, the number of states needed for such a machine may be arbitrarily large, that is, exceed an arbitrarily given cardinal number (Theorem 2). Even for a semi-group which is given by a finite number of generators and a finite number of relations there may be no finite state machine which distinguishes the elements (Theorem 3). In the language of data processing, this last statement implies that starting with a finite number of commands and identifying a finite number of pairs of subroutines, one cannot always find a finite state machine which does different work for nonequivalent programs [2].

The technical meaning of each of the less familiar concepts alluded to above is now given. The reader is referred to [1] for motivation and mathematical properties of these notions.

DEFINITION. A *machine* S is a quintuple $(K, W, Y, \delta, \lambda)$ satisfying the following conditions:

(i) K is a nonempty set (the set of "states").

(ii) W is a semi-group (the set of "inputs").

(iii) Y is a semi-group (the set of "outputs") in which the left cancellation law holds (i.e., if a, b, and c are in Y and $ab=ac$ then $b=c$).

(iv) δ is a function from $K \times W$ into K such that $\delta(q, IJ) = \delta[\delta(q, I), J]$ for all elements I and J in W and each q in K.

(v) λ is a function from $K \times W$ into Y such that $\lambda(q, IJ) = \lambda(q, I)\lambda[\delta(q, I), J]$ for all elements I and J in W and each q in K.

DEFINITION. In a machine two elements I and J of W are said to be *input-indistinguishable* if for each state q and each input M, $\lambda(q, I) = \lambda(q, J)$ and $\lambda(q, IM) = \lambda(q, JM)$. A machine is said to be *input-distinguished*, or to *distinguish between the distinct elements of* W, if there are no two elements of W which are input-indistinguishable.

It is known that a number of different situations related to data processing can be modeled by machines [2]. The left cancellation law of (iii) removes pathological cases and enables certain desired results

Received by the editors September 6, 1960.

[1] This work was performed while Dr. Spanier was consulting at System Development Corporation.

pertaining to indistinguishable states and input-indistinguishable inputs to hold [1].

2. **The existence of input-distinguished machines.** We assume that we are given a semi-group W and seek an input-distinguished machine with W as its set of inputs. If W satisfies the left cancellation law, then the one-state machine $(\{q_1\}, W, W, \delta, \lambda)$, where $\lambda(q_1, I) = I$ for each I in W, is input-distinguished. Thus our problem is reduced to the case where W does not satisfy the left cancellation law, a fact, so far, of little practicality. If we drop the condition of input-distinguishability, then there is no difficulty in finding a machine with W as its set of inputs. In fact, let 1 denote a semi-group with just one element. The one-state machine $(\{q_1\}, W, 1, \delta, \lambda)$ has W as its set of inputs but any two elements of W are input-indistinguishable.

A positive solution to the problem under discussion is furnished by the following result.

THEOREM 1. *Given an arbitrary semi-group W there exists an input-distinguished machine $S = (K, W, Y, \delta, \lambda)$.*

PROOF. For each element I in W let q_I be an abstract symbol. Let $K = \{q_*\} \cup \{q_I / I \text{ in } W\}$, where q_* is a symbol distinct from the q_I. For each I in W let I^* be an abstract element. Let Y be the semi-group generated by the set $\{I^* / I \text{ in } W\}$ and the relations $I^*J^* = J^*$ for all I^* and J^*. Then Y satisfies the left cancellation law. For each I and J in W let $\delta(q_*, I) = q_I$, $\delta(q_J, I) = q_{JI}$, $\lambda(q_*, I) = I^*$, and $\lambda(q_J, I) = (JI)^*$.

Consider the function δ. $\delta(q_*, IJ) = q_{IJ}$ and $\delta[\delta(q_*, I), J] = \delta(q_I, J) = q_{IJ}$; while $\delta(q_M, IJ) = q_{MIJ}$ and $\delta[\delta(q_M, I), J] = \delta(q_{MI}, J) = q_{MIJ}$. Consider the function λ. $\lambda(q_*, IJ) = (IJ)^*$ and $\lambda(q_*, I)\lambda[\delta(q_*, I), J] = I^*(IJ)^* = (IJ)^*$; while $\lambda(q_M, IJ) = (MIJ)^*$ and $\lambda(q_M, I)\lambda[\delta(q_M, I), J] = (MI)^*(MIJ)^* = (MIJ)^*$. Thus δ and λ satisfy the appropriate conditions making S a machine. For $I \neq J$, $\lambda(q_*, I) \neq \lambda(q_*, J)$. Thus no two different elements in W are input-indistinguishable. Consequently S satisfies the conclusion of the theorem. Q.E.D.

The machine S constructed in the proof of the above theorem has exactly one more state (namely q_*) than there are elements in the semi-group W. Thus if W is infinite, the machine constructed has an infinite number of states. It is natural to ask if machines with an arbitrarily large number of states are needed. The next section is concerned with this question.

3. **The number of states of input-distinguished machines.**

THEOREM 2. *For each infinite cardinal number $\aleph_\alpha$ there exists a*

semi-group W such that the number of states in any input-distinguished machine with W as its set of inputs is larger than $\aleph_\alpha$.

PROOF. Let W be the semi-group generated by the set $\{I^\xi/\xi<\omega_{\alpha+1}\}$ ($\omega_{\alpha+1}$, as usual, is the smallest ordinal number of cardinal $\aleph_{\alpha+1}$) and the relations $I^\xi I^\upsilon = I^\theta$, where $\theta = \max\{\xi, \upsilon\}$. Let $S=(K, W, Y, \delta, \lambda)$ be a machine with fewer than $\aleph_{\alpha+1}$ states. We shall show that S cannot be input-distinguished.

Let q be any state in K. Since K has power less than or equal to $\aleph_\alpha$ and W has power $\aleph_{\alpha+1}$, there exists a subset H_q' of W of power $\aleph_{\alpha+1}$ and a state $\bar{q}$ such that $\delta(q, I)=\bar{q}$ for all I in H_q'.

With the notation above define $H_q=\{I/I \text{ in } W, \delta(q, I)=\bar{q}\}$. We shall show that H_q consists of all I^ξ for sufficiently large ξ. To this end we first establish the following subsidiary result.

(i) $\lambda(\bar{q}, I)$ is independent of I in W.

To see this let I^ξ and I^υ be any two elements of W. Select $\gamma>\xi, \upsilon$ such that I^γ is in H_q. Such a choice of γ is possible because H_q has power $\aleph_{\alpha+1}$. Then

$$\lambda(q, I^\gamma) = \lambda(q, I^\gamma I^\xi) = \lambda(q, I^\gamma)\lambda(\bar{q}, I^\xi)$$

and

$$\lambda(q, I^\gamma) = \lambda(q, I^\gamma I^\upsilon) = \lambda(q, I^\gamma)\lambda(\bar{q}, I^\upsilon).$$

Since Y satisfies the left cancellation law, it follows that $\lambda(\bar{q}, I^\xi) = \lambda(\bar{q}, I^\upsilon)$ proving (i).

(ii) If I^ξ is in H_q and $\upsilon>\xi$, then I^υ is also in H_q.

For this choose $\gamma>\upsilon$ such that I^γ is in H_q. Then $\delta(q, I^\upsilon)=\delta(q, I^\xi I^\upsilon) = \delta[\delta(q, I^\xi), I^\upsilon]=\delta[\delta(q, I^\gamma), I^\upsilon]=\delta(q, I^\gamma I^\upsilon)=\delta(q, I^\gamma)=\bar{q}$.

It follows from (ii) that there is an ordinal number $\tau(q)$ such that $H_q=\{I^\xi/\tau(q)\leqq\xi\}$. (Let $\tau(q)$ be the smallest ξ such that I^ξ is in H_q.) To show that S cannot be input-distinguished we need one additional result.

(iii) If $\gamma>\tau(q)$, then $\lambda(q, I^\gamma)$ is independent of I^γ.

This is seen by observing that if $\gamma>\tau(q)$, then $\lambda(q, I^\gamma)=\lambda(q, I^{\tau(q)}I^\gamma) = \lambda(q, I^{\tau(q)})\lambda(\bar{q}, I^\gamma)$. Now $\lambda(q, I^{\tau(q)})$ is independent of I^γ, and, by (i), $\lambda(\bar{q}, I^\gamma)$ is independent of I^γ so (iii) is proved.

To complete the proof of the theorem we note that since K is of power $\leqq\aleph_\alpha$ there exists an ordinal number $\sigma<\omega_{\alpha+1}$ such that $\tau(q)\leqq\sigma$ for all q in K. From (iii) it follows that for $\xi, \upsilon>\sigma$ and for each state q then $\lambda(q, I^\xi)=\lambda(q, I^\upsilon)$. From the definition of $\tau(q)$ it follows that $\delta(q, I^\xi)=\delta(q, I^\upsilon)$. Hence I^ξ and I^υ are input-indistinguishable, and S is not an input-distinguished machine.

The semi-groups constructed in Theorem 2 are not finitely generated. We now consider the case when W is generated by a finite alphabet and a finite number of relations. We are interested in ascertaining whether or not there exists a *finite* state, input-distinguished machine with W as its set of inputs. (Since W is denumerable, it follows from the proof of Theorem 1 that there exists a denumerable state machine with the desired properties.) These finiteness restrictions not only are of mathematical interest but have relevancy in data processing [2].

THEOREM 3. *There exists a semi-group W, generated by a finite alphabet and a finite number of relations, which is not the input semi-group to any finite state, input-distinguished machine.*

PROOF. Let W be the semi-group generated by the finite set $\{I_1, I_2, I_3\}$ and the two relations $I_1I_2 = I_1I_3$ and $I_1I_1I_2 = I_1I_2I_1$. An immediate consequence of the two relations is that $I_1I_1I_3 = I_1I_3I_1$.

(a) $I_1^nI_2^n = I_1^nI_3^n = (I_1I_2)^n$ for all n, where $J^n = J \cdot \cdot \cdot J$ (n times). To see this observe that $I_1I_1I_2I_2 = I_1I_2I_1I_2$. Using induction, suppose that for $k \leqq m$ (i) $I_1^kI_2^k = (I_1I_2)^k$ and (ii) $I_1(I_1I_2)^k = (I_1I_2)^kI_1$. Then $I_1^{m+1}I_2^{m+1} = I_1(I_1^mI_2^m)I_2 = I_1(I_1I_2)^mI_2 = (I_1I_2)^mI_1I_2 = (I_1I_2)^{m+1}$ and $I_1(I_1I_2)^{m+1} = I_1I_1I_2(I_1I_2)^m = I_1I_2I_1(I_1I_2)^m = (I_1I_2)(I_1I_2)^mI_1 = (I_1I_2)^{m+1}I_1$. Thus (i) and (ii) hold for all integers m. Similarly $I_1^mI_3^m = (I_1I_3)^m$ and $I_1(I_1I_3)^m = (I_1I_3)^mI_1$ for all integers m. Then $I_1^nI_2^n = (I_1I_2)^n = (I_1I_3)^n = I_1^nI_3^n$ for all integers n.

(b) $I_1^nI_2^{n+1} = I_1^nI_3^{n+1}$ for no n. The reasoning is as follows. By (a), $I_1^nI_2^{n+1} = (I_1I_2)^nI_2$ and $I_1^nI_3^{n+1} = (I_1I_3)^nI_3 = (I_1I_2)^nI_3$. Assume now that (b) is false. That is, assume that there is an integer n so that $(I_1I_2)^nI_2 = (I_1I_2)^nI_3$. Let $N_1, N_2, \cdot \cdot \cdot, N_p$ be any proof of this last relation, i.e., a finite sequence of words such that N_1 is $(I_1I_2)^nI_2$, N_p is $(I_1I_2)^nI_3$, and N_{i+1} is obtained from N_i by a replacement of either (i) I_1I_3 for I_1I_2 or (ii) I_1I_2 for I_1I_3 or (iii) $I_1I_1I_2$ for $I_1I_2I_1$ or (iv) $I_1I_2I_1$ for $I_1I_1I_2$. Let N_r be the first word of the proof such that the right-most symbol occurrence is replaced in passing to the succeeding word of the proof. Clearly, each N_i, $1 \leqq i \leqq r$, can be written in the form M_iI_2. N_r certainly exists since N_p is not of this form. Moreover, $M_1, M_2, \cdot \cdot \cdot, M_r$ is a valid proof of $M_1 = M_r$. Since N_{r+1} must be obtained from N_r by either (i) or (iv), M_r is JI_1 for some J. M_1 is $(I_1I_2)^n$. It will now be shown that the existence of the proof $M_1, M_2, \cdot \cdot \cdot, M_r$ for $(I_1I_2)^n = JI_1$ leads to a contradiction. It is readily seen that the following three properties about the words $M = M_j$ are preserved in going from M_i to M_{i+1}.

(1) The number of occurrences of I_1^k in M is n.

(2) If M is the word $H_1I_2H_2$ or $H_1I_3H_2$; then H_1 is a nonempty word and $n_2-n_1<n_1$, where n_2 is the length of H_1 and n_1 is the number of occurrences of I_1 in H_1.

(3) M is of length $2n$.

From (1) and (3), JI_1 is not of the form I_1. Thus JI_1 is either of the form $H_1I_2I_1^s$ or $H_1I_3I_1^s$. From (1) and (3), $n_1=n-s$ and $n_2=2n-s-1$. Then $n_1\leqq n-1=n_2-n_1$, which contradicts (2). Thus the proof $M_1, \cdots, M_r$ of $(I_1I_2)^n=JI_1$ does not exist, demonstrating (b).

(c) There is no finite state, input-distinguished machine $S=(K, W, Y, \delta, \lambda)$. For suppose the contrary, i.e., let $S=(K, W, Y, \delta, \lambda)$ be a finite state, input-distinguished machine. Consider the sequence of pairs of elements of W whose typical term is $(I_1^kI_2^{k+1}, I_1^kI_3^{k+1})$. By (b), the two elements in each pair are different elements of W. As S is input-distinguished and K is finite there is a state q_0 which distinguishes[2] infinitely many of these pairs. Hence there is an infinite set A of integers so that for each integer j in A there is a word (possible empty) M_j of W with the property that

$$\lambda(q_0, I_1^jI_2^{j+1}M_j) \neq \lambda(q_0, I_1^jI_3^{j+1}M_j).$$

Let j and k, $j<k$, be two integers in A having the property that $\delta(q_0, I_1^j)=\delta(q_0, I_1^k)$. Since K is finite, the integers j and k certainly exist. Let $q_1=\delta(q_0, I_1^j)$. Then

$$\delta(q_1, I_1^{k-j}) = \delta[\delta(q_0, I_1^j), I_1^{k-j}] = \delta(q_0, I_1^k) = q_1.$$

Hence for any integer m there exists a state q_2 such that $\delta(q_2, I_1^m)=q_1$ (merely let $q_2=\delta(q_1, I_1^n)$, where n is chosen so that $n+m$ is a multiple of $k-j$). Thus there exists a state q_3 such that $\delta(q_3, I_1^{j+1})=q_1$. Then

$$\begin{aligned}\lambda(q_3, I_1^{j+1}I_2^{j+1}M_j) &= \lambda(q_3, I_1^{j+1})\lambda[\delta(q_3, I_1^{j+1}), I_2^{j+1}M_j] \\ &= \lambda(q_3, I_1^{j+1})\lambda(q_1, I_2^{j+1}M_j).\end{aligned}$$

Similarly $\lambda(q_3, I_1^{j+1}I_3^{j+1}M_j)=\lambda(q_3, I_1^{j+1})\lambda(q_1, I_3^{j+1}M_j)$. Since $I_1^{j+1}I_2^{j+1}=I_1^{j+1}I_3^{j+1}$,

$$\lambda(q_3, I_1^{j+1})\lambda(q_1, I_2^{j+1}M_j) = \lambda(q_3, I_1^{j+1})\lambda(q_1, I_3^{j+1}M_j).$$

As left cancellation holds in Y, it follows that $\lambda(q_1, I_2^{j+1}M_j)=\lambda(q_1, I_3^{j+1}M_j)$. Then

[2] A state q_0 is said to *distinguish* the inputs I and J if either $\lambda(q_0, I)\neq\lambda(q_0, J)$ or $\lambda(q_0, I)=\lambda(q_0, J)$ but there exists M such that $\lambda(q_0, IM)\neq\lambda(q_0, JM)$.

$$\lambda(q_0, I_1^j I_2^{j+1} M_j) = \lambda(q_0, I_1^j)\lambda(q_1, I_2^{j+1} M_j)$$
$$= \lambda(q_0, I_1^j)\lambda(q_1, I_3^{j+1} M_j)$$
$$= \lambda(q_0, I_1^j I_3^{j+1} M_j),$$

contradicting the fact that $\lambda(q_0, I_1^j I_2^{j+1} M_j) \neq \lambda(q_0, I_1^j I_3^{j+1} M_j)$. Therefore S cannot be a finite state, input-distinguished machine and (c), thus the theorem, is proved.

REMARKS. (1) It would be of interest to find some general conditions on a semi-group W, generated by a finite alphabet and a finite number of relations, which guarantee the existence of a finite state, input-distinguished machine $(K, W, Y, \delta, \lambda)$.

(2) It is known that there exist semi-groups, generated by a finite alphabet and a finite number of relations, in which the word problem is unsolvable, i.e., there is no finite procedure for deciding whether or not two words are equal [3]. For such a semi-group W, if there exists a finite state, input-distinguished machine with W as its set of inputs, then the word problem in the output semi-group Y is also unsolvable. For suppose that the word problem in Y is solvable. Let I_1 and I_2 be any two words in W. For each state q it can be decided in a finite number of steps whether or not $\lambda(q, I_1) = \lambda(q, I_2)$ and whether or not $\delta(q, I_1)$ and $\delta(q, I_2)$ are indistinguishable states.[3] Thus it can be decided in a finite number of steps whether or not I_1 and I_2 are input-indistinguishable,[4] thus whether or not I_1 and I_2 are equal. Consequently the word problem in W is solvable, which is a contradiction.

In connection with Remark (1) above, the following result, due to the referee (as are the two results after the next theorem), shows that no effective necessary and sufficient conditions exist.

THEOREM 4. *It is recursively unsolvable to determine for an arbitrary semi-group W, given by a finite alphabet and a finite number of defining relations whether or not there exists a finite state, input-distinguished machine $(K, W, Y, \delta, \lambda)$.*

[3] Two states q_1 and q_2 in a machine $S=(K, W, Y, \delta, \lambda)$ are said to be *indistinguishable* if $\lambda(q_1, I) = \lambda(q_2, I)$ for each input I. In case S is a machine with n states, W and Y are free semi-groups generated by the finite alphabets Σ and Δ respectively, and $\lambda(q, I)$ is in Δ for each state q and each I in Σ; then it is known that two states q_1 and q_2 are indistinguishable if and only if $\lambda(q_1, J) = \lambda(q_2, J)$ for all words J of length at most $n-1$ [5]. This result is easily seen to hold for any machine with n states whether W is freely generated by Σ or not.

[4] In any machine I_1 and I_2 are *input-indistinguishable* if and only if for each state q, $\delta(q, I_1)$ and $\delta(q, I_2)$ are indistinguishable states and $\lambda(q, I_1) = \lambda(q, I_2)$ [1].

PROOF. Call a semi-group finitely presented if it can be given by a finite alphabet and a finite number of defining relations. The theorem is a direct application of the following result of Markov [4]. A property P about finitely presented semi-groups is called Markov if

(1) every semi-group isomorphic to a semi-group having property P also has property P;

(2) there is a semi-group W_1 which has property P;

(3) there is a finitely presented semi-group W_2 which does not have property P and is not imbedded in any semi-group having property P.

The cited theorem asserts that for no Markov property P does there exist an algorithm for deciding in a finite number of steps whether or not an arbitrarily given finitely presented semi-group has property P. Thus we need only verify that being the input semi-group of some finite state, input-distinguished machine is a Markov property.

Now (i) is trivial. As to (ii) let W_1 be the semi-group with just one element. With W_1 as the set of inputs, the one state machine $(\{q_1\}, W_1, W_1, \delta, \lambda)$ is input-distinguished. As to (iii), let the semi-group W used in the proof of Theorem 3 be imbedded in a semi-group W'. We assert that there is no finite state, input-distinguished machine of which W' is the set of inputs. The equations (a) and inequations (b) of the proof of Theorem 3 certainly remain valid under the assumption that W is embedded in W'. The nontrivial point is that the argument for (c) of the proof of Theorem 3 remains valid if the variable M_j has W' as its domain. But to see this we need only replace W by W' at all occurrences in the statement of and argument for (c)—with the exception of the second sentence following the statement of (c). Then (a), (b), and (c) thus revised of the proof of Theorem 3 furnish the proof of (iii) needed here.

REMARK. The Markov theorem quoted above yields two other results pertinent to the topic under discussion.

(1) It is recursively unsolvable to determine of an arbitrary machine whether or not it is input-distinguished.

PROOF. The one state machine $(\{q_1\}, W, 1, \delta, \lambda)$ of the first paragraph of §2 is input-distinguished if and only if W is the semi-group with just one element. But, clearly, the property of being the semi-group of just one element is a Markov property of finitely presented semi-groups. Hence the result.

(2) It is recursively unsolvable to determine of an arbitrary finite state machine $(K, W, Y, \delta, \lambda)$, where (i) W is finitely presented and satisfies the left cancellation law, and (ii) Y is finite, whether or not it is input-distinguished.

PROOF. It is known that one cannot determine recursively of a

finitely presented cancellation semi-group whether or not it consists of just one element [6]. This and the construction in (1) above yield the result.

BIBLIOGRAPHY

1. S. Ginsburg, *Some remarks on abstract machines*, Trans. Amer. Math. Soc. vol. 96 (1960) pp. 400–444.

2. ———, *Examples of abstract machines*, TM 517, System Development Corp.

3. S. Kleene, *Introduction to metamathematics*, New York, Van Nostrand Co., 1952.

4. A. Markov, *Impossibility of algorithms for recognizing some properties of associative systems*, Dokl. Akad. Nauk SSSR vol. 77 (1951) pp. 953–956.

5. E. F. Moore, *Gedanken—experiments on sequential machines*, Automata Studies, Annals of Mathematics Studies, No. 34, Princeton University Press, 1956, pp. 129–153.

6. M. D. Rabin, *Recursive unsolvability of group theoretic problems*, Ann. of Math. vol. 67 (1958) pp. 172–194.

SYSTEM DEVELOPMENT CORPORATION AND
UNIVERSITY OF CALIFORNIA, BERKELEY