Cycles of relatively prime length and the Road Coloring Problem

A. Carbone

March 7, 1999

Abstract

We give a partial answer to the *road coloring problem*, a purely graph-theoretical question with applications in both symbolic dynamics and automata theory. The question is whether for any positive integer k and for any aperiodic and strongly connected graph G with all vertices of out-degree k, we can label G with symbols in an alphabet of k letters so that all the edges going out from a vertex take a different label and all paths in G presenting a word W terminate at the same vertex, for some W. Any *aperiodic* graph G contains a set S of cycles where the greater common divisor of the lengths equals 1. We establish some geometrical conditions on S to ensure the existence of a synchronizing coloring.

1 Some background

Let G be a directed graph with set of vertices V and set of edges E. The out-degree of the nodes of the graph is k. If H is a subgraph of G, then the sets of vertices and edges of H will be denoted V_H and E_H respectively. Two subgraphs H and K of G are *disjoint* if $E_H \cap E_K = \emptyset$ and they are *strongly disjoint* if $V_H \cap V_K = \emptyset$.

The graph G is *strongly connected* if any vertex can reach any other vertex by a path in G; G is *aperiodic* if V cannot be partitioned into $d > 1$ sets $V_1, \ldots, V_d = V_0$ such that all edges (u, v) with $u \in V_i$ have $v \in V_{i+1}$. We say that G has a *coloring* if there is a labelling of the edges of G with symbols in $\{a_0, a_1, a_2 \ldots a_{k-1}\}$ such that all edges going out from a node are labelled differently.

Given any coloring of G we define maps $a_i : V \to V$ (for $i = 0 \ldots i-1$) by $a_i(x) = y$ if and only if there is an edge labelled a_i going from x to y in G. We say that G has a *synchronizing coloring* if there is a composition of the maps a_i which maps V into a single vertex.

The *road coloring problem* is to determine whether any aperiodic and strongly connected graph G has a synchronizing coloring. This problem is stated explicitly in [AGW77] in the context of symbolic dynamics and originates in [AW70]. It is generally believed that the question has a positive answer and several partial solutions have been found. In [OBr81] it is shown that a graph with no multiple edges (i.e. no distinct edges in G have the same source and the same target) and with a simple cycle of prime length has a synchronizing coloring. In [F90] it is shown that a graph of out-degree 2 with a simple cycle of length relatively prime to the weight of the graph (i.e. the sum of the components of an integer Perron left eigenvector chosen with relatively prime components) has a synchronizing coloring. Another special case, proven in [PS85], is that an aperiodic graph of out-degree k with all vertices of in-degree 1 except one (these graphs are trees where all leaves merge with the root), has a synchronizing coloring. In [JS95] it is shown that a graph of out-degree k which is decomposable in k disjoint monochromatic subgraphs containing exactly one cycle, has a synchronizing coloring if the greater common divisor of the lengths of the monochromatic cycles equals 1. Besides the results that we have listed, we would like to mention a couple of related points. The first is a result that appears in [AGW77]: let M be the adjacency matrix of G and let n be an integer such that M^n has all positive coefficients; for $k > 0$, let $G^{(k)}$ denote the graph having as vertices the paths of length k in G and as edges the pairs (s, t) with $s = (s_1, \dots, s_k)$, $t = (s_2, \dots, s_k, s_{k+1})$. Then $G^{(2n)}$ has a synchronizing coloring. In the language of symbolic dynamics, this means that the system of finite type associated with G is conjugate to one that has a synchronizing coloring. The second point is an open problem known as the Cerny's conjecture. It states that any graph G of n nodes with synchronizing coloring has a synchronizing word of length at most $(n-1)^2$. It is simple to show that there exists a cubic bound. In [PS85] one finds an example showing that the quadratic bound above cannot be improved.

The road coloring problem is a basic question in graph theory but has fundamental applications in automata theory: a synchronizing coloring makes the behavior of an automaton resistant against *input errors* since, after the detection of an error, a synchronizing word can reset the automaton back to its original state, as if no error had occurred; also, in the *identification* problem of automata, a synchronizing word can put an unknown automaton in a prescribed state and check suitable properties of this state. (For early works in this area, see [P77] and [Pi78].)

In this paper we give a partial answer to the problem. Namely, we look at a set S of cycles in G with greater common divisor of their lengths equal to 1. For any *aperiodic* graph G this set of cycles always exists, and in fact, there might exist several of them. In Theorems 6 and 8 we give sufficient geometrical conditions on S to ensure the existence of a synchronizing coloring. Theorems 3 and 5 are consequences of Theorem 6, but we shall present them first to introduce the ideas which Theorem 6 is based on. Theorem 3 implies, as a corollary, the result in [JS95].

We thank Danièle Beauquier for some comments on a preliminary version of this paper and Misha Gromov for bringing this problem to our attention.

2 Looping back and forth

A map defined over a colored graph G is intended to be a composition of the maps a_i, where $i = 0, \ldots k-1$. When we refer to a map we will always intend it to be defined over a labelled graph. In general, a map is defined from V to V but at our convenience we might indicate the range of the map to be a subset of the set of vertices V. An *extension* of a map h is a map lh obtained by composing h with some map l which is defined over the *same* graph of h.

Proposition 1 *Let G be a connected and directed graph whose nodes have out-degree k and let C be a cycle in it of length q. Suppose G being colored and C being monochromatic. Any map $h : V \to V_C$ defined over G can be extended to a map $h' : V \to V_C$ such that $|h'(V)|$ divides q. In particular, the map h' induces a partition of V_C in $|h'(V)|$ equivalence classes.*

The first part of the statement, i.e. the existence of a map h' such that $|h'(V)|$ divides q, is also proved in [OBr81].

Proof. Suppose that the edges of the cycle C are labelled with the symbol a. Let $h : V \to V_C$ be a map defined over G (notice that the existence of a map with image in V_C implies that G is a *connected* graph) and let a^j be the map defined by composing j times the map a, for some $j \geq 1$. The map a^j induces $h(V)$ to shift j times along C.

First notice that V is divided through h in partitions of the form

$$[v] = \{v \in V \ : \ h(v) = h(u)\}$$

where each $v \in h(V)$ should lie in a different equivalent class by definition.

Let $Y_1, \ldots, Y_r$ be the equivalence classes induced by h such that $Y_i \cap V_C = \emptyset$. It might be that there are no such classes. But, if there are, then we claim that we can always extend h to a function g in such a way that all the equivalence classes induced by g contain at least a node in V_C. Note that $r < |h(V)|$ because there is always at least one equivalence class that contains a node in V_C. Therefore, let us suppose that $r \geq 1$ and let us look at the images $h(u_1), \ldots, h(u_m)$ of V under h, where $[u_1], \ldots, [u_m]$ are the equivalence classes of V. Since $r > 1$, at least one of the equivalence classes does not contain any node in V_C. Therefore there should exist two equivalence classes $[u_i], [u_j]$, for $i, j = 1 \ldots m$ and $i \neq j$, such that $h(h(u_i)) = h(h(u_j))$. If this was not the case, then h would induce a permutation of $h(u_1), \ldots, h(u_m)$ and the equivalence classes of hh would be the same as the equivalence classes of h. But this is impossible because $h(u_1), \ldots, h(u_m) \in V_C$ and by assumption we know that at least one of these equivalence classes does not contain any node in V_C.

Hence, by applying h to $h(V)$ we collapse $[u_i]$ and $[u_j]$, and we decrease the number of equivalence classes of V. (In particular, *several* equivalence classes might collapse with the application of h.) If the number of equivalence classes with no element in V_C is ≥ 1, then we apply the reasoning again until we find a j for which h^j induces a partition of V where all equivalence classes contain a representative in V_C. This is guaranteed by the fact that $|h^{i+1}(V)| < |h^i(V)|$ at each iteration i. We let g be h^j. Clearly, g induces a partition of V_C in $|g(V)|$ equivalence classes.

If $|g(V)|$ divides q we are done and we let h' be the map g. Otherwise, there exists an equivalence class X which contains at least $\lceil q/|g(V)| \rceil$ nodes of V_C, since $|g(V)|$ is not a divisor of q.

For $i = 1 \ldots q$ and $v \in V$ we have $a^i g(v) \in X$ for at least $\lceil q/|g(V)| \rceil$ many i's. In particular, the nodes in the image of g while shifted along C will belong to X at least $\lceil q/|g(V)| \rceil \cdot |g(V)|$ times.

Since $\lceil q/|g(V)| \rceil \cdot |g(V)| > q$, then for some $[v], [w]$ and some $i = 1 \ldots q$, there will be two distinct images $g(v), g(w)$ such that $g(v) \neq g(w)$ and $a^i g(v), a^i g(w) \in X$. But this means that $ha^i g(v) = ha^i g(w)$.

Let us consider the map $ha^i g$. It is clear that $ha^i g(V) \subset V_C$, that $|ha^i g(V)| < |g(V)|$ and that $ha^i g$ induces a partition of V_C in $|ha^i g(V)|$ equivalence classes. If $ha^i g$ satisfies the conclusions of the statement we will take it to be h', otherwise without loss of generality we call it g and re-iterate the construction until the conditions of the statement are satisfied.

$\square$

We formulate now a basic definition. Let A and B be two sets. The symbol A/B denotes the *difference* between A and B.

Definition 2 *Let C be a cycle in G. A C-cover relative to $X \subseteq V$ is a connected subgraph G' of G which satisfies the following properties*
1. $X \subset V_{G'}$ and G' contains C, and
2. $\{x \in V_{G'} \mid$ in-degree$(x) = 0$ in $G'\} = X/V_C$, and
3. for all $x \in V_{G'}$, out-degree$(x) = 1$.

From the definition, it follows immediately that C is the only cycle in G', and that given any $x_0 \in V_C$, for all $x \in X$ there is a unique path in G' from x to x_0 which passes through x_0 only once. In particular, this path has length $< n$, where n is the order of the graph G (here, we do not allow paths to loop around C).

If a C-cover is relative to V then we call it *complete*. Given any strongly connected graph G and any cycle C in it, there is always a complete C-cover for G. Take for instance the subgraph of G whose edges belong either to C or to a chosen minimal path from a node of V to C. (From any node $v \in V$, we choose exactly one path to C. There might be several of them.) There are many different C-covers and this is just one of them. In the following we will be interested to look at C-covers relative to sets of nodes $V_{C'}$, where C' is some cycle in G. We always think of C as being disjoint from C'.

Let us say that the numbers $a, b, c, \ldots, k$ are *relatively prime*, if there is no number but 1 that divides all of them. We shall use the notation $(a, b, \ldots, k) = 1$.

Theorem 3 *Let $\mathcal{L} = \{a_0, \ldots, a_{k-1}\}$ be a language of k letters and G be a directed graph whose nodes have out-degree k. Suppose that G contains h disjoint cycles $C_0, C_1, \ldots C_h$ of relatively prime lengths, for $1 \leq h \leq k$, and that there exists a complete C_0-cover and a C_i-cover relative to V_{C_0}, for each $i = 1 \ldots h$, which are pairwise disjoint. Then G has a synchronizing coloring.*

The idea of the proof is to construct a synchronizing word for the graph G by going back and forth from C_0 to $C_1, \ldots C_h$ and by looping around these cycles in some appropriate way. The conditions imposed on the C_i-covers ensure that this is possible.

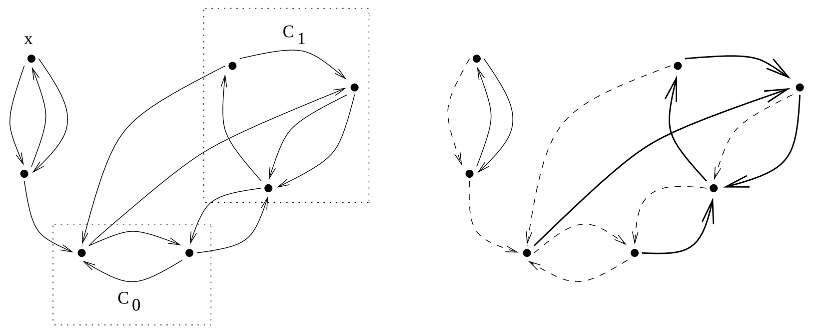
Proof. Let $q_0, q_1, \ldots, q_h$ be the lengths of the cycles $C_0, C_1, \ldots C_h$ in G. We color a_0 the edges belonging to the C_0-cover and we color with a_l, for $l \leq h$, the edges belonging to the C_l-cover. Since the subgraphs are disjoint there is no incompatibility of color assignment. We color all other edges in G in such a way that each edge going out from a node will have a different color assigned to it. In general there will be many ways to assign the remaining colors. Any one of them is fine.

We want to show that there is a synchronizing map for G and we shall build this map by steps. We start by applying to V the map a_0^n, where n is the order of G. After n shifts along edges labelled by a_i we surely end-up into some node of V_{C_0}. This is because any path from $x \in V$ to a node in V_{C_0} has length $< n$, as we noticed in a remark after Definition 2. Hence, $a_0^n(V) \subset V_{C_0}$. Moreover, $V_{C_0} \subset a_0^n(V)$, because the q_0 nodes in V_{C_0} are shifted by a_0^n into q_0 distinct nodes in V_{C_0}. From this we imply that $a_0^n(V) = V_{C_0}$ and that $|a_0^n(V)| = q_0$.

By hypothesis there is a cycle C_i in G whose length q_i does not divide q_0. We extend a_0^n to the map $a_i^n a_0^n$ such that $a_i^n a_0^n(V) \subset V_{C_i}$ (the argument to use to infer the inclusion is the same as above). By Proposition 1 there is an extension h of $a_i^n a_0^n$ such that $h(V) \subset V_{C_i}$ and $|h(V)|$ is a divisor of q_i. This means also that $|h(V)| < |a_0^n(V)|$. If $|h(V)| = 1$ then we are done. Otherwise, we consider the cycle C_j whose length q_j is not divisible by $|h(V)|$ (such a value q_j exists because $(q_0, q_1, \ldots, q_h) = 1$ by hypothesis) and we repeat the reasoning described above until we find $|h(V)| = 1$, for some h.

□

In Theorem 3 we did not explicitly ask the graph G to be strongly connected. In fact, there are graphs that satisfy the conditions of the theorem and which are not strongly connected. Take for instance the graph G below (on the left)



where the node x on the top-left is not reached by any other node on the right. This graph contains two cycles C_0 and C_1 (illustrated in the figure) of relatively prime length. The graph on the right illustrates the complete C_0-cover of G (in dotted lines) and the C_1-cover relative to C_0 (in thicker lines). Notice that there are two edges on the left of the graph which do not belong to any cover. By Theorem 3 the graph has a synchronizing word.

Given k cycles $C_0, \ldots, C_{k-1}$ in G, we say that a *monocyclic decomposition* of a graph G with nodes of out-degree k is a set of k disjoint complete C_i-covers, for $i = 0 \ldots k-1$. It is easy to check that the union of these covers is G.

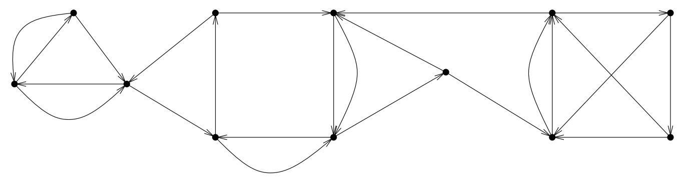
Corollary 4 (Jonoska-Suen [JS95]) *Suppose that G has a monocyclic decomposition relative to the cycles $C_0, \ldots, C_{k-1}$. Suppose also that these cycles have relatively prime lengths. Then G has a synchronizing coloring.*

Proof. The existence of a monocyclic decomposition of G (which, by definition, is a set of k complete coverings of G) implies the existence of $k-1$ coverings relative to C_0. In fact, let each C_i-cover relative to C_0 be the subgraph of the complete C_i-cover which has V_{C_0} as vertices of in-degree 0 and has as edges only those edges which form directed paths from nodes in V_{C_0} to nodes in V_{C_i}, for $i = 1 \ldots k-1$.

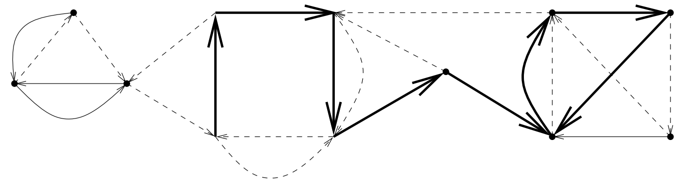
If we consider the C_0-cover of the monocyclic decomposition to be the complete C_0-cover required by the hypothesis of Theorem 3, all conditions are satisfied and G has a synchronizing coloring.

□

To compare the strength of Theorem 3 to the corollary, let us consider the following example (presented in [JS95])

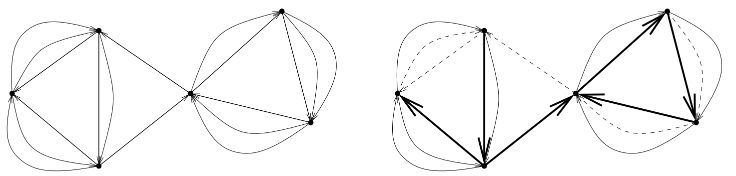


which does *not* have monocyclic decomposition. This is easy to see by noticing that there is a node in the left hand-side of the graph which has only one out-going edge directed towards the right hand-side of the graph. Nevertheless, the graph satisfies the conditions of Theorem 3 as illustrated below



where one can see two cycles C_0 and C_1 (of length 2 and 3, respectively), the complete covering relative to the cycle C_0 which is described by dotted edges, and the C_1-cover relative to C_0 which is described by thick edges. The graph has synchronizing coloring.

Another direction that illustrates the strength of the assumptions in Theorem 3 is described by the following graph with nodes of out-degree 3



where it is sufficient to determine the existence of only *two* covers (as indicated in the graph on the right) instead of the three covers required by the corollary, to assert the colorability of the graph.

3 Looping along a tree-like order of cycles

The statement of Theorem 3 can be generalized by noticing that the C_i-covers need not all be relative to V_{C_0}. In fact it is enough to require a *tree-like order* between the

C_i's (where the root is labelled by C_0) in the sense explained by the following example. Suppose to have five cycles C_0, C_1, C_2, C_3, C_4 and a tree-like order between them which fixes C_0 as the father of C_1, C_1 as the father of C_2, and C_2 as the father of both C_3 and C_4. For us, the word *father* refers to the "immediate predecessor" of a node in the tree-like order, and the symbol $C \succ D$ denotes that C is the father of D. In Theorem 5 we show that the existence of a C_1-cover relative to V_{C_0}, a C_2-cover relative to V_{C_1}, a C_3-cover relative to V_{C_2} and a C_4-cover relative to V_{C_2} implies the colorability of G.

For convenience, we refer to a tree-like order of the "indexes" of the C_i's. Namely, we think of the set $\{0, \ldots, h\}$ as being ordered as a tree: each node of the tree is labelled by a different value in the set and the root is labelled 0.

Theorem 5 *Let $\mathcal{L} = \{a_0, \ldots, a_{k-1}\}$ be a language of k letters and G be a directed graph whose nodes have out-degree k. Suppose that G contains h disjoint cycles $C_0, C_1, \ldots C_h$ of relatively prime lengths (where $1 \leq h \leq k$), that there exists a complete C_0-cover and that, there is a tree-like order of the indexes $\{0, 1, 2, \ldots, h\}$ such that, for each $i = 1 \ldots h$, there is a C_i-cover which is relative to V_{C_j}, for $j \succ i$ in the order. Suppose also that the C_i-covers are pairwise disjoint. Then G has a synchronizing coloring.*

Proof. The proof of this theorem follows the same lines as the proof of Theorem 3. The only difference consists in noticing that to pass from C_i to C_j we need to consider those paths which pass through *all* cycles of index l lying between i and j in the tree-like order of $\{0, 1, 2, \ldots, h\}$. Suppose this order to be $i = j_0 \succ j_1 \succ \ldots \succ j_s = j$. For each j_r we know that there is a way to go from C_{j_r} to $C_{j_{r+1}}$ through the map $a^n_{j_{r+1}}$, hence, by composing the map $a^n_{j_1}$ with $a^n_{j_2}$ and so on, we shall end-up into C_j as wished. In case $j = j_0 \succ j_1 \succ \ldots \succ j_s = i$, then to go from C_i to C_j, we should pass through the cycle C_0. Namely, we should consider the two orderings $i = l_0 \succ l_1 \succ \ldots \succ l_n = 0$ and $0 = l_{n+1} \succ l_{n+2} \succ \ldots \succ l_m = j$ and compose the maps $a^n_{l_r}$'s as indicated above.

□

To see that Theorem 3 is a consequence of Theorem 5, notice that Theorem 3 considered in some implicit way, the tree-like order defined by $C_0 \succ C_i$, for all $i = 1 \ldots h$. Because of this, to go from C_j to C_i was possible by passing through C_0 and by using the map $a^n_i a^n_0$.

In the proofs of Theorems 3 and 5, the synchronizing coloring of the graph G is built by assigning different colors to different covers of G. We could assign the *same* color to *strongly* disjoint covers and still obtain a synchronizing coloring of the graph. This observation leads to a statement where we do not require anymore the number of cycles of relatively prime lengths to be bounded by the cardinality k of the language. In fact, the number of cycles with relatively prime lengths might be much larger than k.

Theorem 6 *Let $\mathcal{L}$ be a language of k letters and G be a directed graph whose nodes have out-degree k. Let $C_0, C_1, \ldots, C_m$ be cycles in G of relatively prime lengths. Suppose that there exists a complete C_0-cover for G and that, there is a tree-like order of the indexes $\{0, 1, 2, \ldots, m\}$ such that, for each $i = 1 \ldots m$, there is a C_i-cover which is relative to V_{C_j}, for $j \succ i$ in the order. Suppose that all C_i-covers are pairwise disjoint and also that $C_1, \ldots, C_m$ can be grouped in h disjoint sets $S_1, \ldots, S_h$, where $1 \leq h < k$, and that for all r, where $1 \leq r < h$, and all pairs of cycles $C_i, C_l \in S_r$, the C_i-cover and the C_j-cover are strongly disjoint. Then G has a synchronizing coloring.*

Proof. The proof follows the same lines of the proof of Theorem 5. The only difference consists in the assignment of the colors to the edges: we assign the color a_i to the edges lying in a C-cover if $C \in S_i$, and we assign the color a_0 to the edges lying in the C_0-cover; we color all other edges in G in such a way that each edge going out from a node will have a different color assigned to it. In general there will be many ways to assign the remaining colors. Any one of them is fine.

To check that there is no conflict in the labelling of G, let x be a node in G. The node either belongs to a cover or not. If the node x does not belong to a cover, then there is only one out-going edge colored a_0 which is forced by the assignment. If it belongs to a cover, say the C_i-cover, then we claim that there is *exactly* one out-going edge from x which is labelled by a_i. This is because all C-covers, for C belonging to the same set S_i, are strictly disjoint and therefore x can belong to only one of them. (Notice also that if a C_j-cover is relative to V_{C_i}, then the C_j-cover and the C_i-cover are not strongly disjoint, and therefore C_i and C_j must belong to different sets and have different colors by construction, as well as their covers.) The node x lying in the C_i-cover might also belong to some C-cover, where $C \in S_j$ and $j \neq i$. In this case, there is an edge going out from x which is labelled a_j. In fact, there is *exactly* one such an edge, for the same reasons as above. Also, there is an out-going edge labelled a_0 which belongs to the C_0-cover. No color for the other out-going edges is forced by the construction.

□

To see that Theorem 5 follows from Theorem 6, let each set S_i be a singleton containing the cycle C_i, for $i = 1, \ldots, h$.

4 Looping between sets of cycles

The next definition introduces a weak notion of covering.

Definition 7 *Let $C_1, \ldots, C_n$ be strongly disjoint cycles in G and $x_1, \ldots x_n$ be nodes in $C_1, \ldots, C_n$ respectively. A $C_1, \ldots, C_n$-cover relative to $X \subseteq V$ is a connected subgraph*

G' of G which satisfies the following properties

1. $X \subset V_{G'}$ and G' contains $C_1, \ldots, C_n$, and
2. $\{x \in V_{G'} \mid$ in-degree$(x) = 0$ in $G'\} = X/V_{C_1} \cup \ldots \cup V_{C_n}$, and
3. the out-degree of each $x \in V_{G'}$ is 1, and
4. for all $i = 1 \ldots n$, there is a node $v_i \in X$ and a path in G' from it to x_i.

As for Definition 2, Definition 7 implies that if there is a path from x to y in G' that passes through y only once, then this path should be unique. Also, notice that once a path reaches a cycle, then it cannot leave it anymore. This fact implies, together with condition 4, that the number of strongly disjoint cycles $n \leq |X|$.

Let S be a set of cycles $C_1, \ldots, C_n$. We shall refer to the $C_1, \ldots, C_n$-cover as S-cover for short, and we shall use the notation V_S to refer to the set of nodes $V_{C_1} \cup \ldots \cup V_{C_n}$.

We say that two numbers are *coprime* if $(a, b) = 1$. We also say that the numbers $a, b, \ldots, k$ are coprime if every two of them are coprime. To say this is to say much more than to say $(a, b, \ldots, k) = 1$.

Theorem 8 *Let $\mathcal{L} = \{a_0, \ldots, a_{k-1}\}$ be a language of k letters and G be a directed graph whose nodes have out-degree k. Suppose that G contains a cycle C_0 and h disjoint sets of strongly disjoint cycles $S_i = \{C_{i,1}, \ldots, C_{i,r_i}\}$, for $1 \leq i \leq h < k$, such that the following properties are satisfied*
1. C_0 is disjoint from the cycles in S_i, and
2. there exists a complete C_0-cover for G, and
3. there is a tree-like order of the indexes $\{0, \ldots, h\}$ such that, for all $i = 1 \ldots h$, there exists a S_i-cover relative to V_{S_j} for $j \succ i$ in the order, and
4. all covers are pairwise disjoint, and
5. there are cycles $C_0, C_{1,j_1}, \ldots, C_{h,j_h}$ (for some index $j_1, \ldots, j_h$) which have relatively prime lengths, and
6. for each $i = 1 \ldots h$, the lengths of the cycles in S_i are coprime.

If G is colored in such a way that each cover be monochromatic, then any map $h : V \to V_{C_0}$ with the property that for each set S_i and each pair of indexes j, l with $j \neq l$ and $1 \leq j, l \leq r_i$

$$\exists v \in V_{C_{i,j}} \exists w \in V_{C_{i,l}}.\ h(v) = h(w)$$

can be extended to a synchronizing coloring map.

The proof needs the Chinese Remainder Theorem which we state here with a notation which is convenient to our purposes.

The Chinese Remainder Theorem *Let $k_1, \ldots, k_n$ be positive integers which are coprime, and let $x_1, \ldots, x_n$ be integers such that $0 \leq x_i < k_i$. Then there exists a positive integer $r \leq k_1 \cdot k_2 \cdot \ldots \cdot k_n$ such that*

$$r \; mod \; k_i = x_i \qquad \text{for all } i = 1 \ldots n$$

Proof. Let G be a colored graph and h be a map which satisfy the condition in the statement. We want to show that h can be extended to a synchronizing map. The argument is more subtle here than in the proof of Theorem 5 but the idea remains the same. We shall describe a way to extend h to a map $h' : V \to V_{C_0}$ by steps so that $|h(V)| > |h'(V)|$. After finitely many steps we shall end-up with a constant map, i.e. a synchronizing map.

Let $q_0, q_1, \ldots, q_h$ be the lengths of the cycles $C_0, C_{1,j_1}, \ldots, C_{h,j_h}$ which, by condition 5, are relatively prime. Let c_i be the color associated to the S_i-cover, where $c_i \in \{a_0, \ldots, a_{k-1}\}$. (Notice that two strongly disjoint covers could be colored with the same color.)

As remarked in the proof of Proposition 1, any map $g : V \to X$ where $X \subset V$ induces a partition of V in equivalence classes of the form

$$[u] \;=\; \{v \in V \;:\; g(v) = g(u)\}$$

where each $v \in g(V)$ should lie in a different equivalent class. In particular, the map h and its extensions induce such partitions and we will use this fact all along this proof.

Our construction (of a map $h' : V \to V_{C_0}$ such that $|h(V)| > |h'(V)|$) is determined by two main cases which depend on whether $|h(V)|$ divides q_0 or not.

If $|h(V)|$ does not divide q_0 then we apply Proposition 1 and extend h to a map $h' : V \to V_{C_0}$ where $|h'(V)|$ divides q_0. Clearly $|h(V)| > |h'(V)|$ and we are done.

If $|h(V)|$ divides q_0, then it does not divide q_i, for some $i = 1 \ldots h$, since $(q_0, \ldots, q_h) = 1$. In this case, let $0 = i_0 \succ i_1 \succ i_2 \succ \ldots \succ i_k = i$ be the relation between the indexes 0 and i, induced by the tree-like order of $\{0, 1, 2, \ldots, h\}$ (see condition 3). We claim that

$$\exists w_0 \in V_{C_0} \exists n_1 \geq 0 \exists n_2 \geq 0 \ldots \exists n_k \geq 0 \;. \quad c_{i_k}^{n_k} c_{i_{k-1}}^{n_{k-1}} \ldots c_{i_2}^{n_2} c_{i_1}^{n_1}(w_0) \in V_{C_{i,j_i}}$$

To see this, let x be a node of $V_{C_{i,j_i}}$ $(= V_{C_{i,j_{i_k}}})$ and apply condition 4 of Definition 7 to find an element y in $V_{S_{i_{k-1}}}$ from which there is a path to x. Notice that there is a $n_k \geq 0$ such that $c_{i_k}^{n_k}(y) = x$, because the S_{i_k}-cover relative to $V_{S_{i_{k-1}}}$ is monochromatic by hypothesis. By applying condition 4 of Definition 7 to the $S_{i_{k-1}}$-cover relative to

$V_{S_{i_{k-2}}}$, we find a node z in $V_{S_{i_{k-2}}}$ such that there is a path from z to y and an integer $n_{k-1} \geq 0$ such that $c_{i_{k-1}}^{n_{k-1}}(z) = y$. By repeating the argument, we find a node $w_0 \in V_{C_0}$ and integers $n_{k-2}, n_{k-3}, \ldots, n_2, n_1 \geq 0$ such that

$$c_{i_k}^{n_k} c_{i_{k-1}}^{n_{k-1}} \ldots c_{i_2}^{n_2} c_{i_1}^{n_1}(w_0) \in V_{C_{i,j_i}}.$$

We extend h to the map $g : V \to V_{S_i}$ defined as $c_{i_k}^{n_k} c_{i_{k-1}}^{n_{k-1}} \ldots c_{i_2}^{n_2} c_{i_1}^{n_1} c_0^{n_0} h$, where n_0 allows to shift the image $h(V)$ in such a way that $w_0 \in c_0^{n_0} h(V)$. (Here, it is important that C_0 be a *cycle* instead of a *set* of cycles, and this is because we need to guarantee that w_0 lies in the image of g. If C_0 was replaced by a set of cycles S_0 in the statement of the theorem and if $w_0 \in C$ for $C \in S_0$, then we could have that no node in V_C would belong to $h(V)$ and therefore we could not be able to extend h in a suitable way. Moreover, even if we would explicitly ask for this condition to be satisfied in the statement, we would not be able to preserve it on the following steps of the construction.)

There are two cases that we shall consider.

First, suppose that the image of $g : V \to V_{S_i}$ lies in several cycles of S_i. Formally speaking we ask that $g(V) \subset V_{C_1} \cup \ldots \cup V_{C_n}$ for $C_1, \ldots, C_n \in S_i$ and that $g(V) \not\subset V_{C_{i,j_i}}$ (think of C_{i,j_i} as being one of the cycles C_i for $1 = 1 \ldots n$). We look whether there are two (or more) values in the image $g(V)$ which belong to the same equivalence class induced by h. If these values exist, then we know that $|hg(V)| < |g(V)|$ and we are done. If they do not exist then by the Chinese Remainder Theorem there is a r such that $c_i^r g(V)$ contains at least two values which belong to the same equivalence class induced by h. We shall consider the extension $hc_i^r g$ and we are done (since $|hc_i^r g(V)| < |c_i^r g(V)|$).

To see how the Chinese Remainder Theorem helps, let $C_1, \ldots, C_n$ be the cycles in S_i where the image of g ends-up. Let $k_0, \ldots, k_n$ be the lengths of these cycles. By hypothesis, there is an equivalence class induced by h (and more precisely by h) which contains at least two nodes lying in two distinct sets V_{C_j}, V_{C_l}, for $1 \leq j, l \leq n$. In fact, the hypothesis says that for *any* pair of indexes j, l such that $j \neq l$ and $1 \leq j, l \leq n$, there are two nodes $x_j \in V_{C_j}$ and $x_l \in V_{C_l}$ such that $h(x_j) = h(x_l)$ (and hence $g(x_j) = g(x_l)$). Let us fix a pair j, l and let us imagine the nodes of the cycles C_i, for $i \in \{j, l\}$, to be numbered from 0 to $k_i - 1$ (following a clockwise orientation) in such a way that 0 coincides with $g(x_j)$ in C_j and that it coincides with $g(x_l)$ in C_l. By the Chinese Remainder Theorem we know that there is a $r \leq k_j \cdot k_l$ such that after r shifts (by looping around the cycles C_j and C_l maybe several times) we end-up into x_j and x_l. This explains the use of the Chinese Remainder Theorem.

Suppose now that $g(V) \subset V_{C_{i,j_i}}$. If $|g(V)| < |h(V)|$ then we let h' to be the map $hg : V \to V_{C_0}$ and we are done. Otherwise, we know that $g(V)$ does not divide q_i.

Hence, we can apply Proposition 1 to extend g to a map $h'' : V \to V_{C_i}$ where $|h''(V)|$ divides q_i. Clearly $|g(V)| > |h''(V)|$. We let h' be the map hh'' and we are done.

This concludes the construction. The argument should be iterated until a constant map is found.

□

References

[AGW77] R.L. Adler, L.W. Goodwyn and B. Weiss. Equivalence of topological Markov shifts. *Israel Journal of Mathematics*, 27:49–63, 1977.

[AW70] R.L. Adler and B. Weiss. Similarity of automorphisms of the torus. *Memoires of the American Mathematical Society*, n.98, Providence, RI, 1970.

[F90] J. Friedman. On the colorability problem. *Proceedings of the American Mathematical Society*, 110:1133–1135, 1990.

[JS95] N. Jonoska and S. Suen. Monocyclic decomposition of graphs and the road coloring problem. *Congressum Numerantium*, 110:201–209, 1995.

[OBr81] G.L. O'Brien. The road coloring problem. *Israel Journal of Mathematics*, 39:145–154, 1981.

[P77] D. Perrin. Codes asynchrones. *Bull. Soc. Math. de France*, 105:385–404, 1977.

[PS85] D. Perrin and M.P. Schützenberger. Synchronizing prefix codes and automata, and the road coloring problem. In *Symbolic Dynamics and Applications*, Contemporary Mathematics, Amer. Math. Soc., 135:295–318, 1992.

[Pi78] J. E. Pin. *Le problème de la synchronisation. Contribution à l'étude de la conjecture de Cerny.* Thèse de doctorat. Université de Paris 6, 1978.

A. Carbone
Mathématiques/Informatique
Université de Paris XII
61 Avenue du Général de Gaulle
94010 Créteil CEDEX
FRANCE