Permutation Automata

by

G. THIERRIN

Département d'Informatique
Université de Montréal

1. Introduction

An automaton ([2], [4]) is a quintuple $A = (S, I, \delta, s_0, F)$, where
(i) S is a finite nonempty set of states;
(ii) I is a finite nonempty set of inputs;
(iii) $\delta: S \times I \to S$ is called the transition function;
(iv) s_0 is an element of S (the initial state of A);
(v) F is a subset of S (the set of final states of A).

Let I^* be the set of all finite sequences of elements of I, including the null sequence Λ. Any element of I^* is called a tape. With the operation of concatenation, the set I^* becomes a semigroup, which is called the free semigroup (with identity Λ) generated by I. The transition function δ can be extended by recursion to $S \times I^*$.

The set $T(A) = \{x \mid x \in I^* \text{ and } \delta(s_0, x) \in F\}$ is called the set of tapes accepted by the automaton A. A subset of U of I^* is said to be a regular set if and only if there exists some automaton A such that $U = T(A)$.

An automaton A is said to be a permutation automaton, or simply a p-automaton, if and only if each input permutes the set of states. A subset U of I^* is said to be a p-regular set if and only if there exists a p-automaton A such that $U = T(A)$. It is the purpose of this paper to give some characterizations of p-regular sets and to determine some operations under which the family of p-regular sets is closed.

2. p-Automata and p-Regular Sets

Definition 2.1. An automaton $A = (S, I, \delta, s_0, F)$ is said to be a permutation automaton, or more simply a p-automaton, if and only if $\delta(s_i, a) = \delta(s_j, a)$, where $s_i, s_j \in S$, $a \in I$, implies that $s_i = s_j$.

It is obvious that the following three conditions are equivalent:
(i) A is a p-automaton;
(ii) $\delta(s_i, x) = \delta(s_j, x)$, where $x \in I^*$, implies that $s_i = s_j$;
(iii) For every $x \in I^*$, we have $\delta(S, x) = S$.

MATHEMATICAL SYSTEMS THEORY, Vol. 2, No. 1
Published by Springer-Verlag New York Inc.

Definition 2.2 An equivalence relation R on I^* is said to be right cancellative [left cancellative] if and only if $ac \equiv bc\ (R)$ [$ca \equiv cb\ (R)$] implies that $a \equiv b\ (R)$. If R is right and left cancellative, then R is said to be a cancellative equivalence relation.

Definition 2.3. Let U be a subset of I^*. We define:
(i) For every $a \in I^*$

$$U \mathbin{.\!\!\cdot}\ a = \{x \mid x \in I^* \text{ and } ax \in U\},$$

$$U \mathbin{\cdot\!\!.}\ a = \{x \mid x \in I^* \text{ and } xa \in U\};$$

(ii) $a \equiv b\ (R_U)$ if and only if $U \mathbin{.\!\!\cdot}\ a = U \mathbin{.\!\!\cdot}\ b$,
$a \equiv b\ ({}_UR)$ if and only if $U \mathbin{\cdot\!\!.}\ a = U \mathbin{\cdot\!\!.}\ b$.

It is easy to see that R_U is a right congruence and that ${}_UR$ is a left congruence. These congruences have been used to characterize the regular sets ([2], [4]). They were first discussed in the general theory of semigroups by Dubreil ([1]).

LEMMA 2.1. *Let R be a right congruence of finite index on I^* and let C be a right congruence on I^* such that $R \subseteq C$. If R is right cancellative, then C is also right cancellative.*

Proof. Let T be a right congruence on I^*. For every $c \in I^*$, let $T(c) = \{y \mid y \in I^*$ and there exists $x \in I^*$ such that $y \equiv xc\ (T)\}$. If T is right cancellative and if $a \not\equiv b\ (T)$, then $ac \not\equiv bc\ (T)$ for every $c \in I^*$. Therefore, a right congruence T of finite index is right cancellative if and only if $T(c) = I^*$ for every $c \in I^*$.

Since R is right cancellative, we have $R(c) = I^*$ for every $c \in I^*$. From $R \subseteq C$, it follows that $R(c) \subseteq C(c)$ and $C(c) = I^*$. Therefore C is right cancellative.

THEOREM 2.1. *Let U be a subset of I^*. Then the following three conditions are equivalent:*

(i) *U is a p-regular set;*

(ii) *U is the union of some classes of a right congruence on I^* of finite index, which is right cancellative.*

(iii) *The right congruence R_U on I^* is right cancellative and of finite index.*

Proof. (i) implies (ii). There exists a p-automaton $A = (S, I, \delta, s_0, F)$ such that $U = T(A)$. Let R be the equivalence relation defined on I^* by: $a \equiv b\ (R)$ if and only if $\delta(s_0, a) = \delta(s_0, b)$. It is known ([2], [4]) that U is the union of some classes of R. Let us show that R is right cancellative. If $ac \equiv bc\ (R)$, then $\delta(s_0, ac) = \delta(s_0, bc)$ and $\delta(\delta(s_0, a), c) = \delta(\delta(s_0, b), c)$. Since A is a p-automaton, we have $\delta(s_0, a) = \delta(s_0, b)$ and $a \equiv b\ (R)$.

(ii) implies (iii). Let $a \equiv b\ (R)$. If $x \in U \mathbin{.\!\!\cdot}\ a$, then $ax \in U$. But $ax \equiv bx\ (R)$. Hence $bx \in U$ and $U \mathbin{.\!\!\cdot}\ a \subseteq U \mathbin{.\!\!\cdot}\ b$. Similarly, $U \mathbin{.\!\!\cdot}\ b \subseteq U \mathbin{.\!\!\cdot}\ a$. Therefore $U \mathbin{.\!\!\cdot}\ a = U \mathbin{.\!\!\cdot}\ b$, $a \equiv b\ (R_U)$ and $R \subseteq R_U$. Since R is right cancellative and of finite index, it follows (Lemma 2.1) that R_U is right cancellative and of finite index.

(iii) implies (i). Let $S = \{[x] \mid x \in I^*\}$ be the set of classes of R_U. By hypothesis, S is finite. Let $s_0 = [\Lambda]$ and $F = \{[x] \mid x \in U\}$. Define $\delta([x], a) = [xa]$.

It is known ([2], [4]) that $A = (S, I, \delta, s_0, F)$ is an automaton such that $U = T(A)$. Let us prove that A is a p-automaton. If $\delta([x], a) = \delta([y], a)$, then

$$[xa] = [ya]$$
$$xa \equiv ya \ (R_U)$$
$$x \equiv y \ (R_U).$$

Hence $[x] = [y]$.

COROLLARY. *A regular set U is p-regular if and only if $U \therefore ac = U \therefore bc$ implies that $U \therefore a = U \therefore b$.*

The next result is a generalisation of part (ii) of the preceding theorem.

THEOREM 2.2. *A subset U of I^* is p-regular if and only if U is the union of some classes of an equivalence relation R of finite index on I^*, which is right cancellative.*

Proof. From the previous theorem, we see that the condition is necessary. In order to show that it is sufficient, we have only to prove that R is a right congruence. Suppose that R is not a right congruence. Then there exist $a, b, c \in I^*$ such that $a \equiv b \ (R)$ and $ac \not\equiv bc \ (R)$. Let $C = \{c_1, c_2, \cdots, c_n\}$ be a subset of I^* such that

(i) $b = c_1$;

(ii) $c_i \not\equiv c_j \ (R)$ for $i \neq j$;

(iii) For every $x \in I^*$, there exists $c_i \in C$ such that $x \equiv c_i \ (R)$.

Since R is of finite index, the set C is finite, and the number n of elements of C is equal to the index of R. Since R is right cancellative, we have

$$c_i c \not\equiv c_j c \ (R) \text{ for } i \neq j,$$

and each class of R contains an element of the form $c_i c$. Therefore there exists $c_i \in C$ such that $c_i c \equiv ac \ (R)$. Hence $c_i \equiv a \ (R)$. Since $a \equiv b \ (R)$, we have $b \equiv c_i \ (R)$ and $c_i = c_1 = b$. Therefore $bc \equiv ac \ (R)$, and we have a contradiction.

Definition 2.4. Let R be an equivalence relation on I^* and let $t \in I^*$. We define

$$a \equiv b \ (R \therefore t) \text{ if and only if } ta \equiv tb \ (R).$$

It is obvious that $R \therefore t$ is an equivalence relation.

THEOREM 2.3. *Let R be a right congruence on I^*. Then*

(i) *$R \therefore t$ is a right congruence.*

(iii) *If R is of finite index n, then $R \therefore t$ is also of finite index m and $m \leqslant n$. Furthermore,*

$$C = \bigcap_{t \in I^*} R \therefore t$$

is a congruence on I^* of finite index and $C \subseteq R$.

(iii) *If R is right cancellative, then $R \therefore t$ is also right cancellative.*

Proof. (i). Let $a \equiv b \ (R \therefore t)$. Then $ta \equiv tb \ (R)$, and, since R is a right congruence, $tax \equiv tbx$ (R) for all $x \in I^*$. Hence $ax \equiv bx$ $(R \therefore t)$.

(ii) Since R is of finite index n, there exists a finite set $A = \{a_1, a_2, \cdots, a_n\}$ of I^* such that (1) $a_i \not\equiv a_j$ (R) for $i \neq j$; (2) for every $c \in I^*$, there exists $a_i \in A$ such that $a_i \equiv c$ (R). Let $[tI^*] = \{x \mid x \in I^*$ and there exists $r \in I^*$ such that $tr \equiv x$ $(R)\}$. The subset $B = A \cap [tI^*]$ is nonempty. Let $B = \{b_1, b_2, \cdots, b_k\}$. Since $B \subseteq A$, we have $k \leqslant n$. For each $b_i \in B$, we can choose an element $r_i \in I^*$ such that $tr_i \equiv b_i$ (R). Let $T = \{r_1, r_2, \cdots, r_k\}$. For every $y \in I^*$, there exists $a_j \in A$ such that $ty \equiv a_j$ (R). Since $B = A \cap [tI^*]$, there exist $b_i \in B$ and $r_i \in T$ such that $a_j = b_i$ and $tr_i \equiv b_i$ (R). Therefore $ty \equiv tr_i$ (R) and $y \equiv r_i$ $(R \therefore t)$. This proves that $m \leqslant k \leqslant n$, where m is the index of $R \therefore t$.

It is obvious that C is a right congruence. Let us prove that C is a congruence and that $C \subseteq R$. Let $a \equiv b$ (C). Then for every $t \in I^*$, we have $a \equiv b$ $(R \therefore t)$ and $ta \equiv tb$ (R). If we take $t = \Lambda$ (the identity element of I^*), then $a \equiv b$ (R). Hence $C \subseteq R$.

Let $x \in I^*$. Then, for every $t \in I^*$,

$$txa \equiv txb \ (R),$$

$$xa \equiv xb \ (R \therefore t).$$

Hence $xa \equiv xb$ (C) and C is a congruence.

It remains to prove that C is of finite index. Let $D = \bigcap_{a_i \in A} R \therefore a_i$. Since A is finite and since $R \therefore a_i$ is of finite index, D is of finite index and $C \subseteq D$. Let $a \equiv b$ (D). If $t \in I^*$, then there exists $a_i \in A$ such that $t \equiv a_i$ (R). Since R is a right congruence, we have $ta \equiv a_ia$ (R) and $tb \equiv a_ib$ (R). But $a \equiv b$ $(R \therefore a_i)$ and $a_ia \equiv a_ib$ (R). Therefore $ta \equiv tb$ (R) and $a \equiv b$ $(R \therefore t)$. Since this is true for every t, we have $a \equiv b$ (C) and $D \subseteq C$. Hence $C = D$ and C is of finite index.

(iii) Let $ac \equiv bc$ $(R \therefore t)$. Then

$$tac \equiv tbc \ (R),$$

$$ta \equiv tb \ (R),$$

$$a \equiv b \ (R \therefore t).$$

Hence $R \therefore t$ is right cancellative.

THEOREM 2.4. *Let U be a subset of I^*. Then the following three conditions are equivalent.*

(i) *U is a p-regular set.*

(ii) *U is the union of some classes of a cancellative congruence of finite index on I^*.*

(iii) *U is the union of some classes of a congruence C on I^* such that the quotient semigroup I^*/C is a finite group.*

Proof. (i) implies (ii). The subset U is the union of some classes of a right congruence R of finite index, which is right cancellative (Theorem 2.1). Let $C = \bigcap_{t \in I^*} R \therefore t$. From Theorem 2.3 it follows that C is a congruence of finite index such that $C \subseteq R$. Hence U is the union of some classes of C. Since R is right cancellative, Theorem 2.3 shows that $R \mathrel{.\cdot} t$ is right cancellative for every $t \in I^*$. Therefore C is right cancellative.

Let $T = I^*/C$ be the quotient semigroup modulo C. The semigroup T is a finite and right cancellative semigroup with an identity element. It is well known that such a semigroup is a group. Since a group is right and left cancellative, it follows that C is a cancellative congruence of finite index.

(ii) implies (iii). This follows immediately from the previous results.

(iii) implies (i). Obvious.

COROLLARY 1. *If U is a p-regular set, then $U \mathrel{.\cdot} a$ and $U \mathrel{\cdot.} a$ are nonempty sets for every $a \in I^*$.*

COROLLARY 2. *A nonempty finite subset of I^* cannot be a p-regular set.*

Definition 2.5. An equivalence relation R on I^* is said to be right limitative ([5]) if and only if $ac \equiv bc \equiv a\ (R)$ implies that $a \equiv b\ (R)$.

Every right cancellative equivalence relation is obviously right limitative.

THEOREM 2.5. *A subset U of I^* is p-regular if and only if U is the union of some classes of a right congruence R of finite index on I^*, which is right limitative.*

Proof. The condition is necessary by Theorem 2.1. Let us show that it is also sufficient. Let $C = \bigcap_{t \in I^*} R \mathrel{.\cdot} t$. We know (Theorem 2.3) that C is a congruence of finite index and that $C \subseteq R$. Hence U is the union of some classes of C. If $ac \equiv bc \equiv a\ (R \mathrel{.\cdot} t)$, then

$$tac \equiv tbc \equiv ta\ (R)$$

$$ta \equiv tb\ (R)$$

$$a \equiv b\ (R \mathrel{.\cdot} t).$$

Hence $R \mathrel{.\cdot} t$ is right limitative for every $t \in I^*$. It is immediate that the intersection of right limitative equivalence relations is also right limitative. Therefore C is right limitative. The quotient semigroup $T = I^*/C$ is a finite semigroup with an identity element 1 such that $ac = bc = a$, where $a, b, c \in T$, implies that $a = b$. Let us show that T is a group. Let e be an idempotent element of T. We have

$$(1 \cdot e) \cdot e = 1 \cdot e = (1 \cdot e)$$

Hence $1 \cdot e = 1$ and $e = 1$. Since T is finite, then, for every $a \in T$, there exists a positive integer n such that $a^n = e$, where e is an idempotent element. But $e = 1$. Therefore, for every $a \in T$, there exists $x \in T$ such that $ax = 1$ and T is a group.

From Theorem 2.4, it follows that U is p-regular.

3. Equivalence of p-Automata

We recall the following result.

THEOREM 3.1. (Hartmanis-Stearns [3]). *Every p-automaton A is equivalent to a strongly connected p-automaton B.*

Proof. Let $U = T(A)$. Then U is a p-regular set and U is the union of some classes of a congruence C such that I^*/C is a finite group (Theorem 2.4). Let $S = \{[a_1], \cdots, [a_n]\}$ be the set of classes of C, where $[a_1]$ is the class containing Λ, and let F be the set of classes of C containing the elements of U. For every $a \in I$, define $\delta([a_i], a) = [a_i a]$. Then $B = (S, I, \delta, [a_1], F)$ becomes an automaton such that $U = T(B)$. Hence A is equivalent to B. Since I^*/C is a group, B is a p-automaton and, for every pair $[a_i]$, $[a_j]$, there exists $[a_k]$ such that $[a_i]\,[a_k] = [a_j]$. Therefore $\delta([a_i], a_k) = [a_j]$ and B is strongly connected.

THEOREM 3.2. *Every automaton $A = (S, I, \delta, s_0, F)$ such that $\delta(s_i, a) = \delta(s_j, a) = s_i$, where $a \in I^*$, implies that $s_i = s_j$ is equivalent to a strongly connected p-automaton.*

Proof. We have only to prove that $U = T(A)$ is a p-regular set. Define

$$a \equiv b\ (R) \text{ if and only if } \delta(s_0, a) = \delta(s_0, b).$$

Then R is a right congruence of finite index and U is the union of some classes of R. Let $ac \equiv bc \equiv a\ (R)$. Then

$$\delta(s_0, ac) = \delta(s_0, bc) = \delta(s_0, a)$$

$$\delta(\delta(s_0, a), c) = \delta(\delta(s_0, b), c) = \delta(s_0, a).$$

Hence $\delta(s_0, a) = \delta(s_0, b)$ and $a \equiv b\ (R)$. Therefore R is right limitative and U is p-regular (Theorem 2.5).

4. Operations on p-Regular Sets

THEOREM 4.1. *The family of p-regular sets of I^* is a Boolean algebra of sets.*

Proof. If U is p-regular, then the right congruence R_U is right cancellative (Theorem 2.1). If $\bar{U}$ is the complement of U, we have $R_U = R_{\bar{U}}$. Therefore, $\bar{U}$ is also p-regular (Theorem 2.1).

Let U_1 and U_2 be two p-regular sets. Then U_1 and U_2 are respectively the union of some classes of right congruences R_1 and R_2 of finite index which are right cancellative (Theorem 2.1). The intersection $R = R_1 \cap R_2$ is a right congruence of finite index and R is also right cancellative. It is obvious that $U_1 \cap U_2$ is the union of some classes of R. Therefore $U_1 \cap U_2$ is a p-regular set.

THEOREM 4.2. *If U is a p-regular set of I^*, then the transpose U^T of U is also a p-regular set.*

Proof. Recall that if $a = a_1 a_2 \cdots a_k$ is an element of I^*, where $a_1, a_2, \cdots, a_k \in I$, then the transpose a^T of a is the element $a^T = a_k \cdots a_2 a_1$.

The set U is the union of some classes of a cancellative congruence C of finite index on I^* (Theorem 2.4). Define

$$a \equiv b\ (C^T) \text{ if and only if } a^T \equiv b^T\ (C).$$

We see easily that C^T is a cancellative congruence of finite index on I^* and that $U^T = \{x^T \mid x \in U\}$ is the union of some classes of C^T. Therefore U^T is p-regular.

THEOREM 4.3. *If U is a p-regular set of I^* and if X is a subset of I^*, then the two sets*

$$U_1 = U/X = \{v \mid v \in I^* \text{ and } vX \cap U \neq \varnothing\}$$
$$U_2 = U\backslash X = \{w \mid w \in I^* \text{ and } Xw \cap U \neq \varnothing\}$$

are p-regular.

Proof. First we shall prove that $R_U \subseteq R_{U_1}$. Let $a \equiv b\ (R_U)$ and let $y \in U_1 \therefore a$. Then $ay \in U_1$ and there exists $x \in X$ such that $ayx \in U$. Hence $yx \in U \therefore a = U \therefore b$ and $byx \in U$. Therefore $by \in U_1, y \in U_1 \therefore b$ and $U_1 \therefore a \subseteq U_1 \therefore b$. Similarly, $U_1 \therefore b \subseteq U_1 \therefore a$. Therefore

$$U_1 \therefore a = U_1 \therefore b,$$
$$a \equiv b\ (R_{U_1}).$$

Since U is p-regular, R_U is a right congruence of finite index and R_U is right cancellative (Theorem 2.1). From $R_U \subseteq R_{U_1}$ and Lemma 2.1, it follows that R_{U_1} is of finite index and right cancellative. Therefore U_1 is p-regular.

We see easily that $U_2^T = U^T/X^T$. Since U is p-regular, U^T is p-regular. Therefore U_2^T is p-regular, and since $U_2 = (U_2^T)^T$, U_2 is also p-regular.

We shall show now that the family of p-regular sets of I^* is not closed under the operations of product and star.

Let $I = \{a\}$; then $I^* = \{a^n \mid n \geqslant 0\}$.

Let $U = \{a^{2n+1} \mid n \geqslant 0\}$. It is easy to see that R_U is a cancellative congruence of index 2 on I^*. Hence U is a p-regular set of I^*. The congruence R_{U^2} is not cancellative since

$$a^0 \cdot a^1 \equiv a^2 \cdot a^1\ (R_{U^2})$$

and

$$a^0 \not\equiv a^2\ (R_{U^2}).$$

Therefore, the product $U \cdot U = U^2 = \{a^{2n} \mid n > 0\}$ is not a p-regular set.

Let $U = \{a^{3n+2} \mid n \geqslant 0\}$. Then

$$U^* = \bigcup_{k=0}^{\infty} U^k = \{a^0\} \cup \{a^2\} \cup \{a^n \mid n \geqslant 4\}.$$

We see easily that R_U is a cancellative congruence of index 3 on I^*. Hence

U is p-regular. The congruence R_{U^*} is not cancellative, since

$$a^0 \cdot a^4 \equiv a^1 \cdot a^4 \ (R_{U^*})$$

and

$$a^0 \not\equiv a^1 \ (R_{U^*}).$$

Therefore U^* is not a p-regular set.

REFERENCES

[1] P. DUBREIL, Contribution à la théorie des demi-groupes. *Mém. Acad. Sci. Inst. France* (2) **63** (1941), no. 3, 1–52.
[2] S. GINSBURG, *An Introduction to Mathematical Machine Theory.* Addison-Wesley, Reading, Mass., 1962.
[3] G. HARTMANIS and R. E. STEARNS, *Algebraic Structure Theory of Sequential Machines.* Prentice-Hall, Englewood Cliffs, N. J., 1966.
[4] M. O. RABIN and D. SCOTT. Finite automata and their decision problems. *IBM J. Res. Develop.* **3** (1959), 114–125.
[5] G. THIERRIN, Sur la caractérisation des groupes par leurs équivalences régulières. *C.R. Acad. Sci. Paris* **238** (1954), 1954–1956.

(Received 14 September 1967)