Kybernetika

Marie Demlová; Václav Koubek

Fast diagnosis of some semigroup properties of automata

Kybernetika, Vol. 22 (1986), No. 1, 92--99

Persistent URL: http://dml.cz/dmlcz/125541

FAST DIAGNOSIS OF SOME SEMIGROUP PROPERTIES OF AUTOMATA

MARIE DEMLOVÁ, VÁCLAV KOUBEK

The aim of this note is to improve the results of Watanabe and Nakamura. We present algorithms which for a given automaton A decide whether the transition semigroup of A contains left or right identity, or whether the transition semigroup of A is a left or a right group, or permutation group in linear time (i.e. it requires $O(|Q| \cdot |X|)$ time where Q is the set of states of A, X is the set of inputs of A). Further we give algorithms which for a given automaton A decide whether A is quasi-state independent, or state independent and requires $O(|Q|^2 \cdot |X|)$ time.

A recent paper by T. Watanabe and A. Nakamura, [5], offers several useful algorithms with aid of which one can quickly recognize some elementary properties of the transition semigroups of automata, such as, for example, the presence of one-sided or both-sided identities, cancellation properties, etc. The transition semigroup of an automaton A is given by a family of generators of $S(A)$ usually described by the transition function $\delta\colon Q \times X \to Q$ of A (specifying the action of inputs X on states Q), hence the input data for the algorithms in question may be considered as of size $Q \times X$.

When applying to the algorithms in [5] one of the most common efficiency criterion, namely, the asymptotic worst-case time complexity related to the RAM model with uniform cost function (without arithmetical operations), one can see almost immediately there is a margin left for improvement on Watanabe-Nakamura algorithms, what we actually do in the present note.

An automaton A will be given by two-dimensional $|Q \times X|$-array

	x_0	x_1	$\dots$	x_i	$\dots$
q_0	$\delta(q_0, x_0)$	$\delta(q_0, x_1)$	$\dots$	$\delta(q_0, x_i)$	$\dots$
q_1	$\delta(q_1, x_0)$	$\delta(q_1, x_1)$	$\dots$	$\delta(q_1, x_i)$	$\dots$
$\vdots$					
q_j	$\delta(q_j, x_0)$	$\delta(q_j, x_1)$	$\dots$	$\delta(q_j, x_i)$	$\dots$
$\vdots$					

A function f from a set Z will be given by one-dimensional $|Z|$-array

z_0	z_1	...	z_i	...
$f(z_0)$	$f(z_1)$	...	$f(z_i)$	...

Thus the values $\delta(q_j, x_i)$ or $f(z_k)$ are computed in one step of computation.

First let us recall some elementary semigroup notions (see [2]). An element x of a semigroup S is called *left* (or *right*) *identity* if for every $y \in S$ we have $xy = y$ (or $yx = y$, respectively). If x is both left and right identity then it is called *identity*. A semigroup S is called *left-zero* (or *right-zero*) if for every pair x, y of elements of S we have $xy = x$ (or $xy = y$, respectively). We say that a semigroup S is a *left group* (or a *right group*) if S is isomorphic to a product of a group and a left-zero (or right-zero, respectively) semigroup. A transformation semigroup F on a finite set is said to be a *permutation group* if every transformation in F is a bijection. For an automaton A denote by $S(A)$ the transformation semigroup on the set Q generated by $\{\delta(-, x); x \in X\}$. We recall that we compose mapping from the left to the right, i.e. $f \circ g(x) = f(g(x))$.

The following improves Theorem 4 in [5]:

Theorem 1. There exists an algorithm deciding for a given automaton A that of the following conditions hold:

a) $S(A)$ has a left identity;
b) $S(A)$ has a right identity;
c) $S(A)$ has an identity;
d) $S(A)$ is a left-zero semigroup;
e) $S(A)$ is a right-zero semigroup;
f) $S(A)$ is a left group;
g) $S(A)$ is a right group;
h) $S(A)$ is a group;
i) $S(A)$ is a permutation group,

and requiring $O(|Q| \cdot |X|)$ time.

The corresponding algorithms in [5] require $O(|Q|^2 \cdot |X|)$ time.

An automaton A is called *quasi-state independent* if some state $q \in Q$ fulfils:
(+) for every pair f, g of different mappings from $S(A)$ we have $f(q) \neq g(q)$.
An automaton is said to be *state independent* if every state fulfils (+). Quasi-state independent and state independent automata were investigated in papers [6] and [7]. For example, for every finite semigroup S there exists a quasi-state independent automaton A such that $S(A)$ and S are isomorphic. On the other hand, if an automaton A is state independent, then $S(A)$ is a right group.

The second result of this note improves Theorems 7 and 8 in [5].

Theorem 2. There exists an algorithm deciding whether a given automaton is state independent, or quasi-state independent, requiring $O(|Q|^2 \cdot |X|)$ time.

The corresponding algorithms in [5] require $O(\max\{|Q|^3 |X|, |Q|^5\})$ time for quasi-state independent automata, $O(\max\{|Q| . |X|^2, |Q|^2 . |X|, |Q|^4\})$ time for state independent automata.

For a mapping $f: Z \to Y$, $\mathrm{Im}\, f$ denotes the image of f, $\mathrm{Ker}\, f$ denotes the kernel of f(i.e. $(x, y) \in \mathrm{Ker}\, f$ iff $f(x) = f(y)$).

The proof of Theorem 1 is based on the following lemmas:

Lemma 3. a) $S(A)$ has a right identity if and only if there exists $x \in X$ such that $|\mathrm{Im}\, \delta(-, x)| = |\mathrm{Im}\, \delta(-, x)^2|$ and for every $y \in X$, $\mathrm{Ker}\, \delta(-, x) \subseteq \mathrm{Ker}\, \delta(-, y)$.

b) $S(A)$ has a left identity if and only if there exists $x \in X$ such that $|\mathrm{Im}\, \delta(-, x)| = |\mathrm{Im}\, \delta(-, x)^2|$ and for every $y \in X$, $\mathrm{Im}\, \delta(-, x) \supseteq \mathrm{Im}\, \delta(-, y)$.

Proof. For a word $v \in X^+$ denote by $f_v = \delta(-, v)$. Now, assume that $f \in S(A)$ is a right identity of $S(A)$. Then for every $g \in S(A)$ we have $g \circ f = g$ and hence $\mathrm{Ker}\, f \subseteq \mathrm{Ker}\, g \circ f = \mathrm{Ker}\, g$. If $f = f_{x_1} \circ f_{x_2} \circ \ldots \circ f_{x_n}$ where $x_1, x_2, \ldots, x_n \in X$ then evidently $\mathrm{Ker}\, f_{x_n} \subseteq \mathrm{Ker}\, f \subseteq \mathrm{Ker}\, f_{x_n}$. Thus set $x = x_n$, then $\mathrm{Ker}\, f_x \subseteq \mathrm{Ker}\, f_y$ for every $y \in X$. Since $\mathrm{Ker}\, f_{x_n}^2 \subseteq \mathrm{Ker}\, f_{x_{n-1}} \circ f_{x_n} \subseteq \mathrm{Ker}\, f$ we have $\mathrm{Ker}\, f_x^2 = \mathrm{Ker}\, f_x$ and hence $|\mathrm{Im}\, f_x^2| = |\mathrm{Im}\, f_x|$.

On the other hand, if $|\mathrm{Im}\, f_x^2| = |\mathrm{Im}\, f_x|$ then the fineteness of Q implies that there exists n such that f_x^n is an idempotent and $|\mathrm{Im}\, f_x^n| = |\mathrm{Im}\, f_x|$. Thus $\mathrm{Ker}\, f_x^n = \mathrm{Ker}\, f_x$. Since $\mathrm{Ker}\, f_x \subseteq \mathrm{Ker}\, f_y$ for every $y \in X$ we have that $\mathrm{Ker}\, f_x^n = \mathrm{Ker}\, f_x \subseteq \mathrm{Ker}\, f_v$ for every non-empty word $v \in X^+$. The idempotency of f_x^n and this fact imply $f_v \circ f_x^n = f_v$ for every $v \in X^+$ — hence f_x^n is a right identity of $S(A)$.

The proof of b) is dual. If $f = f_{x_1} \circ f_{x_2} \circ \ldots \circ f_{x_n} \in S(A)$ is a left identity of $S(A)$ and $x_1, x_2, \ldots, x_n \in X$ then $f_{x_1} \circ f = f_{x_1}$ implies $\mathrm{Im}\, f_{x_1} \subseteq \mathrm{Im}\, f \subseteq \mathrm{Im}\, f_{x_1}$ and hence $\mathrm{Im}\, f_{x_1} = \mathrm{Im}\, f$. Further $\mathrm{Im}\, f_{x_1} = \mathrm{Im}\, f \supseteq \mathrm{Im}\, g$ for every $g \in S(A)$ because $f \circ g = g$ for $g \in S(A)$. Moreover $\mathrm{Im}\, f \subseteq \mathrm{Im}\, f_{x_1} \circ f_{x_2} \subseteq \mathrm{Im}\, f_{x_1}^2$ and therefore $|\mathrm{Im}\, f_{x_1}^2| = |\mathrm{Im}\, f_{x_1}|$. Thus it suffices to set $x = x_1$.

On the other hand, analogously as above, there exists n with f_x^n an idempotent and $\mathrm{Im}\, f_x^n = \mathrm{Im}\, f_x$. Hence for every non-empty word $v \in X^+$ $\mathrm{Im}\, f_v \subseteq \mathrm{Im}\, f_x = \mathrm{Im}\, f_x^n$ and the idempotency of f_x^n implies $f_x^n \circ f_v = f_v$. Thus f_x^n is a left identity of $S(A)$. □

Lemma 4. a) $S(A)$ is a right group if and only if for every pair $x, y \in X$, we have $\mathrm{Im}\, f_x = \mathrm{Im}\, f_y$ and $|\mathrm{Im}\, f_x| = |\mathrm{Im}\, f_x^2|$.

b) $S(A)$ is a left group if and only if for every pair $x, y \in X$ we have $\mathrm{Ker}\, f_x = \mathrm{Ker}\, f_y$ and $|\mathrm{Im}\, f_x| = |\mathrm{Im}\, f_x^2|$.

Proof. Assume that $S(A)$ is a right group, then there exist a group G, a right-zero semigroup S, and an isomorphism $\varphi: G \times S \to S(A)$. For a simplicity we identify every pair (g, s) with $\varphi(g, s)$ (i.e. we assume that $S(A) = G \times S$). Let e be the identity of G. Take $g \in G$, $s \in S$, then $(g^{-1}, s) \circ (g, s) = (e, s)$, $(g, s) \circ (e, s) = (g, s)$. Hence $\mathrm{Im}\,(g, s) \subseteq \mathrm{Im}\,(e, s) \subseteq \mathrm{Im}\,(g, s)$ and therefore $\mathrm{Im}\,(g, s) = \mathrm{Im}\,(e, s)$. Further for $s_1, s_2 \in S$ we have $(e, s_1) \circ (e, s_2) = (e, s_1)$, $(e, s_2) \circ (e, s_1) = (e, s_2)$ and thus

$\operatorname{Im}(e, s_1) = \operatorname{Im}(e, s_2)$. As a consequence we have $\operatorname{Im}(g_1, s_1) = \operatorname{Im}(g_2, s_2)$ for any $g_1\ g_2 \in G$, $s_1, s_2 \in S$. Hence for every $x, y \in X$ we obtain $\operatorname{Im} f_x = \operatorname{Im} f_y$ and $|\operatorname{Im} f_x| = |\operatorname{Im} f_x^2|$.

On the other hand suppose that for every $x, y \in X$ it holds $\operatorname{Im} f_x = \operatorname{Im} f_y$ and $|\operatorname{Im} f_x| = |\operatorname{Im} f_x^2|$. Since $\{f_x; x \in X\}$ generates $S(A)$ we get $\operatorname{Im} f = \operatorname{Im} g$ for every pair $f, g \in S(A)$. Set $E = \{f \in S(A); f = f^2\}$, then for every $f \in S(A)$, $g \in E$ we have $g \circ f = f$. Therefore E is a right-zero semigroup. For any $f \in S(A)$, set $S_f = \{g \in S(A); \operatorname{Ker} g = \operatorname{Ker} f\}$ then S_f is a subsemigroup of $S(A)$ with $|E \cap S_f| = 1$. Since for every $g \in S(A)$ there exists n such that g^n is an idempotent we get that S_f is a group. For every pair $e_1, e_2 \in E$, define $\varphi_{e_1,e_2}: S_{e_1} \to S_{e_2}$ as follows: $\varphi_{e_1,e_2}(f) = f \circ e_2$. Since $\operatorname{Ker} f \circ e_2 \supseteq \operatorname{Ker} e_2$ and $\operatorname{Im} f \circ e_2 = \operatorname{Im} e_2$ we obtain by finiteness of Q that $\operatorname{Ker} f \circ e_2 = \operatorname{Ker} e_2$ – thus φ_{e_1,e_2} is a mapping from S_{e_1} to S_{e_2}. Since e_1 and e_2 are left identities of $S(A)$ we conclude that φ_{e_1,e_2} is a homomorphism and $\varphi_{e_2,e_1} \circ \varphi_{e_1,e_2}(f) = f$, $\varphi_{e_1,e_2} \circ \varphi_{e_2,e_1}(g) = g$ for any $f \in S_{e_1}$, $g \in S_{e_2}$. Therefore φ_{e_1,e_2} and φ_{e_2,e_1} are isomorphisms. Choose $e \in E$. Define $\psi: E \times S_e \to S(A)$, $\psi(g, f) = f \circ g$ for $g \in E$, $f \in S_e$. Then for $g_1, g_2 \in E$, $f_1, f_2 \in S_e$ we have $\psi(g_1 \circ g_2, f_1 \circ f_2) = \psi(g_1, f_1 \circ f_2) = f_1 \circ f_2 \circ g_2 = f_1 \circ g_1 \circ f_2 \circ g_2 = \psi(g_1, f_1) \circ \psi(g_2, f_2)$ and hence ψ is a homomorphism. Further for every $g \in E$, $f \in S_e$ we have $\psi(g, f) = \varphi_{e,g}(f)$ and $\psi(e, f) = f$ – thus ψ is an isomorphism and $S(A)$ is a right group.

The proof of b) is dual. If $S(A)$ is a left group. Analogously as above there exist a group G and a left-zero semigroup S such that we can identify $S(A)$ with $G \times S$. Then for $g \in G$, $s, s_1, s_2 \in S$, and the identity e of G, the following equations hold $(g, s) \circ (g^{-1}, s) = (e, s)$, $(e, s) \circ (g, s) = (g, s)$, $(e, s_1) \circ (e, s_2) = (e, s_1)$, $(e, s_2) \circ (e, s_1) = (e, s_2)$, and, as a consequence, we obtain $\operatorname{Ker}(g_1, s_1) = \operatorname{Ker}(g_2, s_2)$ for any $g_1, g_2 \in G$, $s_1, s_2 \in S$. Thus for every pair $x, y \in X$ we have $\operatorname{Ker} f_x = \operatorname{Ker} f_y$ and $|\operatorname{Im} f_x^2| = |\operatorname{Im} f_x|$.

On the other hand assume that for every $x, y \in X$ it holds: $\operatorname{Ker} f_x = \operatorname{Ker} f_y$ and $|\operatorname{Im} f_x^2| = |\operatorname{Im} f_x|$. Then for $f, g \in S(A)$ we obtain $\operatorname{Ker} f = \operatorname{Ker} g$. Set $E = \{f \in S(A); f^2 = f\}$. Since for $f \in S(A)$, $g \in E$ we have $f \circ g = f$ we conclude that E is a left-zero semigroup. For $f \in S(A)$ set $S_f = \{g \in S(A); \operatorname{Im} g = \operatorname{Im} f\}$. Then $|E \cap S_f| = 1$ and S_f is a subsemigroup of $S(A)$. By the same reason as above we obtain that S_f is a group. Further, for $e_1, e_2 \in E$, define $\varphi_{e_1,e_2}: S_{e_1} \to S_{e_2}$ such that $\varphi_{e_1,e_2}(f) = e_2 \circ f$. Since $\operatorname{Ker} e_2 = \operatorname{Ker} e_2 \circ f$ and $\operatorname{Im} e_2 \supseteq \operatorname{Im} e_2 \circ f$ we have that $\operatorname{Im} e_2 = \operatorname{Im} e_2 \circ f$ (we use the finiteness of Q) and hence $\varphi_{e_1,e_2}(f) \in S_{e_2}$. Since e_1, e_2 are right identities of $S(A)$ we have that φ_{e_1,e_2} is an isomorphism of S_{e_1} onto S_{e_2}. Choose $e \in E$ and define $\psi: E \times S_e \to S(A)$ as follows: for $g \in E$, $f \in S_e$ set $\psi(g, f) = g \circ f$. By a straightforward calculation – see above – we obtain that ψ is a homomorphism and $\psi(g, f) = \varphi_{e,g}(f)$ for every $g \in E$, $f \in S_e$, hence ψ is an isomorphism. □

To prove Theorem 1 we need two auxiliary algorithms, the first one is an easy exercise, the second one is described in [3] (it is called Algorithm A in that paper).

Lemma 5. a) There is an algorithm which for a given set F of mappings from Y

to Z and for a set $A \subset Y$ computes $|\cup \{f(A); f \in F\}|$ and which requires $O(|F| \cdot |Y|)$ time.

b) There is an algorithm which for a given set F of mappings from Y to Z constructs $\cap \{\operatorname{Ker} f; f \in F\}$ and which requires $O(|F| \cdot |Y|)$ time.

Proof of Theorem 1. Clearly, in $O(|Q| \cdot |X|)$ time we can find $\cap \{\operatorname{Ker} f_x; x \in X\}$, $|\cup \{\operatorname{Im} f_x; x \in X\}|$ and for every $x \in X$, $|\operatorname{Im} f_x|$, $|\operatorname{Im} f_x^2|$.

a) By Lemma 3b) it suffices to decide whether there exists $x \in X$ such that $\operatorname{Ker} f_x = \cap \{\operatorname{Ker} f_y; y \in X\}$ and $|\operatorname{Im} f_x| = |\operatorname{Im} f_x^2|$. Obviously, the inspection of this property requires $O(|Q| \cdot |X|)$ time.

b) By Lemma 3a) it suffices to decide whether there exists $x \in X$ such that $|\operatorname{Im} f_x| = |\operatorname{Im} f_x^2| = |\cup \{\operatorname{Im} f_y; y \in X\}|$. Again, the inspection of this property requires $O(|Q| \cdot |X|)$ time.

c) Since $S(A)$ has an identity iff $S(A)$ has both a left and a right identity we have that c) follows from b) and a).

f) By Lemma 4b) it suffices to decide whether for every $x \in X$ we have $\operatorname{Ker} f_x = \cap \{\operatorname{Ker} f_y; y \in X\}$ and $|\operatorname{Im} f_x| = |\operatorname{Im} f_x^2|$. This requires $O(|Q| \cdot |X|)$ time.

g) By Lemma 4a) it suffices to decide whether for every $x \in X$ we have $|\operatorname{Im} f_x| = |\operatorname{Im} f_x^2| = |\cup \{\operatorname{Im} f_y; y \in X\}|$. This requires $O(|Q| \cdot |X|)$ time.

h) A semigroup is a group iff it is both a left and a right group. Thus h) follows from f) and g).

d) A semigroup is left-zero iff it is a left group and each element is an idempotent. Hence $S(A)$ is a left-zero semigroup iff $S(A)$ is a left group and f_x is an idempotent for every $x \in X$. The inspection of the second condition requires $O(|Q| \cdot |X|)$ time and thus d) follows from f).

e) A semigroup is rigth-zero iff it is a right group and each element is an idempotent. Thus $S(A)$ is a right-zero semigroup iff $S(A)$ is a right group and for every $x \in X$, f_x is an idempotent. Hence e) follows from d) and g).

i) Clearly, any $f \in S(A)$ is a bijection iff f_x is a bijection for every $x \in X$. By finiteness of Q, f_x is a bijection iff $|\operatorname{Im} f_x| = |Q|$. The inspection of this condition requires $O(|X| \cdot |Q|)$ time. □

A point $y \in Y$ is a *distinguishing element* of a transformation semigroup F on Y if for every pair f, g of different mappings in F we have $f(y) \neq g(y)$. Clearly:

Proposition 6. An automaton A is quasi-state independent if and only if $S(A)$ has a distinguishing element. An automaton A is state independent if and only if every element of $S(A)$ is distinguishing.

The following easy lemma shows the basic scheme of the algorithms in Theorem 2.

Lemma 7. Let F be a transformation semigroup on a set Y. Then for every $y \in Y$, $|\{f(y); f \in F\}| \leqq |F|$ and y is distinguishing if and only if the equality holds.

Proof. Clearly, $\varphi: F \to \{f(y); f \in F\}$ such that $\varphi(f) = f(y)$ is an onto mapping, thus $|F| \geqq |\{f(y); f \in F\}|$ and φ is a bijection iff y is distinguishing. Hence the second statement is proved. □

To prove Theorem 2 it suffices to solve by Proposition 6 the following tasks:
Let F be a set of transformation of a set Y to itself.

a) does the transformation semigroup $\hat{F}$ generated by F have a distinguishing element?

b) is every point of Y distinguishing in the transformation semigroup on the set Y generated by F?

Lemma 7 offers us an idea for a solution of the tasks. The task a) can be solved by the following scheme:

1. Find a point y such that the set $\{f(y); f \in \hat{F}\}$ has the greatest number of points;
2. Decide whether y is distinguishing.

By Lemma 7, if $\hat{F}$ has a distinguishing element then necessarily y is distinguishing. The task b) can be solved by the following scheme:

1. Decide whether for every pair x, y of points of Y the following equality $|\{f(y); f \in \hat{F}\}| = |\{f(x); f \in \hat{F}\}|$ holds. If for some pair the equality does not hold then there exists an element of Y which is not distinguishing;
2. Choose a point $y \in Y$ and decide whether y is distinguishing. If the answer is yes, then any point of Y is distinguishing.

Again both statements follow from Lemma 7.

To solve the first step in both algorithms it suffices to determine $|\{f(x); f \in \hat{F}\}|$ for every $x \in Y$. Consider a directed graph (Y, R) where $R = \{(x, f(x)); x \in Y, f \in F\}$, then clearly it holds:

$$\{f(x); f \in \hat{F}\} = \{y;\ \text{there exists a directed path from } x \text{ to } y \text{ in } (Y, R)\}\ .$$

Now, by an easy modification of Tarjan's algorithm for constructing strongly connected components of a directed graph – see [1] or [4] – we obtain (let us remark that $|R| \leqq |F| \cdot |Y|$):

Lemma 8. There exists an algorithm which for a given set F of mappings from a set Y to itself and for a given element $y \in Y$ computes $|\{f(y); f \in \hat{F}\}|$, where $\hat{F}$ is the transformation semigroup generated by F, and which requires $O(|F| \cdot |Y|)$ time.

Thus we have

Corollary 9. A solution of the step 1 in both tasks requires $O(|F| \cdot |Y|^2)$ time.

We describe a procedure which for a given set F of mappings from a set Y to itself and for an element $y \in Y$ decides whether y is a distinguishing element of the transformation semigroup $\hat{F}$ generated by F.

We shall use two auxiliary subsets of Y – the set O of old points, the set W of working points – with $W \cap O = \emptyset$. Moreover, for every $x \in W \cup O$ a mapping $g_x \in \hat{F}$ with $g_x(y) = x$ is constructed.

Procedure DIST ELEM

1) Set $O \leftarrow \emptyset$, $W \leftarrow \{y\}$, $g_y = id_y$
2) **while** $W \neq \emptyset$ **do**
   choose $z \in W$, remove z from W and add z to O
   for every $f \in F$ **do**
   if $f(z) \notin W \cup O$ **then**
      set $g_{f(z)} = f \circ g_z$ and add $f(z)$ to W
      else check whether $g_{f(z)} = f \circ g_z$, **if** the equality does not hold **then** y is not distinguishing element;
3) **if** we have not obtained that y is not distinguishing element
   then y is distinguishing element.

We have to show the correctness of this procedure and to estimate time needed for the procedure.

If the procedure gives the answer "y is not distinguishing" then there exist $g_{f(z)}$, $f \circ g_z \in \hat{F}$ for some $f \in F$, $z \in Y$ such that $g_{f(z)}(y) = f(z) = f \circ g_z(y)$ and $g_{f(z)} \neq f \circ g_z$ — thus the answer is correct. On the other hand, assume that the answer is "y is distinguishing". Then for every $f \in \hat{F}$ we prove that after the end of the procedure $f(y) \in O$ and $f = g_{f(y)}$. Since $f \in \hat{F}$ there exist $f_1, f_2, \ldots, f_n \in F$ with $f = f_1 \circ f_2 \circ \ldots \circ f_n$. We prove by induction over i that for $\hat{f}_i = f_i \circ f_{i+1} \circ \ldots \circ f_n$ we have $\hat{f}_i(y) \in O$ and $\hat{f}_i = g_{f_i(y)}$. Indeed, $y \in O$ and thus in some time it held: $f_n(y) \in W$ and $g_{f_n(y)} = f_n$. Since after the end of the procedure $W = \emptyset$ we have that $f_n(y) \in O$. Assume that the assertion holds for some i, then $\hat{f}_{i-1} = f_{i-1} \circ \hat{f}_i$ and since in some time $\hat{f}_i(y) \in O$ necessary in this time $\hat{f}_{i-1}(y) \in O \cup W$ and $\hat{f}_{i-1} = f_{i-1} \circ \hat{f}_i = g_{\hat{f}_{i-1}(y)}$. Since after the procedure $W = \emptyset$ we obtain $\hat{f}_{i-1}(y) \in O$. Since $f = \hat{f}_1$ the proof is complete and hence the answer "y is distinguishing" is correct.

To estimate the time needed for the procedure we remark that the outer cycle in the step 2 repeats for every $z \in Y$ at most once. Analogously the inner cycle (**for every** $f \in F$ **do**) repeats at most once for every $z \in Y$ and $f \in F$. The main command in the step 2 (**if** ... **then** ... **else** ...) requires $O(|Y|)$ time. Hence the procedure requires $O(Y|^2 \cdot |F|)$ time.

If we summarize these facts we obtain:

Proposition 10. There is an algorithm which for a given set F of mappings from a set Y to itself decides whether the transformation semigroup generated by F has a distinguishing element (or every element of Y is distinguishing) and which requires $O(|F| \cdot |Y|^2)$ time.

Theorem 2 is a consequence of Propositions 6 and 10.

(Received July 11, 1984.)

REFERENCES

[1] A. V. Aho, J. E. Hopcroft and J. D. Ullman: The Design and Analysis of Computer Algorithms. Addison-Wesley, Reading, Mass. 1974.

[2] A. H. Clifford and G. B. Preston: The Algebraic Theory of Semigroups. AMS Providence, Rhode Island 1967.

[3] M. Demlová, J. Demel and V. Koubek: On subdirectly irreducible automata. RAIRO — Inform. Théor. *15* (1981), 23—46.

[4] R. E. Tarjan: Depth first search and linear graph algorithms. SIAM J. Comput. *1* (1971), 146—160.

[5] T. Watanabe and A. Nakamura: On the transformation semigroups of finite automata. J. Comp. System Sci. *26* (1983), 107—138.

[6] T. Watanabe and S. Noguchi: The amalgamation of automata. J. Comp. System Sci. *15* (1977), 1—16.

[7] T. Watanabe and S. Noguchi: Quasi-state independent automata. I.E.C.E. Japan. Trans. *60-D* (1977), 177—179.

RNDr. Marie Demlová, CSc., katedra matematiky elektrotechnické fakulty ČVUT (Department of Mathematics, Faculty of Electrical Engineering — Czech Technical University), Suchbatárova 2, 166 27 Praha 6. Czechoslovakia.

RNDr. Václav Koubek, CSc., Výpočetní centrum Karlovy University (Computing Centre of Charles University), Malostranské nám, 25, 118 00 Praha 1. Czechoslovakia.