ELSEVIER Theoretical Computer Science 295 (2003) 223–232

Theoretical Computer Science

www.elsevier.com/locate/tcs

Synchronizing finite automata on Eulerian digraphs ☆

Jarkko Kari[1]

Department of Computer Science, 15 MLH, University of Iowa, Iowa City, IA 52242 USA

Received 24 August 2001; received in revised form 6 November 2001; accepted 28 November 2001

Abstract

Černý's conjecture and the road coloring problem are two open problems concerning synchronization of finite automata. We prove these conjectures in the special case that the vertices have uniform in- and outdegrees.

Keywords: Finite automata; Synchronization

1. Introduction

Let us call a directed graph $G=(V,E)$ admissible (k-admissible, to be precise) if all vertices have the same outdegree k. A deterministic finite automaton (DFA) without initial and final states is obtained if we color the edges of a k-admissible digraph with k colors in such a way that all k edges leaving any node have distinct colors. Let $\Sigma=\{1,2,\ldots,k\}$ be the labeling alphabet. We use the standard notation Σ^* for the set of words over Σ. Every word $w\in\Sigma^*$ defines a state transition function $f_w : V \to V$ on the vertex set V: the vertex $f_w(v)$ is the endpoint of the unique path that starts at v and whose labels read w. For a set $S\subseteq V$ we define

$$f_w(S) = \{f_w(v) \mid v \in S\},$$

and

$$f_w^{-1}(S) = \{v \mid f_w(v) \in S\}.$$

☆ Research supported by NSF Grant CCR 97-33101.

[1] A preliminary version of this paper has been presented to the Mathematical Foundations of Computer Science, MFCS 2001.

E-mail address: jjkari@cs.uiowa.edu (J. Kari).

PII: S0304-3975(02)00405-X

Word w is called synchronizing if $f_w(V)$ is a singleton set, and the automaton is called synchronized if a synchronizing word exists. A coloring of an admissible graph is synchronized if the corresponding automaton is synchronized.

We investigate the following two natural questions:

- Which admissible digraphs have synchronized colorings?
- What is the length of a shortest synchronizing word on a given synchronized automaton?

The road coloring problem and Černý's conjecture are two open problems related to these questions. The road coloring problem [1,2] asks whether a synchronized coloring exists for every admissible digraph that is strongly connected and aperiodic. A digraph is called aperiodic if the gcd of the lengths of its cycles is one. This is clearly a necessary condition for the existence of a synchronized coloring. The road coloring problem has been solved in some special cases but the general case remains open. In particular, it is known to be true if the digraph has a simple cycle of prime length and there are no multiple edges in the digraph [10].

In this work, we prove the road coloring conjecture in the case the digraph is Eulerian, i.e., also the indegrees of all nodes are equal to k. (We assume k-admissibility throughout this paper.) This partial solution is interesting because such digraphs can also be colored in a completely non-synchronized way: there exist labelings where every color specifies a permutation of the vertex set so that no input word can synchronize any vertices.

Lemma 1. *Let $G=(V,E)$ be a digraph with all in- and outdegrees equal to some fixed k. Then the edges can be colored with k colors in such a way that at every vertex all entering edges have distinct colors and all leaving edges have distinct colors.*

Proof. Let us start by constructing a undirected graph $G'=(V_1\cup V_2,E')$ with twice as many vertices as G. For each vertex v of G graph G' has two vertices $v_1\in V_1$ and $v_2\in V_2$, and for each edge $v \to u$ of G graph G' contains the undirected edge connecting v_1 and u_2, the representatives of v and u in V_1 and V_2, respectively.

Graph G' is bipartite because all edges are between V_1 and V_2, and all vertices of G' have degree k. It follows from the well-known marriage theorem by Frobenius [16] that graph G' has a perfect matching, i.e., a set of edges such that each vertex is incident to exactly one edge. The corresponding directed edges in G leave and enter each vertex exactly once, hence they can be colored with the same color.

Let us remove the newly colored edges from G. The remaining digraph has uniform in- and outdegree $k-1$. Using the principle of mathematical induction we know the remaining edges can be colored with the remaining $k-1$ colors. □

We also prove Černý's conjecture if the underlying digraph is Eulerian. Černý's conjecture [4] states that if an n-state automaton is synchronized, then there always exists a synchronizing word of length at most $(n-1)^2$. Currently, the best known bounds for the shortest synchronizing word are cubic in n, see e.g., [15] and its references. In Section 4, we prove the conjecture in the Eulerian case; In fact, it turns out that we obtain a slightly better upper bound $(n-1)(n-2)+1$ for the length of the shortest synchronizing word.

2. Maximum size synchronized subsets

Our proofs rely on a result by Friedman [6]. We only need this result in the Eulerian case, which we include here for the sake of completeness. This section also introduces the notion of maximum size synchronized sets of vertices, which is crucial in our proofs. All results in this section were originally presented in the Friedman paper [6].

Given an automaton A, let us say that set $S \subseteq V$ is synchronized if there exists a word w such that $f_w(S)$ is a singleton set. Clearly, for every word u, if S is synchronized then also $f_u^{-1}(S)$ is synchronized, synchronized by word uw.

Let us only consider finite automata that are based on Eulerian digraphs, and let k be the in- and outdegree of every node. We are interested in synchronized sets of maximal cardinality, called *maximum size synchronized sets*. Let m be the largest cardinality of any synchronized set. If n-state automaton A is synchronized then $m=n$, but in general $1 \leqslant m \leqslant n$. In a moment we will see that m has to divide n, and that the vertex set V can be partitioned into non-overlapping maximum size synchronized subsets.

Because in the Eulerian case every vertex has k incoming edges we have

$$\sum_{a\in\Sigma} |f_a^{-1}(S)| = k|S| \tag{1}$$

for every $S \subseteq V$. Therefore, if $|S|=m$ we must have $|f_a^{-1}(S)|=m$ for every color $a \in \Sigma$, and more generally $|f_u^{-1}(S)|=m$ for every word u. In other words, predecessors of maximum size synchronized sets have also maximum size.

Consider a collection of i maximum size synchronized sets $S_1, S_2, \ldots, S_i$ that are synchronized by the same word w, and that are hence disjoint. Let y_j denote the unique element of $f_w(S_j)$ for every $j=1,2,\ldots,i$. If $im<n$ then the collection is not yet a partitioning of V and there exists a vertex x that does not belong to any S_j. Because the graph is strongly connected there exists a word u such that $f_u(y_1)=x$. Consider subsets that are synchronized by word wuw. These include S_1 (which is already synchronized by the first w) as well as $f_{wu}^{-1}(S_j)$ for all $j=1,2,\ldots,i$. All these $i+1$ sets are maximum size synchronized sets, and they are different from each other because they are synchronized by wuw into distinct vertices $f_w(x)$ and $y_j = f_w(S_j)$, for $j=1,2,\ldots,i$.

The reasoning above can be repeated until we reach a partitioning of V into maximum size synchronized sets, all synchronized by the same word. We have proved

Proposition 1. *In any DFA that is based on a Eulerian digraph $G=(V,E)$ there exists a word w such that subsets of vertices synchronized by w form a partitioning of V into maximum size synchronized sets.*

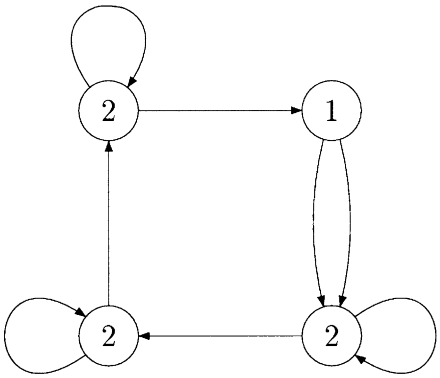

Fig. 1. A non-Eulerian admissible digraph and the weights of its vertices.

As a corollary we see that the maximum size m of synchronized sets must divide n, the number of vertices. It is also clear that if w satisfies the property of the proposition then so does uw for every $u \in \Sigma^*$.

In [6] a more general approach is taken, applicable also in non-Eulerian cases. In this approach the notion of the cardinality of a subset is replaced by its weight. To define weights, note that the adjacency matrix of the digraph has a positive left eigenvector e with eigenvalue k. The eigenvector is chosen with relatively prime integer components. Components of e are the weights of the corresponding vertices, and the weight of a set of vertices is the sum of the weights of its elements. In Eulerian cases the weight of a set is simply its cardinality because $e=(1,1,\ldots,1)$.

Example 1. Consider the non-Eulerian digraph in Fig. 1. The weights are shown inside the vertices. Note the defining property that at each node the weight times k equals the sum of the incoming weights.

Instead of maximum size synchronized sets the non-Eulerian case considers maximum weight synchronized sets. It follows from the way the weights are dedefined that Eq. (1) is valid in the general set-up if the notion of the set cardinality is replaced by the notion of the weight. So we conclude that the predecessors of maximum weight synchronized sets have also maximum weight, and we get the following more general proposition [6]:

Proposition 2. *In any DFA there exists a word w such that subsets of vertices synchronized by w form a partitioning of V into maximum weight synchronized sets.*

3. Synchronized colorings of Eulerian digraphs

To prove the road coloring property of Eulerian digraphs we use the notion of stability from [5]. States x and y of a DFA A are called stable, denoted $x \equiv y$, iff

$$(\forall u \in \Sigma^*)(\exists w \in \Sigma^*), \quad f_{uw}(x) = f_{uw}(y),$$

i.e., for every word u nodes $f_u(x)$ and $f_u(y)$ are synchronized. It is easy to see that stability is a congruence relation, i.e., an equivalence relation respected by all state transitions f_a. This means that each f_a maps equivalence classes into equivalence classes.

Lemma 2. *Relation $\equiv$ is a congruence relation.*

Proof. Trivially $\equiv$ is reflexive and symmetric. Let us prove transitivity. Let $x \equiv y$ and $y \equiv z$, and let u be an arbitrary word. To prove $x \equiv z$ we need to show that there exists a word w such that $\delta(x, uw) = \delta(z, uw)$. Because $x \equiv y$ there exists a word w_1 such that $\delta(x, uw_1) = \delta(y, uw_1)$, and because $y \equiv z$ there exists a word w_2 such that $\delta(y, uw_1w_2) = \delta(z, uw_1w_2)$. Then $\delta(x, uw_1w_2) = \delta(y, uw_1w_2) = \delta(z, uw_1w_2)$, so we can choose $w = w_1w_2$.

If $x \equiv y$ then it is easy to see that also $f_a(x) \equiv f_a(y)$. Hence $\equiv$ is a congruence relation. $\square$

We call the equivalence classes of the stability relation the *stability classes* of the automaton. Because stability is a congruence, one has a well-defined quotient automaton $(A/\equiv)$ whose states are the stability classes.

It was pointed out in [5] that the road coloring problem is equivalent to the conjecture that there always exists a coloring with at least one stable pair of vertices. The idea is that if a coloring with non-trivial stability classes exists, then the quotient automaton $(A/\equiv)$ has fewer states than A. The quotient automaton is also strongly connected and aperiodic if the original automaton has these properties. One uses mathematical induction and assumes that the quotient automaton can be relabeled into a synchronized automaton. The relabeling can be lifted to the original automaton, providing it with a synchronized coloring because a relabeling does not break the stability of any nodes that were in the same stability class.

In the following we adapt this reasoning to the Eulerian case, and prove:

Theorem 1. *The road coloring conjecture is true for Eulerian digraphs.*

Proof. We use mathematical induction on the number of vertices. If $|V| = 1$ the claim is trivial. Assume then that $G = (V, E)$ is an admissible, strongly connected and aperiodic Eulerian digraph with $|V| > 1$, and that the road coloring conjecture has been proved for such digraphs with fewer vertices.

Let us start with a fully non-synchronized coloring of G, where all vertices have different colors on all entering and leaving edges (Lemma 1). Let x be a vertex and a and b two colors such that $f_a(x) \neq f_b(x)$. These must exist because otherwise the digraph would be periodic. Let $y = f_a(x)$ and $z = f_b(x)$. Let us swap the colors of edges $x \to y$ and $x \to z$. Then two edges labeled a enter z, and two edges labeled b enter node y. Because all other nodes have one edge of each color entering them, it is clear that for any set S of vertices

$$z \in S, y \notin S \Rightarrow |f_a^{-1}(S)| > |S|$$

and

$$y \in S, z \notin S \Rightarrow |f_b^{-1}(S)| > |S|.$$

Therefore, any maximum size synchronized set of vertices must either contain both y and z or neither of them. Consequently, any word w from Proposition 1 synchronizes y and z.

Let us prove that $y \equiv z$: Let $u \in \Sigma^*$ be arbitrary, and let w be a word satisfying Proposition 1. Then also uw satisfies Proposition 1, which means that $f_{uw}(y) = f_{uw}(z)$.

Because there are non-trivial stability classes the quotient automaton $(A/\equiv)$ has fewer states than the original automaton. It is clear that (the underlying digraph of) the quotient automaton is admissible, strongly connected and aperiodic, because the original digraph G has these properties. To prove that it is also Eulerian, it is enough to show that there are edges of all colors entering all stability classes. This is trivially true for any class that contains any node different from y and z as all these nodes have incoming edges of all colors. And since y and z are in the same stability class, also that class has entering edges of all colors.

The quotient automaton has fewer states, so according to the induction hypothesis there exists a synchronized recoloring of the quotient automaton. This induces a synchronized coloring of the original automaton as follows: We recolor each vertex x using the same permutation of colors that was used to recolor the equivalence class containing x. Each stable pair of vertices remains stable because the recoloring respects the stability classes. In addition, there exists a word w that takes all states into one equivalence class. Such w is any synchronizing word of the recolored quotient automaton. This means that the re-colored automaton is synchronized. □

The reasoning fails on non-Eulerian digraphs. It is, however, easy to see that even in the non-Eulerian case nodes x and y are stable if and only if every maximum weight synchronized set either contains both x and y or neither of them. In other words, stability classes are intersections of maximum weight synchronized sets.

4. The Černý's conjecture

We have proved that Eulerian digraphs have synchronized colorings. In this section we show that any such coloring admits a synchronizing word of length at most $(n-1)(n-2)+1$, where $n = |V|$.

Let us view the vertex set V as an orthonormal basis of the n-dimensional vector space $\mathbb{R}^n$, and subsets of V as vectors obtained as sums of their elements: Set $S \subseteq V$ is viewed as the vector $\sum_{x \in S} x$.

It is useful to view functions f_a^{-1} as linear transformations of this vector space, for all $a \in \Sigma$. Because we know how each f_a^{-1} acts on the vectors in the basis V, there is a unique way to extend f_a^{-1} into a linear $\mathbb{R}^n \to \mathbb{R}^n$ mapping. In other words, the transformation matrix of f_a^{-1} with respect to basis V is the transpose of the adjacency matrix for edges colored with a.

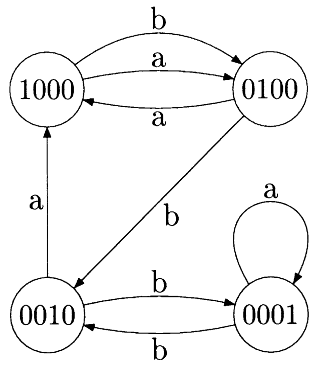

Fig. 2. A DFA defining linear functions f_a^{-1} and f_b^{-1} over $\mathbb{R}^4$.

Note that $f_a^{-1}(S)$ for $S \subseteq V$ has the same meaning as before. Its old definition is consistent with the linearity. As before, functions f_w^{-1} for $w \in \Sigma^*$ are obtained as compositions of the single letter functions f_a^{-1}. Our reason for investigating functions f_w^{-1} is the fact that w is synchronizing if and only if f_w^{-1} maps one of the basis vectors into the vector $(1,1,\ldots,1)$ representing set V.

Example 2. Consider the DFA in Fig. 2. We have, e.g., $f_a^{-1}(1,0,0,1) = (0,1,1,1)$ and $f_{aba}^{-1}(1,0,0,0) = (1,1,1,1)$. Word *aba* is synchronizing.

If the DFA is Eulerian we say that the *weight* of a vector is the sum of its components (under the basis V). More generally, a weight of a vector x is the inner product of x with the left eigenvector e defined in the end of Section 2. Note that the two definitions are consistent as in the Eulerian case we have $e = (1,1,\ldots,1)$. We denote the weight of vector x by $|x|$. Our choice of notation is explained by the fact that in the Eulerian case the weight of the vector representing a set $S \subseteq V$ is the same as the cardinality of the set. It is important that the weight function $x \mapsto |x|$ is a linear function $\mathbb{R}^n \to \mathbb{R}$.

The weight function satisfies Eq. (1) in Section 2. The equation holds even for arbitrary vectors, and the general non-Eulerian DFA: For every $x \in \mathbb{R}^n$

$$\sum_{a \in \Sigma} |f_a^{-1}(x)| = k|x|. \tag{2}$$

It follows from (2) that for every $x \in \mathbb{R}^n$ either

$$(\forall a \in \Sigma) \quad |f_a^{-1}(x)| = |x|$$

or

$$(\exists a \in \Sigma) \quad |f_a^{-1}(x)| > |x|.$$

More generally, if $|f_w^{-1}(x)| \neq |x|$ for some $w \in \Sigma^*$ then $|f_u^{-1}(x)| > |x|$ for some u that has the same length as w.

For any given $x\in\mathbb{R}^n$ we would like to establish an upper bound for the length of the shortest word u such that $|f_u^{-1}(x)|>|x|$, if such a word exists. Based on the observation above, it is enough to find the shortest word w such that $|f_w^{-1}(x)|\neq|x|$.

Let

$$Z_0=\{x\in\mathbb{R}^n \mid |x|=0\}$$

be the set of zero weight vectors. Clearly, Z_0 is an $(n-1)$-dimensional subspace of $\mathbb{R}^n$. Let

$$Z_1=\{(r,r,\dots,r)\mid r\in\mathbb{R}\}$$

be the one-dimensional subspace of $\mathbb{R}^n$ that is generated by V. Because $V\notin Z_0$ every vector $x\in\mathbb{R}^n$ has a unique representation $x=x_0+x_1$ where $x_i\in Z_i$. As we have $f_w^{-1}(x_1)=x_1$ for every $w\in\Sigma^*$, it follows that $|f_w^{-1}(x)|\neq|x|$ if and only if $|f_w^{-1}(x_0)|\neq|x_0|=0$. This on the other hand is equivalent to $f_w^{-1}(x_0)\notin Z_0$.

Let us show that if the DFA is synchronized then for every $x_0\in Z_0\setminus\{0\}$ there exists a word w of length at most $n-1$ such that $f_w^{-1}(x_0)\notin Z_0$. First, we observe that since the DFA is synchronized there exists some word w such that $f_w^{-1}(x_0)\notin Z_0$. In fact, if w is a synchronizing word that takes the DFA into a state corresponding to a non-zero coefficient r in x_0 then $f_w^{-1}(x_0)=(r,r,\dots,r)\notin Z_0$. The rest of the claim follows directly from the following lemma:

Lemma 3. *Let U be a linear subspace of $\mathbb{R}^n$, and let $x\in U$. Let Σ be an alphabet and for every $a\in\Sigma$ let $\varphi_a:\mathbb{R}^n\to\mathbb{R}^n$ be a linear transformation. For every word $w\in\Sigma^*$ we define the linear transformation φ_w that is the composition of the linear transformations φ_a corresponding to the letters of w. Then, if there exists a word w such that $\varphi_w(x)\notin U$ then there exists such word w of length at most* $\dim U$.

Proof. Consider vector spaces $U_0\subseteq U_1\subseteq\dots$ where U_i is generated by

$$\{\varphi_w(x)\mid \text{length of } w \text{ is at most } i\}.$$

Clearly, if $U_{i+1}=U_i$ for some i then $U_j=U_i$ for every $j\geqslant i$. Namely, $U_{i+1}=U_i$ means that $\varphi_a(U_i)\subseteq U_i$ for all $a\in\Sigma$.

Let i be the smallest number such that $\varphi_w(x)\notin U$ for some w of length i, that is, the smallest i such that $U_i\nsubseteq U$. This means that in $U_0\subset U_1\subset\dots\subset U_i$ all inclusions are proper. In terms of dimensions of the vector spaces:

$$1=\dim U_0<\dim U_1<\dots<\dim U_{i-1}<\dim U_i,$$

which means that $\dim U_{i-1}\geqslant i$. But $U_{i-1}\subseteq U$ so that we also have $\dim U_{i-1}\leqslant\dim U$, which means that $i\leqslant\dim U$. □

If in the lemma we take $U=Z_0$ and $\varphi_a=f_a^{-1}$ we have the desired result. The following lemma summarizes what we have proved so far.

Lemma 4. *Assume that the DFA is synchronized. Let* $x \in \mathbb{R}^n$, $x \notin Z_1$. *Then there exists a word* w *of length at most* $n-1$ *such that* $|f_w^{-1}(x)| > |x|$.

Using this lemma we can easily prove the main theorem of this section:

Theorem 2. *If the underlying digraph* $G = (V, E)$ *of a synchronized DFA is Eulerian then there exists a synchronizing word of length at most* $(n-2)(n-1)+1$, *where* $n = |V|$ *is the number of vertices.*

Proof. The weights of vectors representing sets of vertices are integers. Therefore, it follows from Lemma 4 that for every proper subset S of V there exists a word w of length at most $n-1$ such that $|f_w^{-1}(S)| \geqslant |S| + 1$. By repeatedly applying this result i times, for any i, we see that for some word w of length at most $i \times (n-1)$ we have $|f_w^{-1}(S)| \geqslant |S| + i$, provided $|S| + i \leqslant |V|$. In particular, choosing $i = |V| - |S|$ gives us the result that for every $S \subseteq V$ there exists a word w of length at most $(|V| - |S|) \times (n-1)$ such that $f_w^{-1}(S) = V$.

Let v be a vertex such that $S = f_a^{-1}(v)$ contains at least two vertices, for some input letter a. From the previous paragraph we know that $f_w^{-1}(S) = V$ for some word w whose length is at most $(|V| - |S|)(n-1)$. Hence wa is a synchronizing word of length at most $(|V| - |S|)(n-1) + 1$. In the Eulerian case, $|V| = n$ and $|S| \geqslant 2$. □

Note that in the general (non-Eulerian) case the same reasoning gives an upper bound $(|V| - W_{\max}) \times (n-1)$ for the length of a shortest synchronizing word, where $W_{\max}$ denotes the largest weight of any single vertex, and $|V|$ is the sum of the weights of all vertices.

5. Conclusion

We have proved two well-known conjectures of symbolic dynamics and automata theory in the special case when the digraph has uniform in- and outdegrees. Intuitively, such balance in the incoming edges should make a digraph difficult to synchronize. Imbalance offers (even forces) more opportunities for synchronization: every state that has more incoming edges than there are letters in the alphabet is a place where synchronization takes place. Our results contrast this view. They indicate that perfect balance actually offers opportunities for synchronization. It seems that the “difficult” types of graphs to investigate for a general proof of the road coloring and the Černý conjectures are digraphs that have nearly—but not fully—balanced indegrees.

References

[1] R.L. Adler, L.W. Goodwyn, B. Weiss, Equivalence of topological Markov shifts, Israel J. Math. 27 (1977) 49–63.
[2] R.L. Adler, B. Weiss, Similarity of automorphisms of the torus, Mem. Amer. Math. Soc. 98 (1970).
[3] A. Carbone, Cycles of relatively prime length and the road coloring problem, Israel J. Math. 123 (2001) 303–316.

[4] J. Černý, K. Poznámka, homogénnym experimenton s konečnými automatmi, Mat. Fyz. SAV 14 (1964) 208–215.
[5] K. Culik, J. Karhumäki, J. Kari, Synchronized automata and the road coloring problem, TUCS Technical Report 323, Turku Centere for Computer Science, University of Turku, 1999.
[6] J. Friedman, On the road coloring problem, Proc. Amer. Math. Soc. 110 (1990) 1133–1135.
[7] W. Göhring, Minimal initializing word: a contribution to Černý's conjecture J. Automata, Languages Combin. 2 (1997) 209–226.
[8] N. Jonoska, S. Suen, Monocyclic decomposition of graphs and the road coloring problem, Congr. Numer. 110 (1995) 201–209.
[9] A. Mateescu, A. Salomaa, Many-valued truth functions, Černý's conjecture and road coloring, EATCS Bull. 68 (1999) 134–150.
[10] G.L. O'Brien, The road coloring problem, Israel J. Math. 39 (1981) 145–154.
[11] D. Perrin, M.P. Schützenberger, Synchronizing prefix codes and automata, and the road coloring problem, in: P. Walters (Ed.), Symbolic Dynamics and Applications, Contemporary Mathematics, Vol. 135, American Mathematical Society, Providence, RI, 1992, pp. 295–318.
[12] J.-E. Pin, Utilisation de l'algèbre linéaire en théorie des automates, Act. Collouq. AFCET-SMF Math. Appl. II (1972) 85–92.
[13] J.-E. Pin, Le problème de la synchronisation, contribution à l'étudia de la conjecture de Černý, Thèse, 3e cycle, Université Paris, 1978.
[14] J.-E. Pin, On two combinatorial problems arising from automata theory, Ann. Discrete Math. 17 (1983) 535–548.
[15] A. Salomaa, Synchronization of finite automata. Contributions to an old problem, Turku Centere for Computer Science, Technical Report, Vol. 365, 2000.
[16] D.B. West, Introduction to Graph Theory, Prentice-Hall, Englewood Cliffs, NJ, 1996.