A note on Černý's Conjecture and rational series

Marie-Pierre Béal*

January 14, 2003

Abstract

Černý's Conjecture claims that each synchronized n-state automaton possesses a synchronizing word of length at most $(n-1)^2$. It has been shown to be true for particular classes of automata like circular automata, or automata with an underlying Eulerian graph for instance. By the use of rational series, we give a simple proof of the known fact that a synchronized circular automaton possesses a synchronizing word of length at most quadratic, without achieving the exact bound $(n-1)^2$ of the Conjecture. We also use rational series to derive a simple proof of the Conjecture for automata with an Eulerian graph. Moreover, we improve the bound for this class of automata by showing that a synchronized automaton with an Eulerian graph possesses a synchronizing word of length at most n^2-3n+3, which is strictly less than $(n-1)^2$ for $n > 2$.

Keywords: Černý's Conjecture, synchronized automata, rational series.

1 Introduction

Synchronized automata are deterministic and complete finite-state automata admitting a synchronizing word, that is a word which takes each state of the automaton to a single special state. The Černý's Conjecture claims that each n-state synchronized automaton has a synchronizing word of length at most $(n-1)^2$ [2] . Recently, an extension of this Conjecture due to Pin [6, 8] was shown to be false by Kari [4]. The Conjecture has been shown to be true for particular classes of automata like the class of circular automata by Dubuc [3] (see also [7]). An $O(n^2 \log n)$ bound has been recently obtained by Trahtman [9] for aperiodic automata.

In this note, we give a proof of a $2n^2-6n+5$ bound for circular automata which is simpler than the one given in [3]. Nevertheless, it does not allow us

*Institut Gaspard-Monge, Université de Marne-la-Vallée, 77454 Marne-la-Vallée Cedex 2, France. beal@univ-mlv.fr.

to get the tight $(n-1)^2$ bound. The proof uses rational series and specially the fact that a rational series of rank n which is null for all words of length at most $n-1$, is null everywhere [1].

The formulation of the problem in terms of rational series also provides a simple proof of a recent result from Kari [5] which proves Černý's Conjecture for automata with an underlying Eulerian graph. Moreover we improve slightly the bound for these automata by showing that a synchronized automaton with an underlying Eulerian graph possesses a synchronizing word of length at most $n^2 - 3n + 3$, which is strictly less than $(n-1)^2$ as soon as $n > 2$. In other words, the class of synchronized automata with an Eulerian graph does not contain any instance achieving Černý's bound for $n > 2$.

2 Černý's Conjecture

Let A be a finite alphabet and A^* be the set of finite words drawn from the alphabet A, the empty word ϵ included.

In this paper, we will consider a finite-state *complete deterministic automaton* on the alphabet A, that is a pair $\mathcal{A} = (Q, \delta)$ where Q is the finite set of states and δ the transition function which is defined for any state of Q and any letter of A. We will denote the number of states of $\mathcal{A}$ by n. The automaton is not complete if δ is a partial function. If p is a state and a is a letter of A, we denote by $p \cdot a$ the state $\delta(p, a)$. This notation is extended from the letters to the words. If u is a word and P is a subset of Q, we denote by $P \cdot u$ the set $\{p \cdot u \mid p \in P\}$ and by Pu^{-1} the set $\{p \mid p \cdot u \in P\}$. A word u is said to be an *augmenting word* for a subset P of Q if $\mathrm{card}(Pu^{-1}) > \mathrm{card}(P)$. A subset P of Q is said *k-augmentable* if there is an augmenting word for P of length at most k.

If u is a word, we denote by M_u the transition matrix of the action of u on the states defined as follows.

$$\begin{aligned}(M_u)_{pq} &= 1 \text{ if } p \cdot u = q,\\ (M_u)_{pq} &= 0 \text{ otherwise.}\end{aligned}$$

The matrix $M_{u^{-1}} = {}^t M_u$ is the transition matrix of the action of u^{-1} on the states. Remark that if u, v are two words, $M_{uv} = M_u M_v$.

The *rank* of a word u is the cardinal of $Q.u$. Note that since the automaton is complete deterministic, this rank is non null. A *synchronizing word* of $\mathcal{A}$ is a word of rank one. A *synchronized automaton* is an automaton which has a synchronizing word. We can now state the Černý Conjecture.

Černý's Conjecture: Each synchronized n-state automaton possesses a synchronizing word of length at most $(n-1)^2$.

We describe the property of being augmentable for a subset of the set of states of the automaton in terms of rational series.

Let us denote by $\mathbf{l}$ et $\mathbf{c}$ the row and column vectors of size n whose components are all equal to 1. Since $\mathcal{A}$ is a deterministic complete automaton, we easily get the following lemma.

Lemma 1 *For any word $u \in A^*$, $M_u\mathbf{c} = \mathbf{c}$.*

Let P be a subset of Q and $\mathbf{v}$ (resp. $\mathbf{w}$) be the characteristic row (resp. column) vector of a subset P. The word u is an augmenting word for P if and only if

$$\begin{aligned} & \mathrm{card}(Pu^{-1}) > \mathrm{card}(P) \\ \iff\ & \mathbf{v}M_{u^{-1}}\mathbf{c} \ > \ \mathbf{v}\cdot\mathbf{c} \\ \iff\ & \mathbf{l}M_u\mathbf{w} \ > \ \mathbf{l}\cdot\mathbf{w} \\ \iff\ & \mathbf{l}(M_u - I)\mathbf{w} \ > \ 0 \\ \iff\ & \langle S, u\rangle > 0, \end{aligned}$$

where we note

$$\langle S, u\rangle = \mathbf{l}(M_u - I)\mathbf{w}.$$

Thus $S = \sum_{u\in A^*} \langle S, u\rangle\, u$, is a series in $\mathbb{Z}\langle\langle A\rangle\rangle$ depending on the set P, which is omitted in the notation. The set P is k-augmentable if and only if there is a word u with $|u| \leq k$, such that $\langle S, u\rangle > 0$.

The series S is $\mathbb{Z}$-rational. Indeed, the series S has the following linear representation (λ, μ, γ) with $\lambda \in \mathbb{Z}^{1\times 2n}, \mu : A^* \to \mathbb{Z}^{2n\times 2n}, \lambda \in \mathbb{Z}^{2n\times 1}$,

$$\lambda = (\mathbf{l}, -\mathbf{l}), \mu(u) = \begin{bmatrix} M_u & \mathbf{0} \\ \mathbf{0} & I \end{bmatrix}, \gamma = \begin{bmatrix} \mathbf{w} \\ \mathbf{w} \end{bmatrix},$$

since $\langle S, u\rangle = \lambda\mu(u)\gamma$.

We now regard the series S as a rational series in $\mathbb{R}\langle\langle A\rangle\rangle$. Recall that the rank of a rational series is the minimal dimension of a linear representation of the series.

Lemma 2 *The rank of S is at most n.*

Proof: The rank of S is bounded above by the dimension of the vectorial space generated by the row vectors $(\mathbf{l}M_u, -\mathbf{l})$. This space is included in the vectorial space generated by the vectors $(\mathbf{l}M_u - \mathbf{l}, \mathbf{0})$ and the row vector $(\mathbf{l}, -\mathbf{l})$, where $\mathbf{0}$ is the null row vector of size n. Thus the rank of S is at most the dimension of the vectorial space V generated by the vectors $\mathbf{l}(M_u - I)$, plus one. We now show that the dimension of V is at most $n-1$. By lemma 1, and since the automaton is complete deterministic, for any $u \in A^*$, $\mathbf{l}(M_u - I)\cdot\mathbf{c} = 0$. Thus V is included in the hyperspace orthogonal to the vector $\mathbf{c}$. Its dimension is thus at most $n-1$. $\square$

3 Černý's Conjecture for circular automata

A *circular* automaton is a deterministic complete automaton on the alphabet A such that there is a letter a of A which induces a circular permutation of the states, i.e. such that M_a is a circular permutation matrix. In [3] it is shown that Černý's Conjecture is true for circular synchronized automata.

Proposition 3 (Dubuc) *A circular synchronized automaton of size n has a synchronizing word of size $(n-1)^2$.*

We give below a proof of the fact that a circular synchronized automaton of size n has a synchronizing word of size $2n^2 - 6n + 5$. Remark that $2n^2 - 6n + 5 \leq 2(n-1)^2$ as soon as $n > 2$. Although the method does not seem to allow us to obtain the Černý bound got in [3], we get the quadratic bound in a much simpler way than the one used in [3].

Proof: Let $\mathcal{A}$ be the synchronized circular automaton whose set of states is Q. We denote by a a letter of A which induces a circular permutation of the states of Q. Let P be a non-empty strict subset of Q and S be the rational series associated to this set P defined as above. We denote by $\mathbf{w}$ the characteristic column vector of P.

For any word u, we have

$$\langle S, au\rangle = \langle S, u\rangle\,,$$
$$\sum_{i=0}^{n-1} \left\langle S, ua^i\right\rangle = 0.$$

Indeed,

$$\begin{aligned}\langle S, au\rangle &= \mathbf{1}M_{au}\mathbf{w} - \mathbf{1}\cdot\mathbf{w}\\ &= \mathbf{1}M_aM_u\mathbf{w} - \mathbf{1}\cdot\mathbf{w}\\ &= \mathbf{1}M_u\mathbf{w} - \mathbf{1}\cdot\mathbf{w}\\ &= \langle S, u\rangle\,.\end{aligned}$$

and

$$\begin{aligned}\sum_{i=0}^{n-1} \left\langle S, ua^i\right\rangle &= \sum_{i=0}^{n-1} \mathbf{1}(M_{ua^i} - I)\mathbf{w} = \sum_{i=0}^{n-1} \mathbf{1}M_uM_{a^i}\mathbf{w} - \mathbf{1}\cdot\mathbf{w}\\ &= \sum_{i=0}^{n-1} \mathbf{1}M_uM_{a^i}\mathbf{w} - \mathbf{1}M_{a^i}\mathbf{w} = \sum_{i=0}^{n-1} \mathbf{1}(M_u - I)M_{a^i}\mathbf{w}\\ &= \mathbf{1}(M_u - I)(\sum_{i=0}^{n-1} M_{a^i}\mathbf{w}) = \mathbf{1}(M_u - I)(\sum_{i=0}^{n-1} w_i)\mathbf{c}\\ &= (\sum_{i=0}^{n-1} w_i)\mathbf{1}(M_u - I)\mathbf{c} = 0.\end{aligned}$$

Let us assume that P is not $2(n-1)$-augmentable. Thus for any word u with $|u| \leq 2(n-1)$, $\langle S, u\rangle \leq 0$. Then for any word u of length at most $n-1$ and any integer $0 \leq i \leq n-1$, $\left\langle S, ua^i\right\rangle \leq 0$. Since $\sum_{i=0}^{n-1} \left\langle S, ua^i\right\rangle = 0$, for any integer $0 \leq i \leq n-1$, $\left\langle S, ua^i\right\rangle = 0$. We get that for any u with $0 \leq |u| \leq n-1$, $\langle S, u\rangle = 0$. Then by Lemma 2 and [1, Corollary 3.6, p. 33], $\langle S, u\rangle = 0$ for any word u. This contradicts the fact that , in a synchronized automaton with a strongly connected graph, any non-empty strict subset of Q is augmentable.

Thus any non-empty and not full set P is $2(n-1)$-augmentable. Since it is trivial that there is state p such that $\{p\}$ is 1-augmentable, This proves the existence of a synchronizing word of length at most $1+2(n-1)(n-2) = 2n^2 - 6n + 5$. □

4 Černý's Conjecture for Eulerian automata

In [5], Kari shows that Černý's Conjecture is true for automata with an underlying Eulerian graph, that is, with a graph which has a constant out and in-degree for each state. We show below how this result can be easily derived from the above formulation. Moreover, we prove that such an automaton has a synchronizing word of length at most $n^2 - 3n + 3$, which is strictly less than the Černý bound $(n-1)^2$, as soon as $n > 2$.

Proposition 4 *If a synchronized automaton has an Eulerian graph, it possesses a synchronizing word of length at most $n^2 - 3n + 3$.*

Proof: We show that any non-empty and not full subset P of the set of states is $(n-1)$-augmentable. Let us assume the opposite. The automaton is synchronized and there is a non-empty and not full subset P of the set of states which is not $(n-1)$-augmentable. Thus for any word u of length at most $n-1$, $\langle S, u\rangle \leq 0$, where S is the rational series associated to the set P as in Section 2.

We claim that, for any integer $k \geq 1$, either $\langle S, u\rangle = 0$ for any word u of length k or there is a word u of length k such that $\langle S, u\rangle > 0$. Indeed, if $\mathbf{w}$ denotes the column characteristic vector of P, for any $k \geq 1$, and since the graph is Eulerian,

$$\sum_{u \in A^k} \langle S, u\rangle = (\mathbf{1} \sum_{u \in A^k} M_u) \cdot \mathbf{w} - \sum_{u \in A^k} \mathbf{1} \cdot \mathbf{w} = |A^k| \mathbf{1} \cdot \mathbf{w} - |A^k| \mathbf{1} \cdot \mathbf{w} = 0,$$

which proves the claim.

We get that $\langle S, u\rangle = 0$ for any word u of length at most $n-1$. By Lemma 2 and [1, Corollary 3.6, p. 33], $\langle S, u\rangle = 0$ for any word u. Then any non-empty and not full subset of the set of states is $(n-1)$-augmentable. Since the automaton is synchronized there is at least one state p such that $\{p\}$ is 1-augmentable. This implies that there is a synchronizing word of length at most $1 + (n-1)(n-2) = n^2 - 3n + 3$. □

5 Remarks

Černý's Conjecture is true for an n-state synchronized automaton such that each augmentable subset of the set of states has an augmenting word of size at most n leading to another augmentable subset. We call this property the property of uniform augmentation for an n-state automaton. If this property is satisfied and if the automaton has a word of rank r, then there is such a word of length less than or equal to $1+(n-1-r)*n = n^2-(r+1)n+1$. For $1 < r < n$, this bound is greater than the $(n-r)^2$ bound of the Černý-Pin conjecture which was shown to be false by Kari [5].

The automaton of Kari [5] shows that the property of uniform augmentation is not always satisfied. This automaton is a synchronized 6-state automaton $\mathcal{A} = (Q, \delta)$, where $Q = (0,1,2,3,4,5)$, defined by $\delta(Q,a) = (1,2,0,4,5,3)$ and $\delta(Q,b) = (0,1,5,3,2,2)$. It can be checked by hand that the subset $P = \{0,2,3,4,5\}$ is 8-augmentable and is not m-augmentable for $m < 8$. Thus Kari's automaton has not the property of uniform augmentation, although this part is not equal to $Q.u$ for some word u. For this subset, the corresponding rational series is a rational series of rank at most n, which is less than or equal to zero for words of length at most $n+1$, and which is positive for a word of length $n+2$.

References

[1] J. Berstel and Ch. Reutenauer, *Rational Series and their Languages*, Springer-Verlag, 1988.

[2] J. Černý, *Poznámka k. homogénnym experimentom s konecnými automatmi*, Mat. fyz. čas SAV, 14 (1964), pp. 208–215.

[3] L. Dubuc, *Sur les automates circulaires et la conjecture de Černý*, RAIRO Inform. Théor. Appl., 32 (1998), pp. 21–34.

[4] J. Kari, *A counter example to a conjecture concerning synchronizing words in finite automata*, EATCS Bulletin, 73 (2001), p. 146.

[5] ——, *Synchronizing finite automata on Eulerian digraphs*, in MFCS'2001, no. 2136 in LNCS, Berlin, 2001, Springer, pp. 432–438.

[6] J.-E. Pin, *Le problème de la synchronisation et la conjecture de Černý*, thèse de 3ème cycle, Université Paris VI, 1978.

[7] ——, *Sur un cas particulier de la conjecture de Černý*, in 5th ICALP, no. 62 in LNCS, Berlin, 1978, Springer, pp. 345–352.

[8] ——, *On two combinatorial problems arising from automata theory*, Annals of Discrete Mathematics, 17 (1983), pp. 535–548.

[9] A. N. Trahtman, *The existence of synchronizing word and Černý conjecture for some finite automata.* to appear in Discrete Appl. Math., 2002.