Gabriel Thierrin
Simple automata

Kybernetika, Vol. 6 (1970), No. 5, (343)--350

Persistent URL: http://dml.cz/dmlcz/125755

KYBERNETIKA ČÍSLO 5, ROČNÍK 6/1970

Simple Automata

GABRIEL THIERRIN

In a recent article Barnes [1] introduced the notion of full subautomaton. We show that a subset of the set of states of an automaton $\mathscr{A}$ is the set of states of a full subautomaton of $\mathscr{A}$ if and only if it is a class of a congruence of $\mathscr{A}$. An automaton with only trivial subautomata is called simple. Every minimal full subautomaton of an automaton is a simple automaton. To every maximal congruence of an automaton is associated a simple automaton. Some characteristic properties of an automaton are given in this paper. For example, an automaton is simple if and only if it has only trivial congruences. If the group of automorphisms of a simple automaton has more than one element, then the automaton is a permutation automaton and the order of the group is a prime number which is equal to the number of states of the automaton.

DEFINITIONS AND PRELIMINARY RESULTS

Definition 1. An *automaton* is a triple $\mathscr{A} = (S, I, M)$ where

(1) S is a nonempty finite set (the set of states);
(2) I is a monoid, that is a semigroup possessing a unit element e (the monoid of inputs);
(3) M is a function (the next state function) mapping $S \times I$ into S such that

$$M(M(s, x)\, y) = M(s, xy) \quad \text{and} \quad M(s, e) = s$$

for all $x, y \in I$ and $s \in S$.

Definition 2. Let $\mathscr{A} = (S, I, M)$ be an automaton. A *subautomaton* of the automaton $\mathscr{A}$ is a triple $\mathscr{A}' = (S', I', M')$ where

(1) S' is a nonempty subset of S;
(2) I' is a submonoid of I such that $e \in I'$;
(3) for all $s \in S'$ and all $x \in I'$, we have $M(s, x) \in S'$;
(4) M' is the restriction of M to $S' \times I'$.

Definition 3. Let $\mathscr{A} = (S, I, M)$ be an automaton. A subautomaton $\mathscr{B} = (S', I', M')$ with the property that if $x \in I$ and $M(s, x) \in S'$ for at least one $s \in S'$ then $x \in I'$, is called a *full subautomaton* (Barnes [1]).

Definition 4. Let $\mathscr{A} = (S, I, M)$ be an automaton. Every equivalence relation R on S, such that $s \equiv t(R)$ implies that $M(s, x) \equiv M(t, x)$ for all $x \in I$, is called a *congruence* of $\mathscr{A}$.

Let $\bar{S}$ be the set of all classes of a congruence R of the automaton $\mathscr{A} = (S, I, M)$. For every $\bar{s} \in \bar{S}$ ($\bar{s}$ being the class of $s \in S$) and for every $x \in I$, let us define $\overline{M}(\bar{s}, x) = \overline{M(s, x)}$. We obtain then an automaton $\overline{\mathscr{A}} = (\bar{S}, I, \overline{M})$ which is called the *quotient automaton* of $\mathscr{A}$ by R. We write $\overline{\mathscr{A}} = \mathscr{A}/R$.

Let H be a subset of the set of states S of the automaton $\mathscr{A} = (S, I, M)$. For every $s \in S$, let $H : s = \{x \mid x \in I, M(s, x) \in H\}$. We define $s \equiv t(R_H)$ if and only if $H : s = H : t$. We see easily that R_H is a congruence of $\mathscr{A}$. If R is a congruence of $\mathscr{A}$ and if H is a class of R, then H is also a class of R_H and $R \subseteq R_H$, that is $s \equiv t(R)$ implies that $s \equiv t(R_H)$.

Proposition 1. *A nonempty subset H of S is a class of a congruence of the automaton $\mathscr{A} = (S, I, M)$ if and only if $M(H, x) \cap H \neq \emptyset$ implies that $M(H, x) \subseteq H$, where $M(H, x) = \{M(h, x) \mid h \in H\}$.*

Proof. It is obvious that the condition is necessary. In order to show that it is sufficient, we shall prove that H is a class of the congruence R_H. Let $s_1, s_2 \in H$ and $x \in H : s_1$. Then $M(s_1, x) \in H$ and $M(H, x) \cap H \neq \emptyset$. Hence $M(H, x) \subseteq H$, $x \in H : s_2$ and $H : s_1 \subseteq H : s_2$. By symmetry, we have $H : s_2 \subseteq H : s_1$. Therefore $H : s_1 = H : s_2$ and $s_1 \equiv s_2(R_H)$. Let $s_1 \equiv t(R_H)$. Then, from $e \in H : s_1$ and $H : s_1 = H : t$, it follows that $t \in H$. Therefore H is a class of R_H.

Proposition 2. *Let $\mathscr{A} = (S, I, M)$ be an automaton. A nonempty subset S' of S is the set of states of a full subautomaton $\mathscr{A}' = (S', I', M')$ of $\mathscr{A}$ if and only if S' is a class of a congruence R of $\mathscr{A}$.*

Proof. Let $\mathscr{A}' = (S', I', M')$ be a full subautomaton of $\mathscr{A}$ and let $M(S', x) \cap S' \neq \emptyset$. Then there exists $s \in S'$ such that $M(s, x) \in S'$. This implies that $x \in I'$ and $M(S', x) \subseteq S'$. Hence, by Proposition 1, S' is a class of a congruence of $\mathscr{A}$.

Let S' be a class of a congruence R of $\mathscr{A}$. Let $I' = \{x \mid x \in I, M(S', x) \subseteq S'\}$. This set I' is a submonoid of I and $e \in I'$. The automaton $\mathscr{A}' = (S', I', M')$ is a full subautomaton of $\mathscr{A}$. Indeed, if $M(s, x) \in S'$ with $s \in S'$, then $M(S', x) \cap S' \neq \emptyset$ and, by Proposition 1, $M(S', x) \subseteq S'$. Therefore $x \in I'$.

MINIMAL FULL SUBAUTOMATA

If E is a finite set, the number of elements in E is denoted by $|E|$.

Definition 5. A full subautomaton $\mathscr{A}' = (S', I', M')$ of the automaton $\mathscr{A} = (S, I, M)$ is said to be *minimal* if

(1) $|S'| > 1$,

(2) for every full subautomaton $A'' = (S'', I'', M'')$ of $\mathscr{A}$ such that $S'' \subset S'$, we have $|S''| = 1$.

Every automaton $\mathscr{A}$ such that $|S| > 1$ contains at least one minimal full subautomaton.

Proposition 3. *A full subautomaton $\mathscr{A}' = (S', I', M')$ with $|S'| > 1$ of the automaton $\mathscr{A} = (S, I, M)$ is minimal if and only if for every nonempty subset T of S', $T \neq S'$ the equality $T : s_1 = T : s_2$ with $s_1, s_2 \in S'$ implies that $s_1 = s_2$.*

Proof. The condition is necessary. Let $T : s_1 = T : s_2$ with $s_1, s_2 \in S'$ and let us suppose that $s_1 \neq s_2$. We have $s_1 \equiv s_2(R_T)$, and by Proposition 2, S' is a class of a congruence R of $\mathscr{A}$. The intersection $R_1 = R_T \cap R$ is a congruence of $\mathscr{A}$ and we have $s_1 \equiv s_2(R_1)$. Let S_1 be the class of the congruence R_1 containing s_1 and s_2. By Proposition 2, there exists a full subautomaton $\mathscr{A}_1 = (S_1, I_1, M_1)$ of $\mathscr{A}$ such that S_1 is the set of states of $\mathscr{A}_1$. Since $|S_1| > 1$ and $S_1 \subseteq S'$, we have because of the minimality of $\mathscr{A}'$, $S_1 = S'$ and $T : s_1 = T : s_i$ for all $s_i \in S'$. Since $T \neq S'$, there exists $s \in S'$ such that $s \notin T$. If $t \in T$, then $e \in T : t = T : s$ and $M(s, e) = s \in T$ which is a contradiction.

The condition is sufficient. Let $\mathscr{A}_1 = (S_1, I_1, M_1)$ be a full subautomaton of $\mathscr{A}$ such that $S_1 \subset S'$ and let us suppose that $|S_1| > 1$. Then S_1 is a class of the congruence R_{S_1}. Hence $S_1 : s_1 = S_1 : s_2$ for every pair $s_1, s_2 \in S_1$, which is a contradiction.

Proposition 4. *Let $\mathscr{A} = (S, I, M)$ be an automaton and let S' be a subset of S such that $|S'| > 1$. The set S' is the set of states of a minimal full subautomaton of $\mathscr{A}$ if and only if*

(1) *There exists $s_1, s_2 \in S'$, $s_1 \neq s_2$, such that $S' : s_1 = S' : s_2$.*

(2) *For every nonempty subset T of S', $T \neq S'$, the equality $T : s_i = T : s_j$, with $s_i, s_j \in S'$, implies that $s_i = s_j$.*

Proof. The condition is necessary. This follows immediately from Proposition 2 and 3.

The condition is sufficient. We have only to show that S' is a class of the congruence $R_{S'}$. Let S_1 be the class of $R_{S'}$ containing s_1. Then $s_2 \in S_1$ and it is obvious that $S_1 \subseteq S'$. If $S_1 \neq S'$, then $S_1 : s_1 = S_1 : s_2$ implies that $s_1 = s_2$, which is a contradiction. Hence $S_1 = S'$.

Proposition 5. *Let $\mathscr{A}' = (S', I', M')$ be a minimal full subautomaton of the automaton $\mathscr{A} = (S, I, M)$. For every $s' \in S'$, we have either $M'(s', I') = S'$ or $|M'(s', I')| = 1$.*

Proof. Let $M'(s', I') \neq S'$. Then $\mathscr{A}'' = (S'', I'', M'')$, with $S'' = M'(s', I')$ and $I'' = I'$, is a full subautomaton of $\mathscr{A}$. Since $S'' \subset S'$ and $\mathscr{A}'$ is minimal, we have $|S''| = |M'(s', I')| = 1$.

Let us remark that the condition $|M'(S', I')| = 1$ is equivalent to the condition $M(s', I') = s'$, since $e \in I'$ and $M(s', e) = s'$.

SIMPLE AUTOMATA

Definition 6. An automaton $\mathscr{A} = (S, I, M)$ is called *simple* if for every full subautomaton $\mathscr{A}' = (S', I', M')$ of $\mathscr{A}$ we have $S' = S$ or $|S'| = 1$.

In other words, an automaton $\mathscr{A}$ is simple if the only full subautomata of $\mathscr{A}$ are the subautomaton $\mathscr{A} = (S, I, M)$ and the full subautomata with only one state.

Every automaton $\mathscr{A} = (S, I, M)$ such that $|S| \leqq 2$ is simple.

Definition 7. A nonempty subset H of the set of states S of the automaton $\mathscr{A} = (S, I, M)$ is called *disjunctive* if the equality $H : s_i = H : s_j$ with $s_i, s_j \in S$ implies that $s_i = s_j$.

Proposition 6. *Let $\mathscr{A} = (S, I, M)$ be an automaton. Then the following three conditions are equivalent:*

(1) *$\mathscr{A}$ is simple.*

(2) *Every congruence of $\mathscr{A}$ is trivial, that is R is the equality or R has only one class.*

(3) *Every nonempty subset H of S, $H \neq S$, is disjunctive.*

Proof. (1) implies (2). This follows immediately from Proposition 2.

(2) implies (3). Let us suppose that there exists a nonempty subset H of S such that $H \neq S$ and $H : s_i = H : s_j$ with $s_i \neq s_j$. Then the congruence R_H is not the equality. Let $u \in H$ and $v \notin H$. Since $e \in H : u$ and $e \notin H : v$, we have $H : u \neq H : v$. Therefore, S is not a class of R_H and R_H is a non trivial congruence of $\mathscr{A}$, which is a contradiction.

(3) implies (1). Let $A' = (S', I', M')$ be a full subautomaton of $\mathscr{A}$ such that $|S'| > 1$. Since every non empty subset H of S, $H \neq 0$, is disjunctive, then $\mathscr{A}$ is, by Proposition 3, a minimal full subautomaton of $\mathscr{A}$. Therefore $S' = S$ and $\mathscr{A}$ is simple.

Definition 8. A congruence R of the automaton $\mathscr{A} = (S, I, M)$ is called *maximal* if:

(1) S is not a class of R.

(2) If R' is a congruence of $\mathscr{A}$ such that $R \subset R'$, then S is a class of R'.

Proposition 7. *Let $\mathscr{A} = (S, I, M)$ be an automaton. Then*

(1) *Every minimal full subautomaton $\mathscr{A}' = (S', I', M')$ of $\mathscr{A}$ is a simple automaton.*

(2) *If R is a maximal congruence of $\mathscr{A}$, the quotient automaton $\mathscr{A}/R$ is a simple automaton.*

Proof. (1) Let $\mathscr{A}'' = (S'', I'', M'')$ be a full subautomaton of $\mathscr{A}'$. It is obvious that $\mathscr{A}''$ is also a full subautomaton of $\mathscr{A}$. Since $\mathscr{A}'$ is minimal, we have $S'' = S'$ or $|S''| = 1$ and $\mathscr{A}'$ is simple.

(2) It is obvious that every congruence of $\mathscr{A}/R$ is trivial. Hence, by Proposition 6, $\mathscr{A}/R$ is simple.

Definition 9. An automaton $\mathscr{A} = (S, I, M)$ is called *strongly connected* if for any pair of states $s_i, s_j \in S$, there exists an $x \in I$ such that $M(s_i, x) = s_j$.

Let us remark that every full subautomaton of a strongly connected automaton is also strongly connected.

Definition 10. An automaton $\mathscr{A} = (S, I, M)$ is called *pseudo-strongly connected* if

(1) $|S| > 1$.

(2) S has a null state s_0, that is a state s_0 such that $M(s_0, x) = s_0$ for all $x \in I$.

(3) For any pair $s_i, s_j \in S$, $s_i \neq s_0$, there exists an $x \in I$ such that $M(s_i, x) = s_j$.

Proposition 8. *Every simple automaton $\mathscr{A} = (S, I, M)$ such that $|S| > 2$ is either strongly connected or pseudo-strongly connected.*

Proof. Let us suppose that $\mathscr{A}$ is not strongly connected. Then there exists at least one state s_0 such that $M(s_0, I) \neq S$. The subautomaton $\mathscr{A}' = (S', I', M')$ where $S' = M(s_0, I)$ and $I' = I$, is a full subautomaton of $\mathscr{A}$. Since $S' \neq S$, we have $|S'| = 1$ and $M(s_0, I) = s_0$. Hence s_0 is a null state of S. If s_0' is a null state of S, $s_0' \neq s_0$, then $\mathscr{A}'' = (S'', I'', M'')$, where $S'' = \{s_0, s_0'\}$ and $I'' = I$, is a full subautomaton of $\mathscr{A}$. But this is impossible, since $|S| > 2$ and $\mathscr{A}$ is simple. Therefore for every state $s \neq s_0$, we have $M(s, I) = S$ and $\mathscr{A}$ is pseudo-strongly connected.

Let S be a nonempty finite set and let I be a semigroup of mappings of S into S acting on the right of S, that is for every $s \in S$ and every $a \in I$, $(s)a$ is the image of s by the mapping a. If the identity mapping belongs to I, then the triple $\mathscr{A} = (S, I, M)$ where $M(s, a) = (s)a$ is an automaton. If I is the set of all mappings of S into S, then $\mathscr{A} = (S, I, M)$ is a simple automaton which is strongly connected. If $|S| > 1$, if s_0 is a fixed element of S and if I is the set of all mappings of S into S such that $(s_0)\, a = s_0$, then $\mathscr{A} = (S, I, M)$ is a simple automaton which is pseudo-strongly connected and which has null state s_0.

Remark. The automaton $\mathscr{A} = (S = \{1, 2\}, I = \{a\}, M(1, a) = M(2, a) = 1)$ shows that Proposition 8 is false if $|S| = 2$.

Definition 11. Let $\mathscr{A} = (S, I, M)$ be an automaton and let α be a one-to-one mapping of S onto S. The mapping α is an *automorphism* of $\mathscr{A}$ if $\alpha(M(s, x)) = M(\alpha(s), x)$ for all $s \in S$ and $x \in I$.

The set $G(\mathscr{A})$ of all automorphisms of an automaton forms a group. If $\mathscr{A}$ is strongly connected and if α is an automorphism such that $\alpha(s_i) = s_i$ for some $s_i \in S$ then α is the identity mapping (Fleck [2]). This implies that the order of $G(\mathscr{A})$ divides the number of states in S (Weeg [4]).

Proposition 9. *Let $\mathscr{A} = (S, I, M)$ be a simple automaton and $G(\mathscr{A})$ be the group of automorphisms of $\mathscr{A}$. If $|G(\mathscr{A})| > 1$, then $|G(\mathscr{A})|$ is a prime number and $|G(\mathscr{A})| = |S|$. Furthermore, $\mathscr{A}$ is a permutation automaton, that is the equality $M(s_i, a) = M(s_j, a)$ implies that $s_i = s_j$.*

Proof. From $|G(\mathscr{A})| > 1$, it follows that $|S| > 1$. First, we shall consider the case where $|S| = 2$. Obviously $|G(\mathscr{A})| = |S| = 2$. Let us suppose that $\mathscr{A}$ is not a permutation automaton. Then there exists $s_0 \in S$ and $a \in I$ such that $M(S, a) = s_0$. Let $S = \{s_0, s_1\}$. Since $|G(\mathscr{A})| = 2$, there exists $\alpha \in G(\mathscr{A})$ such that $\alpha(s_0) = s_1$ and $\alpha(s_1) = s_0$. Hence $s_0 = M(s_0, a) = M(\alpha(s_1), a) = \alpha(M(s_1, a)) = \alpha(s_0) = s_1$, which is a contradiction.

Let us suppose now that $|S| > 2$. Let K be a subgroup of $G(\mathscr{A})$ and, for every $s \in S$, let $K(s) = \{\alpha(s) \mid \alpha \in K\}$. The triple $\mathscr{A}' = (S', I', M')$ where $S' = K(s)$ and $I' = \{x \mid x \in I, M(S', x) \subseteq S'\}$ is a full subautomaton of $\mathscr{A}$. Indeed, let $M(t, x) \in S'$ with $t \in S'$. There exists $\alpha \in K$ such that $t = \alpha(s)$ and $M(t, x) = M(\alpha(s), x) = \alpha(M(s, x))$. Since $\alpha(M(s, x)) \in S'$, there exists $\beta \in K$ such that $\alpha(M(s, x)) = \beta(s)$. Since K is a group, we have $M(s, x) = \alpha^{-1}\beta(s)$. If $\delta \in K$, then $M(\delta(s), x) = \delta(M(s, x)) = \delta\alpha^{-1}\beta(s) \in K(s) = S'$. Therefore $M(S', x) \subseteq S'$ and $x \in I'$.

Since the automaton $\mathscr{A}$ is simple, for every $s \in S$ and for every subgroup K of $G(\mathscr{A})$ we have either $|K(s)| = 1$ or $K(s) = S$.

Let s be a state of $\mathscr{A}$ such that $M(s, I) = S$. Since $|S| > 2$, such a state exists by Proposition 8. Let $\alpha \in G(\mathscr{A})$ such that $\alpha(s) = s$. Then α is the identity mapping. Indeed, for every $t \in S$ there exists $a \in I$ such that $M(s, a) = t$ and $\alpha(t) = \alpha(M(s, a)) = M(\alpha(s), a) = M(s, a) = t$. Let $\alpha, \beta \in G(\mathscr{A})$, $\alpha \neq \beta$. Then $\alpha(s) \neq \beta(s)$. Indeed, if $\alpha(s) = \beta(s)$, then $\alpha^{-1}\beta(s) = s$ and $\alpha^{-1}\beta$ is the identity mapping. Hence $\alpha = \beta$ which is a contradiction. Let K be a subgroup of $G(\mathscr{A})$ such that $|K| > 1$. Then $|K(s)| = |S| = |K|$. Therefore $|G(A)| = |S|$ and $G(A)$ has only trivial subgroups. If follows then that the order of $G(A)$ is a prime number.

Finally, let us show that A is a permutation automaton. Let us suppose the contrary. Then there exist $s, t \in S$, $s \neq t$, and $a \in I$ such that $M(s, a) = M(t, a)$. By Proposition 8, for at least one of the states s and t, let s for example, we have $M(s, I) = S$ and then $G(\mathscr{A})(s) = S$. Therefore, there exists an automorphism α such that $\alpha(s) = t$ and $M(t, a) = M(\alpha(s), a) = \alpha(M(s, a)) = \alpha(M(t, a))$. Let $u = M(t, a)$. There exists an

automorphism β such that $\beta(s) = u$. Then we have $\beta(s) = u = \alpha(u) = \alpha\beta(s)$. Since $M(s, I) = S$, this implies that $\beta = \alpha\beta$. Therefore, α is the identity mapping and $s = t$, which is a contradiction.

Examples. Let $\mathscr{A} = (S = \{1, 2, 3\}, I = \{a, b, c\}^*, M)$ where $\{a, b, c\}^*$ is the free monoid generated by the set $\{a, b, c\}$ and where M is defined by the following table:

	a	b	c
1	1	3	2
2	2	2	2
3	1	3	3

This automaton $\mathscr{A}$ is simple and its group of automorphisms has only one element.

Let $\mathscr{A} = (S = \{1, 2, 3\}, I = \{a\}, M)$ where M is defined by

	a
1	2
2	3
3	1

This automaton $\mathscr{A}$ is simple and its group of automorphisms is the group of order 3.

SIMPLE SEQUENTIAL MACHINES

Definition 12. A *sequential machine* is a quintuple $\mathscr{M} = (S, I, O, M, \lambda)$ where

(1) S is a finite nonempty set of states;
(2) I is a finite nonempty set of inputs;
(3) M is a function mapping $S \times I$ into S (the next state function);
(4) O is a finite nonempty set of outputs;
(5) λ is a function mapping $S \times I$ into O (the output function).

Let I^* be the set of all finite sequences of inputs, including the null sequence A. With the operation of concatenation, I^* is a monoid and the triple $\mathscr{A} = (S, I^*, M)$ becomes an automaton with the extension to I^* of the next state function M. Every congruence of the automaton $\mathscr{A}$ is said to be a congruence of the sequential machine $\mathscr{M}$. The congruences of a sequential machine $\mathscr{M}$ are an important tool in the theory of serial or parallel decompositions of $\mathscr{M}$ (see Hartmanis and Stearns [3]).

A sequential machine $\mathscr{M} = (S, I, O, M, \lambda)$ is said to be *simple* if the automaton $\mathscr{A} = (S, I^*, M)$ is simple.

Proposition 10. *A sequential machine $\mathscr{M}$ is simple if and only if $\mathscr{M}$ has no nontrivial serial decompositions of its state behavior.*

Proof. Following Hartmanis and Stearns [3], a sequential machine $\mathscr{M}$ has a nontrivial serial decomposition of its state behavior if and only if there exists a nontrivial

congruence of $\mathscr{M}$. The proposition is then an immediate consequence of this result and Proposition 6.

(Received June 23, 1969.)

REFERENCES

[1] Barnes, B.: Groups of automorphisms and sets of equivalence classes of input for automata. J. ACM *12* (Oct. 1965), 561—565.
[2] Fleck A. C.: Isomorphism groups of automata. J. ACM *9* (Oct. 1962), 469—476.
[3] Hartmanis, G., Stearns, R. E.: Algebraic structure theory of sequential machines. Prentice-Hall, Englewood Cliffs, N. J. 1966.
[4] Weeg, G. P.: The structure of an automaton and its operation-preserving transformation group. J. ACM *9* (July 1962), 345—349.

VÝTAH

Jednoduché automaty

GABRIEL THIERRIN

Barnes zavedl nedávno ve své práci [1] pojem úplného podautomatu. V této práci bude ukázáno, že podmnožina množiny stavů automatu $\mathscr{A}$ je množinou stavů úplného podautomatu $\mathscr{A}$ právě tehdy, když je třídou nějaké kongruence na $\mathscr{A}$. Jednoduchý automat je automat, který má pouze triviální podautomaty. Ke každé maximální kongruenci na automatu je asociován jednoduchý automat. Některé charakteristické vlastnosti jednoduchých automatů jsou popsány v této práci. Na příklad, automat je jednoduchý právě tehdy, když má jen triviální kongruence. Jestliže grupa automorfismů jednoduchého automatu má více než jeden prvek, pak tento automat je permutační automat a řád grupy je prvočíslo, které je rovno počtu stavů automatu.

Professor Gabriel Thierrin, Département d'informatique, Université de Montréal, Case Postale 6128, Montréal 101, Canada.