ELSEVIER

Theoretical Computer Science 172 (1997) 273–279

Theoretical Computer Science

Note

Reset words for commutative and solvable automata

Igor Rystsov

Glushkov Institute of Cybernetics, Kiev, 252187, Ukraine

Received December 1995; revised April 1996
Communicated by A.A. Letichevsky

Abstract

A reset word takes all states of a finite automaton to a single state. In this paper, it is shown that the length of the shortest reset word for a solvable automaton with n states is at most $n-1$ and this bound is reachable.

1. Introduction

The results of this paper originated from the investigation of Cerny's hypothesis about the minimum length of reset words for a finite automaton [1]. Cerny supposed that this length for an n-state automaton is at most $(n-1)^2$ and showed that this bound is reachable [1]. This hypothesis has been proved for several special cases [2, 9]. The general upper bound $(n^3-n)/6$ has been obtained for arbitrary automaton with n states [5].

It is easy to see that the minimum length of reset words for a monogenic (one input) n-state automaton is at most $n-1$. In this paper, we prove that this bound is also valid for commutative, solvable and strongly reset automata.

2. Definitions and preliminaries

A finite deterministic automaton (without outputs) A is defined as a homomorphism of monoids:

$$A : X^* \to Map(S), \tag{1}$$

where X^* is the free monoid of words over a finite input alphabet X and $Map(S)$ is the multiplicative monoid of unary mappings on a finite set of states S. The number $n = |S|$ is the number of states of an automaton A.

PII S0304-3975(96)00136-3

Homomorphism (1) associates with a word $w = x_1 \dots x_m$ the composition (superposition) of mappings $A(w) = A_w = A(x_1) \cdot \dots \cdot A(x_m)$. The identical mapping is associated with the empty word. The submonoid $A(X^*)$ of $Map(S)$ is called the monoid of an automaton A and is denoted by $Mon(A)$.

The value $A_w(s)$ of the mapping A_w in the state $s \in S$ is denoted also by $A(s,w)$. The image of a subset of states $T \subseteq S$ under the action of a word w in A is defined by the formula

$$A(T,w) = \{A(s,w) \mid s \in T\}.$$

The number $r(w) = |A(S,w)|$ is called the rank of a word w with respect to A.

If $r(w) = 1$, then w is said to be a reset word for A. In this case $A(w)$ is a constant mapping. An automaton is called reset if there is a reset word for it. The following proposition is evident.

Proposition 2.1. *An automaton A is reset if and only if for every two states s,t there is a word w such that $A(s,w) = A(t,w)$.*

A state $s \in S$ is stable for A if $A(s,x) = s$ for all $x \in X$. A reset automaton with a stable state is called a 0-automaton. In this case there exists only stable state which is called the zero state 0. Note that the zero state is reachable from any other state.

The mapping Z such that $Z(s) = 0$ for all $s \in S$ is called the zero mapping for a 0-automaton. If w is a reset word for a 0-automaton A, then $A(w) = Z$ and $A(w)$ is an algebraic zero of the monoid $Mon(A)$. Therefore, reset words are called zero words for a 0-automaton. An automaton is monogenic (autonomous) if $|X| = 1$. The following proposition is obvious.

Proposition 2.2. *Any reset monogenic automaton is a 0-automaton, and there is a zero word of length at most $n-1$ for it.*

If we let $A(s_i,x) = s_{i+1}$ for all i, $1 \leqslant i < n$, and $A(s_n,x) = s_n$, then x^{n-1} will be the shortest zero word. Thus, the bound in Proposition 2.2 is tight.

A subset $T \subseteq S$ defines a subautomaton B of A if $A(T,x) \subseteq T$ for all $x \in X$. In this case it is supposed that $B(s,x) = A(s,x)$ for all $s \in T$ and $x \in X$. A subset T defines a proper subautomaton if $T \subset S$.

The factorautomaton A/B is defined for a subatomaton B of A on the factorset $S \setminus T \cup \{T\}$ in the usual way: $A/B(s,x) = A(s,x)$ if $A(s,x) \notin T$ and $A/B(s,x) = A/B(T,x) = T$ if $A(s,x) \in T$ for all $s \in S \setminus T$ and $x \in X$. Thus, the state $\{T\}$ is stable for the factorautomaton A/B. Note that any subautomaton and factorautomaton of a 0-automaton are also 0-automata.

Proposition 2.3. *If w is a zero word for a subautomaton B and v is a zero word for the factorautomaton A/B, then vw is a zero word for an automaton A.*

An automaton A is transitive (strongly connected) if for every pair of states s,t there is a word w such that $A(s,w) = t$. A 0-automaton is called 0-transitive if

each of its state is reachable from any nonzero state. The following proposition is evident.

Proposition 2.4. *An automaton* (0-*automaton*) *is transitive* (0-*transitive*) *if and only if there are no proper* (*nonzero*) *subautomata in it.*

Denote by $Cen(A)$ the submonoid of mappings in $Map(S)$ which commute with all mappings in $A(X) = \{A(x) \mid x \in X\}$. The submonoid $Cen(A)$ is called the centralizer of an automaton A. If $f \in Cen(A)$, then $f \cdot A(x) = A(x) \cdot f$ for all $x \in X$, and f is called an endomorphism of A. Note that the zero state of a 0-automaton A is a stable point for all endomorphisms in $Cen(A)$. Therefore, the zero mapping Z is an algebraic zero of the monoid $Cen(A)$. The next conjecture is the multiplicative analog of the well-known Shur's lemma from ring theory [6].

Lemma 2.5. *The centralizer of a transitive* (0-*transitive*) *automaton is a group* (*with zero*).

Proof. We sketch the proof only for 0-automata. Let A be a 0-transitive automaton and $f \in Cen(A)$. It is easy to see that the subset $f(S)$ of states defines a subautomaton of A. Then, by Proposition 2.4, we conclude that $f(S) = S$ or $f(S) = \{0\}$. In the first case f is a bijection, and in the second case f is the zero of $Cen(A)$. Thus, all nonzero mappings in $Cen(A)$ form a subgroup. □

3. Commutative automata

An automaton A is commutative if $A(x) \cdot A(y) = A(y) \cdot A(x)$ for all $x, y \in X$. Note that each subautomaton and factorautomaton of a commutative automaton are also commutative.

Theorem 3.1. *There is a zero symbol $x \in X$ for a commutative* 0-*transitive automaton A.*

Proof. We have $A(X) \subseteq Cen(A)$ for a commutative 0-automaton A. Then from Lemma 2.5 it follows that all nonzero mappings in $A(X)$ are permutations. Thus, there is the zero mapping in $A(X)$, since the zero state is reachable from other states. □

Now consider reset commutative automata. It is evident that any monogenic automaton is commutative. Therefore, the following theorem generalizes Proposition 2.2 [11, 4].

Theorem 3.2. *Any reset commutative automaton A is a* 0-*automaton, and there is a zero word of length at most $n - 1$ for it.*

Proof. We argue by induction on n. If $n = 1$, then the theorem is trivial. If $n > 1$, then there is a proper subautomaton of A. Indeed, otherwise by Proposition 2.4 and Lemma 2.5 an automaton A is transitive and $Cen(A)$ is a group of permutations. Since A is commutative, then $A(X) \subseteq Cen(A)$ and all mappings in $A(X)$ are permutations. Then by Proposition 2.1 A is not reset, and we have a contradiction.

Let B be a maximal proper subautomaton of A with the subset of states T. Then the factorautomaton A/B is 0-transitive. Indeed, for any two states $s, t \in S \setminus T$ there is a word v such that $A(s, v) = t$, and $A(s, w) \in T$ for a reset word w. Thus, by Theorem 3.1, there is a zero symbol x for A/B. By induction hypothesis, B is a 0-automaton, and there is a zero word w for B whose length is at most $n-2$. Hence, from Proposition 2.3 it follows that xw is a zero word for A of length at most $n-1$. □

The tightness of this bound follows from the tightness of the bound in Proposition 2.2.

4. Solvable 0-automata

In this section, we extend Theorem 3.2 to more general class of automata. A composite chain for a 0-automaton A is a series of subautomata:

$$\{0\} = B_0 \subset B_1 \subset \cdots \subset B_m = A, \tag{2}$$

in which all composite factors B_i/B_{i-1}, $1 \leqslant i \leqslant m$, are 0-transitive. It is well known that composite factors are isomorphic to the strongly connected components (layers) of a 0-automaton [7]. Therefore, two composite chains have isomorphic composite factors and the same length. In other words, the analog of Jordan–Helder's theorem from algebra [6] takes place for 0-automata. Thus, we may define the length $l(A)$ of a 0-automaton A as the length m of its composite chain (2).

A 0-automaton is called solvable if its composite factors are commutative. It is evident that any commutative 0-automaton is solvable. Another interesting subclass of solvable automata consists of nilpotent automata. A 0-automaton is nilpotent if there is a number m such that all words of length at least m are zero words. It is easy to see that a 0-automaton is nilpotent if and only if there are no cycles and loops which pass through nonzero states. It is evident that any nilpotent automaton is solvable but not vice-versa. As an example, consider the automaton with three states: $A(x) = (133)$, $A(y) = (223)$. This 0-automaton is solvable but not commutative or nilpotent.

Theorem 4.1. *There is a zero word of length at most $l(A)$ for a solvable automaton A.*

Proof. For each composite factor B_i/B_{i-1}, by Theorem 3.1, there is a zero symbol x_i, $1 \leqslant i \leqslant m$. Then by Proposition 2.3 the word $x_m x_{m-1} \ldots x_1$ is a zero word for A. □

This theorem and the trivial inequality $l(A) < n$ imply the following statement.

Corollary 4.2. *There is a zero word of length at most* $n-1$ *for a solvable* 0*-automaton with* n *states.*

5. Strongly reset automata

It is evident that there are many reset automata without a zero state. However, sometimes it is possible to extend the results from 0-automata to reset automata. Here we demonstrate this for strongly reset automata.

Let us refer to a 0-automaton as a strongly reset automaton (SR0-automaton) if for each of its composite factors there is a zero input symbol. Theorem 3.1 implies that commutative and solvable 0-automata are SR0-automata. The proof of Theorem 4.1 is directly extended to SR0-automata, so we have the following statement.

Theorem 5.1. *There is a zero word of length at most* $l(A)$ *for a strongly-reset* 0*-automaton* A.

Now let us consider a reset automaton $A : X^* \to Map(S)$. Denote by A^2 the square of A which is defined on the set $S \times S$ as follows: $A^2((s,t),x) = (A(s,x),A(t,x))$. The subautomaton of A^2 defined on the diagonal $D = \{(s,s) \mid s \in S\}$ is isomorphic to A. Therefore, we may consider the factorautomaton $A_2 = A^2/A$ which is called the pair automaton of A. The next proposition is evident.

Proposition 5.2. *A word is reset for* A *if and only if it is a zero word for* A_2.

Thus an automaton is reset if and only if its pair automaton is a 0-automaton. A reset automaton is called nilpotent (solvable) if its pair automaton is a nilpotent (solvable) 0-automaton. Proposition 5.2 implies that an automaton is nilpotent if and only if any sufficiently long input word is reset for it. Nilpotent automata are known also as definite automata [3, 8]. It is easy to see that there are nilpotent automata without a zero state. The simplest example is the following automaton with two states and two input symbols (trigger): $A(x) = (11), A(y) = (22)$.

An automaton is said to be strongly reset (SR-automaton) if its pair automaton is an SR0-automaton. It is evident from definitions that any nilpotent automaton is solvable and any solvable automaton is strongly reset.

A binary relation R, $D \subset R \subseteq S \times S$ is called invariant for A if $A^2(R,x) \subseteq R$ for all $x \in X$. Every invariant relation R defines the subautomaton $A(R)$ of A^2 and vice versa. An invariant equivalence relation is called a congruence of A. The rank of a congruence is the number of classes in it. For an invariant relation R denote by $cg(R)$ the minimal congruence which contains it. Note that $cg(R)$ is the transitive closure of the relation $R \cup R^{-1}$, where R^{-1} is the inverse relation for R. From the definitions it is easy to prove the following statement.

Proposition 5.3. *If E is a congruence of A, $E \subseteq R$ and x is a zero symbol for the factorautomaton $A(R)/A(E)$, then x is also a zero symbol for the factorautomaton $A(cg(R))/A(E)$.*

Proof. Note that x is a zero symbol for $A(R)/A(E)$ if and only if $A^2(R,x) \subseteq E$. Then $A^2(cg(R),x) \subseteq E$, since E is a congruence. Thus x is a zero symbol for the factorautomaton $A(cg(R))/A(E)$. □

The maximal length m of the following chain of congruences:

$$D = E_0 \subset E_1 \subset \cdots \subset E_m = S \times S \tag{3}$$

is called a height $h(A)$ of an automaton A. Note that $h(A) < n$, since the rank of E_i decreases for $0 \leqslant i \leqslant m$. Now we can prove the most general result.

Theorem 5.4. *There is a reset word of length at most $h(A)$ for any strongly reset automaton A.*

Proof. Let (3) be a maximal chain of congruences of an SR-automaton A and R_i be a minimal invariant relation which satisfies the condition $E_{i-1} \subset R_i \subseteq E_i$, $1 \leqslant i \leqslant m$. Then each factorautomaton $A(R_i)/A(E_{i-1})$, $1 \leqslant i \leqslant m$, is a composite factor of A_2. We also have $cg(R_i) = E_i$ for all i, $1 \leqslant i \leqslant m$, since there are no congruences between E_{i-1} and E_i in A. Then from the definition of SR-automata and Proposition 5.3 it follows that for each factorautomaton $A(E_i)/A(E_{i-1})$ there is a zero symbol x_i, $1 \leqslant i \leqslant m$. Hence, from Proposition 2.3 we conclude that the word $x_m x_{m-1} \ldots x_1$ is a zero word for A_2. Then Proposition 5.2 and the inequality $m \leqslant h(A)$ imply the statement of the theorem. □

Theorem 5.4 and the inequality $h(A) < n$ imply the following fact.

Corollary 5.5. *There is a reset word of length at most $n-1$ for a strongly reset (nilpotent, solvable) automaton with n states.*

6. General 0-automata

It is easy to see that any 0-automaton with n states has a zero word of length at most $(n-1)^2$. Thus Cerny's hypothesis for 0-automata is trivially true. The tight bound for 0-automata was obtained in [10] and is given in the following statement.

Theorem 6.1. *There is a zero word of length at most $(n^2+n)/2$ for any 0-automaton with n nonzero states, and this bound is tight.*

Proof. It is easy to see that the length of the shortest word in a 0-automaton A which takes some state from a subset T to the zero state is not greater than $n+1-|T|$.

Hence, the length of the shortest zero word is not greater than the following number:

$$\sum_{i=n}^{1}(n+1-i)=\sum_{j=1}^{n}j=\frac{(n^2+n)}{2}.$$

To prove the tightness of this bound let us consider the automaton with states $S=\{0,1,\ldots,n\}$, input symbols $X=\{x_1,\ldots,x_n\}$ and the transition function which is defined as follows. Let $A(x_1)=(0,0,2,\ldots,n)$ and let $A(x_i)=(i-1,i)$ be a transposition of states $i-1$ and i for all $i>1$. Denote by $sum(T)$ the sum of the states in a subset T and by $l(w)$ the length of an input word w. Using the definition of A the following inequality may be proved for all T and x_i:

$$sum(T)-1\leqslant sum(A(T,x_i)).$$

From this by induction on the length of a word w we get the following inequality:

$$sum(S)-l(w)\leqslant sum(A(S,w)).$$

Then we have $(n^2+n)/2=sum(S)\leqslant l(w)$ for a zero word w, since in this case $sum(A(S,w))=0$. So the theorem is proved. □

7. Conclusion

Theorem 3.2 is surprising in some sense. It shows that reset properties of commutative automata are similar to those of monogenic automata. Corollary 5.5 demonstrate that the same bound is valid for nilpotent, solvable and strongly reset automata. In opposite to Theorem 6.1 Cerny's hypothesis for general reset automata is still open.

References

[1] J. Cerny, Poznamka *k* homogennym experimentom *s* konecnymy automatami, *Math. Fyz. Casopis* **14** (1964) 208–215.
[2] D. Eppstein, Reset sequences for monotonic automata, *SIAM J. Comput.* **19** (1990) 500–510.
[3] B. Imreh, On finite definite automata, *Acta Cybernet.* **7** (1985) 61–65.
[4] B. Imreh and M. Steinby, Some remarks on directable automata, *Acta Cybernet.* **12** (1995) 23–35.
[5] A. Klyachko, I. Rystsov and M. Spivak, Extremal combinatorial problem associated with the bound on the length of a synchronizing word in an automaton, *Cybernetics* **23** (1987) 165–171.
[6] S. Lang, *Algebra* (Addison-Wesley, Reading, MA, 1965).
[7] A. Letichevsky, Minimization of finite automata, *Cybernetics* **1** (1965) 20–30.
[8] M. Perles, M. Rabin and E. Shamir, The theory of definite automata, *IEEE Trans. Electron Comput.* **12** (1963) 233–243.
[9] J. Pin, Sur un cas particulier de la conjecture de la Cerny, in: *Proc. ICALP'78*, Lecture Notes in Computer Science, Vol. 62 (Springer, Berlin, 1978) 345–352.
[10] I. Rystsov, Estimation of the length of a kernel word for a finite automaton, in: *Automata*, preprint No. 2 (Saratov Univ. Press, Saratov, 1977) 45–50.
[11] I. Rystsov, Exact linear bound for the length of reset words in commutative automata, *Publ. Math.* **48/3–4** (1996) 405–409.