Acta Cybernetica **12** (1995) 145-152.

Quasioptimal Bound for the Length of Reset Words for Regular Automata

I.K. Rystsov *

1 Introduction

In 1964 J. Cerny stated the hypothesis that in a finite reset automaton with n states there is a reset (synchronizing) word whose length is at most $(n-1)^2$ and showed that this bound can be achieved [1]. In [2] this hypothesis was proved by direct enumeration of automata with small number of states. J. Pin used algebraic methods to prove this hypothesis for cyclic automata with prime number of states [3]. The general upper bound $(n^3-n)/6$ has been obtained in [4] for any reset n-state automaton.

The aim of this paper is to obtain the quasioptimal bound $2\cdot(n-1)^2$ for regular reset automata with n states and to extend the class of automata for which the optimal bound is valid.

2 Basic notions

A *finite deterministic automaton* A is a function $A : S \times X \to S$, where S is a *nonempty* finite set of states and X is a finite alphabet of input letters. This function can be considered as a function from X to the multiplicative monoid $Map(S)$ of unary mappings on S. So it can be naturally extended to a homomorphism from the free monoid X^* of words generated by X to the monoid $Map(S)$:

$$A : X^* \to Map(S).$$

This homomorphism associates with a word $w = x_1 \dots x_m$ the composition of mappings $A(w) = A(x_1) \cdot \dots \cdot A(x_m)$. Note that the empty word is mapped to the identical mapping. The submonoid $A(X^*)$ of $Map(S)$ is called the monoid of the automaton A.

Denote by $A(s,w)$ the value of the mapping $A(w)$ in the state $s \in S$. For a subset of states $T \subseteq S$ let us define $A(T,w) = \{A(s,w) \mid s \in T\}$. The *rank* of a word w with respect to A is equal to the number of states in the subset $A(S,w)$. A word is said to be *reset* for A if its rank with respect to A is equal to one . An

*Glushkov Institute of Cybernetics, Kiev, GSP, 252650, Ukraine

automaton is called *reset* if there is a reset word for it. The following proposition is evident.

Proposition 1 A finite automaton A is reset if and only if, for every pair of states s, t, there is a word w such that $A(s, w) = A(t, w)$.

For a word $w = x_1 \dots x_m$, $l(w) = m$ denotes its length. The set of all input words of length less than m is denoted by X_m. A finite nonempty set of input words will be called a *collection*. The length $l(W)$ of a collection W is the length of a longest word in it.

Let n be the number of states in A. A collection W is *transitive* for A if its length is less than n and for every pair of states s, t there is a word $w \in W$ such that $A(s, w) = t$. An automaton is said to be *transitive (strongly-connected)* if there is a transitive collection for it. In the sequel we shall consider only transitive automata because it is sufficient to prove the Cerny's hypothesis for this class of automata [5].

Definition 1 A transitive collection of words W is called regular for A if it contains the empty word and there is a natural number $k \geq 1$ such that for every pair of states s, t, there are exactly k words in W which take the state s into the state t. The constant k will be called the regularity degree.

An automaton is called *regular* if there is a regular collection of words for it. For example, an automaton is regular if there is an input letter which cyclically permutates all its states. More generally, an automaton A with n states is regular if the subset of mappings $A(X_n)$ contains a regular subgroup of permutations. Note that a regular group of permutations is a (noncommutative) scheme of relations [6].

3 Directed automata

The preimage of a subset $T \subseteq S$ under the inverse action of a word w is defined in the following way:

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

The next proposition is evident.

Proposition 2 A word w is reset for A if and only if there is a state s for which $A^o(s, w) = S$.

The number of states in a subset T is denoted by $\mid T \mid$. A word w is said to be *increasing for a subset* T if $\mid A^o(T, w) \mid > \mid T \mid$. A subset of states is *proper* if it is nonempty and is not equal to S.

Definition 2 A collection of words W is called increasing for A if for any proper subset of states in A there is an increasing word in W.

An automaton is called *directed* if there is an increasing collection of words for it.

Theorem 1 An automaton is directed if and only if it is reset and transitive.

Proof. Let A be a reset transitive automaton and w be a reset word for A. Then $A(S,w) = \{s_1\}$, for some state s_1. From transitivity of A it follows that for any state $s_i \in S$, there is a word w_i such that $A(s_1,w_i) = s_i$, $1 \leq i \leq n$. Thus we have $A^o(s_i,ww_i) = S$, for all $1 \leq i \leq n$, hence the collection of words $\{ww_i \mid 1 \leq i \leq n\}$ will be increasing for A.

Conversely, let A be a directed automaton and W be an increasing collection for it. Let us fix any state s_1 as an initial state. Then there is an increasing word $w_1 \in W$ for the subset $\{s_1\}$. Let $S_1 = A^o(s_1,w_1)$. If the subset S_1 is proper then there is an increasing word $w_2 \in W$ for S_1 and we take $S_2 = A^o(S_1,w_2)$. This step can be repeated several times until the set S will be obtained. By construction, we have the following series:

$$1 <\mid S_1 \mid <\mid S_2 \mid < \ldots <\mid S_m \mid = n. \tag{1}$$

As the result we obtain the word $w = w_m \ldots w_1$ such that $A^o(s_1,w) = S$. So, by proposition 2, the word w is reset for A. It is also easy to see that A is transitive, because an initial state can be choosed arbitrarily. Thus the theorem is proved. □

Let $res(A)$ be the minimal length of reset words for a directed automaton A and $inc(A)$ be the minimum over the lengthes of increasing collections of words for A. Theorem 1 implies the following relationship between these functions.

Theorem 2 For any directed automaton A with $n > 1$ states, the inequality $res(A) \leq inc(A) \cdot (n-2) + 1$ is valid.

Proof. Let A be a directed automaton and W be an increasing collection for it of minimal length $inc(A)$. According to theorem 1 A is reset, therefore there is an input letter $x_1 \in X$ for which the mapping $A(x_1)$ is not bijective. Then there is a state s_1 such that $\mid A^o(s_1,x_1) \mid > 1$. Let us fix s_1 as an initial state and repeat the procedure from theorem 1 with $w_1 = x_1$. From (1) it follows that the length of the resulting reset word is at most $l(W) \cdot (n-2) + 1$. This completes the proof. □

This theorem shows that inequality $inc(A) \leq n$ implies Cherny's hypothesis. Since it is difficult to obtain this bound by combinatorial methods, in the next section, we shall use more powerful methods of linear algebra.

4 Linear extensions of automata

Let R be the field of real numbers and R^n the n-dimensional vector space over R. Denote by $\langle u,v \rangle$ the scalar product of vectors u and v in this space. The

standard basis E in this space consists of binary vectors $e_i, 1 \leq i \leq n$, where the i-th component of e_i is equal to one and the others are zeros.

For a collection of vectors V, denote by $Af(V)$ its affine span which consists of affine linear combinations of vectors in V with real coefficients [7]. If a set of vectors is equal to its affine span, then it is called an *affine subspace* of R^n. The *dimension of an affine subspace* is defined as the dimension of the parallel linear subspace [7].

The sum of basic vectors will be called the *unit vector* $e = (1, \ldots 1)$. This vector defines the linear function from R^n to R in the usual way $\mid v \mid = \langle e, v \rangle$. The unit vector belongs to the following hyperplane:

$$P^n = \{v \mid \langle e, v \rangle = n\},$$

which is an $(n-1)$-dimensional affine subspace of R^n.

We say that a collection of vectors $V \subset P^n$ is *complete* if $Af(V) = P^n$. The *centre* c(V) of a collection $V = \{v_1, \ldots, v_m\}$ is defined by the formula:

$$c(V) = \frac{1}{m} \sum_{i=1}^{m} v_i.$$

A collection of vectors V is *central* if $c(V) = e$.

Definition 3 A collection of vectors is called balanced if it is complete and central.

Let A be a finite deterministic automaton with a set of states $S = \{s_1, \ldots, s_n\}$. Then there is a one-to-one correspondence f between S and the standard basis E of the space R^n which is defined as follows $f(s_i) = e_i, 1 \leq i \leq n$. Note that e_i is the characteristic vector of the subset $\{s_i\}$.

Now we define an isomorphic automaton L_A on the set E by the formula $L_A(e_i, x) = e_j$ iff $A(s_i, x) = s_j$. Then we can extend the transition function to the whole linear space as follows:

$$L_A(\sum_{i=1}^{m} r_i \cdot e_i, x) = \sum_{i=1}^{m} r_i \cdot L_A(e_i, x).$$

Thus we obtain the linear automaton L_A which is called the *linear extension* of the automaton A over the field R.

In general case when the basis is fixed, a linear automaton can be considered as a function from X into the algebra $Mat_n(R)$ of $n \times n$ matrices over R. In our case every matrix $L_A(x)$ is binary and row-monomial, because A is deterministic. The element (i, j) of the matrix $L_A(x)$ is equal to one if $A(s_i, x) = s_j$, otherwise it is zero. The product of matrices $L_A(w) = L_A(x_1) \cdot \ldots \cdot L_A(x_m)$ corresponds to the input word $w = x_1 \ldots x_m$. The value of the transition function $L_A(v, w)$ is equal to the product of the row-vector v and the matrix $L_A(w)$.

Let us fix the unit vector $e = (1, \ldots, 1)$ as the initial state of the automaton L_A. The collection of vectors $L_A(e, W) = \{L_A(e, w) \mid w \in W\}$ is associated with

a collection of words W. It is easy to see that $L_A(e,W) \subset P^n$ for any collection W. A collection of words W is called *complete (central, balanced)* for L_A if the collection of vectors $L_A(e,W)$ is complete (central, balanced).

The *product (concatenation)* of two collections of words W, Y is defined in the usual way $WY = \{wy \mid w \in W, y \in Y\}$. The following proposition is linear analog of well-known Moore's theorem [9].

Theorem 3 For any directed automaton A with n states, the collection of words X_n is complete for its linear extension L_A.

Proof. Let w be a reset word of length $res(A)$ and W be a transitive collection of words for A of length $n-1$. Then we have $L_A(e, \{w\}W) = n \cdot E$. So the collection of words X_m, where $m = res(A) + n$, is complete because it contains the complete subcollection $\{w\}W$.

Now let us consider the increasing sequence of affine subspaces $Af(L_A(e, X_i)), 1 \leq i \leq m$. Dimensions of these subspaces are less than n, so there is a positive integer $i < n$ such that $Af(L_A(e, X_i)) = Af(L_A(e, X_{i+1}))$. Hence, we conclude that $Af(L_A(e, X_i)) = Af(L_A(e, X_j))$, for all $j > i$. Therefore, we have

$$Af(L_A(e, X_i)) = Af(L_A(e, X_n)) = Af(L_A(e, X_m)) = P^n$$

and our theorem is proved. □

Let $f(T)$ be the binary characteristic vector of a subset $T \subseteq S$ of length n. Note that the number of states in T is equal to the scalar product $\langle e, f(T)\rangle$.

Lemma 1 If a collection of words W is complete for L_A, then for any proper subset T of S there is a word $w \in W$ satisfying $\langle L_A(e,w), f(T)\rangle \neq \mid T \mid$.

Proof. Consider the following hyperplane:

$$P(T) = \{v \mid \langle v, f(T)\rangle = \mid T \mid\}.$$

The intersection $Q = P(T) \cap P^n$ is a proper affine subspace of P^n because $f(T) \notin P^n$. Hence, $L_A(e,W) \not\subseteq Q$ since the collection of vectors $L_A(e,W)$ is complete. Thus the lemma is proved. □

The inverse transition on a vector e_i and a letter x in the automaton L_A is defined as the product of e_i and the transposed matrix $L_A(x)^o$. Note that the matrix $L_A(x)^o$ is column-monomial, and so, there is an isomorphism between inverse transitions in automata A and L_A which can be described for a subset T and a word w by the following formula:

$$f(A^o(T,w)) = f(T) \cdot L_A(w)^o. \tag{2}$$

There is also the following well-known relationship between the scalar product and inverse action of a matrix which holds for any vectors u, v and word w [8]:

$$\langle u \cdot L_A(w), v\rangle = \langle u, v \cdot L_A(w)^o\rangle. \tag{3}$$

Now we can prove one of the main theorem.

Theorem 4 If a collection of words is balanced for the linear automaton L_A, then it is increasing for A.

Proof. Let $W = \{w_1, \ldots, w_m\}$ be a balanced collection of words for L_A and T be a proper subset of states in A. Denote the collection of vectors $L_A(e, W)$ by V. By our assuption, we have the following equalities:

$$\langle c(V), f(T)\rangle = \langle e, f(T)\rangle = \mid T \mid .$$

By the definition of $c(V)$, we have the following property:

$$\sum_{i=1}^{m} \langle L_A(e, w_i), f(T)\rangle = m \cdot \mid T \mid . \tag{4}$$

Then by Lemma 4, we conclude that there is a word w_j in W for which the following inequlity holds:

$$\langle L_A(e, w_j), f(T)\rangle > \mid T \mid . \tag{5}$$

Indeed, in the opposite case we should have $\langle L_A(e, w_i), f(T)\rangle \leq \mid T \mid$, for all $i, 1 \leq i \leq m$. Then Lemma 4 implies a contradiction because in this case the left-hand side of (4) should be less than the right-hand side.

Properties (2) and (3) implies the following equalities:

$$\langle L_A(e, w_j), f(T)\rangle = \langle e, f(T) \cdot L_A(w_j)^o\rangle = \mid A^o(T, w_j) \mid .$$

So the inequality $\mid A^o(T, w_j) \mid > \mid T \mid$ will be hold for the word w_j satisfying (5). Thus the word w_j is increasing for the subset T, which completes the proof. □

5 Regular automata

Let A denote a regular reset automaton of n states. Let us fix a regular collection of words $Y = \{y_1, \ldots, y_m\}$ for this automaton with regularity degree $k \geq 1$. By definition 1, the parameters k, m, n satisfy the equality $k \cdot n = m$. Recall that the collection Y contains the empty word and $l(Y) < n$.

Consider the linear extension L_A of A over the field R. The bistochastic matrix each element of which is equal to $1/n$ is denoted by J_n. It is easy to see that the following matrix equality holds:

$$\frac{1}{m} \sum_{j=1}^{m} L_A(y_j) = J_n. \tag{6}$$

From this we obtain the next proposition.

Lemma 2 For any collection W, the collection of words WY is central for L_A.

Proof. Let $W = \{w_1, \ldots, w_l\}$. If we multiply the equality (6) from left by the vector $c(L_A(e, W))$, then we get the following equality:

$$\frac{1}{lm} \sum_{i=1}^{l} \sum_{j=1}^{m} L_A(e, w_i y_j) = e.$$

Therefore, the lemma is proved. □

Now we can prove the main result.

Theorem 5 There is a reset word for A whose length is at most $2 \cdot (n-1)^2$.

Proof. Consider the collection of words $W = X_n Y$. Since the collection Y contains the empty word, we have the inclusion $X_n \subset W$. Hence, from Theorem 3 we conclude that the collection W is complete for L_A. Lemma 6 implies that the collection W is central, and so, it is balanced for L_A. Then by Theorem 5, we get that the collection W is increasing for A. So we have the following inequalities:

$$inc(A) \leq l(W) \leq l(X_n) + l(Y) \leq 2 \cdot (n-1).$$

Now using Theorem 2, we obtain the following bounds:

$$res(A) \leq 2 \cdot (n-1) \cdot (n-2) + 1 \leq 2 \cdot (n-1)^2.$$

Thus the theorem is proved. □

At last we give a sufficient condition which implies the validity of Cerny's hypothesis.

Theorem 6 If the collection of words XY is complete for the linear extension of A, then $res(A) \leq (n-1)^2$.

Proof. Indeed, by Lemma 6, the collection XY is central, and so, it is balanced. Then by Theorem 5 we conclude that $inc(A) \leq n$. Thus the required statement follows from Theorem 2.

6 Conclusion

Note that theorem 8 gives the largest class of automata for which the optimal bound is known, because cyclic automata from papers [1] and [3] satisfy its condition. It is interesting to study the following hypothesis.

Hypothesis. *Any transitive automaton is regular.*

If this hypothesis is valid, then from Theorem 7 it follows that the quasioptimal bound $2 \cdot (n-1)^2$ holds for any reset n-state automaton.

References

[1] Cerny, J., Poznamka k homogennym experimentom s konecnymy automatami, *Math. Fyz. Cas. SAV,* v.14 (1964), 208-215.

[2] Cerny, J., Pirica, A., Rosenauerova B. On directable automata, *Kybernetika,* v.7 (1971), 289-298.

[3] Pin, J.E., Sur un cas particulier de la conjecture de Cerny, Lect. Notes Comp. Sci., v.62 (1978), 345-352.

[4] Kljachko, A., Rystsov, I., Spivak M. Extremal combinatorial problem concerning the length of the reset word in a finite automaton, *Cybernetics,* v.23 (1987), 165-170. (Tranlated from Russian)

[5] Rystsov, I.K., Rank of a finite automaton, *Cybernetics and System Analysis,* v.28 (1992), 323-328. (Translated from Russian)

[6] Bannai, E., Ito, T., *Algebraic combinatorics (Association schemes),* The Benjamin/Cummings Publishing Company, 1984.

[7] Brondsted, A., *An introduction to convex polytopes,* Springer-Verlag, 1983.

[8] Halmos, P.R., *Finite-dimentional vector space,* Van-Nostrand, 1963.

[9] Moore, E., Gedanken experiments with sequential machines, in: Automata Studies, Princeton University Press, 1956.

Received January, 1995