The Road Coloring Problem

A.N. Trahtman*†

Israel Journal of Mathematics, 172, N 1, 51-60, 2009

Bar-Ilan University, Dep. of Math., 52900, Ramat Gan, Israel

Abstract

A synchronizing word of a deterministic automaton is a word in the alphabet of colors (considered as letters) of its edges that maps the automaton to a single state. A coloring of edges of a directed graph is synchronizing if the coloring turns the graph into a deterministic finite automaton possessing a synchronizing word.

The road coloring problem is the problem of synchronizing coloring of a directed finite strongly connected graph with constant outdegree of all its vertices if the greatest common divisor of lengths of all its cycles is one. The problem was posed by Adler, Goodwyn and Weiss over 30 years ago and evoked noticeable interest among the specialists in the theory of graphs, deterministic automata and symbolic dynamics.

The positive solution of the road coloring problem is presented.

Keywords: road coloring problem, graph, deterministic finite automaton, synchronization.

Introduction

The road coloring problem originates in [2] and was stated explicitly in [1] for a strongly connected directed finite graph with constant outdegree of all its vertices where the greatest common divisor (gcd) of lengths of all its cycles is one. The edges of the graph are unlabeled. The task is to find a labelling of the edges that turns the graph into a deterministic finite automaton possessing a synchronizing word. So the road coloring problem is connected with the problem of existence of synchronizing word for deterministic complete finite automaton.

The condition on gcd is necessary [1], [5]. It can be replaced by the equivalent property that there does not exist a partition of the set of vertices on subsets $V_1, V_2, ..., V_k = V_1$ $(k > 1)$ such that every edge which begins in V_i has its end in V_{i+1} [5], [13]. The outdegree of the vertex can be considered also as the size of an alphabet where the letters denote colors.

*Email: trakht@macs.biu.ac.il

†http://www.cs.biu.ac.il/∼trakht

The road coloring problem is important in automata theory: a synchronizing coloring makes the behavior of an automaton resistant against input errors since, after detection of an error, a synchronizing word can reset the automaton back to its original state, as if no error had occurred. The problem appeared first in the context of symbolic dynamics and is important also in this area.

Together with the Černy conjecture [15], [16], the road coloring problem belongs to the most fascinating problems in the theory of finite automata. The problem is discussed even in "Wikipedia" - the popular Internet Encyclopedia. However, at the same time it was considered as a "notorious open problem" [11], [5] and "unfeasible" [8].

For some positive results in this area see [3], [4], [6], [7], [8], [9], [10], [13], [14]; a detailed history of investigations can be found in [4].

The concept of Friedman [6] of the weight of a vertex and the concept of a stable pair of states [5], [10] of Culik, Karhumaki and Kari with corresponding results and consequences are used below.

We prove that the road coloring problem has a positive solution. So a finite directed strongly connected graph with constant outdegree of all vertices and with gcd of the lengths of all its cycles equal to one has a synchronizing coloring.

Preliminaries

A finite directed strongly connected graph with constant outdegree of all its vertices where the gcd of lengths of all its cycles is one will be called *AGW graph* as aroused by Adler, Goodwyn and Weiss.

The bold letters will denote the vertices of a graph and the states of an automaton.

If there exists a path in an automaton from the state $\mathbf{p}$ to the state $\mathbf{q}$ and the edges of the path are consecutively labeled by $\sigma_1, ..., \sigma_k$, then for $s = \sigma_1...\sigma_k \in \Sigma^+$ let us write $\mathbf{q} = \mathbf{p}s$.

Let Ps be the map of the subset P of states of an automaton by help of $s \in \Sigma^+$ and let Ps^{-1} be the maximal set of states Q such that $Qs \subseteq P$. For the transition graph Γ of an automaton let Γs denote the map of the set of states of the automaton.

$|P|$ - the size of the subset P of states from an automaton (of vertices from a graph).

A word $s \in \Sigma^+$ is called a *synchronizing* word of the automaton with transition graph Γ if $|\Gamma s| = 1$.

A coloring of a directed finite graph is *synchronizing* if the coloring turns the graph into a deterministic finite automaton possessing a synchronizing word.

A pair of distinct states $\mathbf{p}, \mathbf{q}$ of an automaton (of vertices of the transition graph) will be called *synchronizing* if $\mathbf{p}s = \mathbf{q}s$ for some $s \in \Sigma^+$. In the opposite case, if for any s $\mathbf{p}s \neq \mathbf{q}s$, we call the pair *deadlock*.

A synchronizing pair of states $\mathbf{p}$, $\mathbf{q}$ of an automaton is called *stable* if for any word u the pair $\mathbf{p}u, \mathbf{q}u$ is also synchronizing [5], [10].

We call the set of all outgoing edges of a vertex a *bunch* if all these edges are incoming edges of only one vertex.

Let u be a left eigenvector with positive components having no common divisor of adjacency matrix of a graph with vertices $\mathbf{p}_1$, ..., $\mathbf{p}_n$. The i-th component u_i of the vector u is called *the weight* of the vertex $\mathbf{p}_i$ and denoted by $w(\mathbf{p}_i)$. The sum of the weights of the vertices from a set D is denoted by $w(D)$ and is called *the weight* of D [6].

The subset D of states of an automaton (of vertices of the transition graph Γ of the automaton) such that $w(D)$ is maximal and $|Ds| = 1$ for some word $s \in \Sigma^+$ let us call *F-maximal* as introduced by Friedman [6].

The subset Γs of states (of vertices of the transition graph Γ) for some word s such that every pair of states from the set is deadlock will be called an *F-clique*.

1 Some properties of F-clique and of coloring free of stable pairs

The road coloring problem was formulated for *AGW* graphs [1] and only such graphs are considered below. We exclude from the consideration also the primitive cases of graphs with loops and of only one color [1], [13]. Let us formulate two important results from [6] and [10] in the following form:

Theorem 1 *[6] There exists a partition of Γ on F-maximal sets (of the same weight).*

Some side conditions on the *AGW* graph stated in [6] were not used in the proof of this statement.

Let us recall that a binary relation ρ on the set of the states of an automaton is called *c*ongruence if ρ is equivalence and for any word u from $\mathbf{p}\ \rho\ \mathbf{q}$ follows $\mathbf{p}u\ \rho\ \mathbf{q}u$.

Theorem 2 *[10] Let us consider a coloring of AGW graph Γ. Stability of states is a binary relation on the set of states of the obtained automaton; denote this relation by ρ. Then ρ is a congruence relation, Γ/ρ presents an AGW graph and synchronizing coloring of Γ/ρ implies synchronizing recoloring of Γ.*

The last theorem shows that if every *AGW* graph has a coloring with a stable pair, then every *AGW* graph has a synchronizing coloring.

Lemma 1 *Let w be the weight of F-maximal set of the AGW graph Γ via some coloring. Then the size of every F-clique of the coloring is the same and equal to $w(\Gamma)/w$ (the size of partition of Γ on F-maximal sets).*

Proof. Two states from an F-clique could not belong to one F-maximal set because this pair is not synchronizing. By Theorem 1 there exists a partition of Γ on F-maximal sets of weight w. So the partition consists from $w(\Gamma)/w$ F-maximal sets and to every F-maximal set belongs at most one state from F-clique. Consequently, the size of any F-clique is not greater than $w(\Gamma)/w$.

Let Γs be an F-clique. The sum of the weights $\mathbf{q}s^{-1}$ for all $\mathbf{q} \in \Gamma s$ is the weight of Γ. So

$$w(\Gamma) = \sum_{q \in \Gamma s} w(\mathbf{q}s^{-1})$$

The number of addends (the size of the F-clique) is not greater than $w(\Gamma)/w$. The weight of the set $\mathbf{q}s^{-1}$ for every $\mathbf{q} \in \Gamma s$ is not greater than w. Therefore $\mathbf{q}s^{-1}$ is an F-maximal set of weight w for every $\mathbf{q} \in \Gamma s$ and the size of any F-clique is $w(\Gamma)/w$, the number of F-maximal sets in the corresponding partition of Γ.

Lemma 2 *Let F be F-clique via some coloring of AGW graph Γ. For any word s the set Fs is also an F-clique and any state [vertex]* $\mathbf{p}$ *belongs to some F-clique.*

Proof. Any pair $\mathbf{p}$, $\mathbf{q}$ from an F-clique F is a deadlock. To be deadlock is a stable binary relation, therefore for any word s the pair $\mathbf{p}s$, $\mathbf{q}s$ from Fs also is a deadlock. So all pairs from Fs are deadlocks.

For the F-clique F there exists a word t such that $\Gamma t = F$. Thus $\Gamma ts = Fs$, whence Fs is an F-clique.

For any $\mathbf{r}$ from a strongly connected graph Γ, there exists a word u such that $\mathbf{r} = \mathbf{p}u$ for $\mathbf{p}$ from the F-clique F, whence $\mathbf{r}$ belongs to the F-clique Fu.

Lemma 3 *Let A and B ($|A| > 1$) be distinct F-cliques via some coloring without stable pairs of the AGW graph Γ. Then $|A| - |A \cap B| = |B| - |A \cap B| > 1$.*

Proof. Let us assume the contrary: $|A| - |A \cap B| = 1$. By Lemma 1, $|A| = |B|$. So $|B| - |A \cap B| = 1$, too. The pair of states $\mathbf{p} \in A \setminus B$ and $\mathbf{q} \in B \setminus A$ is not stable. Therefore for some word s the pair $(\mathbf{p}s, \mathbf{q}s)$ is a deadlock. Any pair of states from the F-clique A and from the F-clique B as well as from F-cliques As and Bs is a deadlock. So any pair of states from the set $(A \cup B)s$ is a deadlock. One has $|(A \cup B)s| = |A| + 1 > |A|$.

In view of Theorem 1, there exists a partition of size $|A|$ (Lemma 1) of Γ on F-maximal sets. To every F-maximal set belongs at most one state from $(A \cup B)s$ because every pair of states from this set is a deadlock and no deadlock could belong to an F-maximal set. This contradicts the fact that the size of $(A \cup B)s$ is greater than $|A|$.

Lemma 4 *Let some vertex of AGW graph Γ have two incoming bunches. Then any coloring of Γ has a stable couple.*

Proof. If a vertex $\mathbf{p}$ has two incoming bunches from vertices $\mathbf{q}$ and $\mathbf{r}$, then the couple $\mathbf{q}$, $\mathbf{r}$ is stable for any coloring because $\mathbf{q}\alpha = \mathbf{r}\alpha = \mathbf{p}$ for any letter (color) $\alpha \in \Sigma$.

2 The spanning subgraph of cycles and trees with maximal number of edges in the cycles

Définition 1 *Let us call a subgraph S of the AGW graph Γ a* spanning subgraph *of Γ if to S belong all vertices of Γ and exactly one outgoing edge of every vertex.*

A maximal subtree of the spanning subgraph S with root on a cycle from S and having no common edges with cycles from S is called a tree *of S.*

The length of path from a vertex $\mathbf{p}$ through the edges of the tree of the spanning set S to the root of the tree is called the level *of $\mathbf{p}$ in S.*

Remark 1 *Any spanning subgraph S consists of disjoint cycles and trees with roots on cycles; any tree and cycle of S is defined identically, the level of the vertex from cycle is zero, the vertices of trees except root have positive level, the vertex of maximal positive level has no incoming edge from S.*

Lemma 5 *Let N be a set of vertices of level n from some tree of the spanning subgraph S of AGW graph Γ. Then in a coloring of Γ where all edges of S have the same color α, any F-clique F satisfies $|F \cap N| \leq 1$.*

Proof. Some power of α synchronizes all states of given level of the tree and maps them into the root. Any couple of states from an F-clique could not be synchronized and therefore could not belong to N.

Lemma 6 *Let AGW graph Γ have a spanning subgraph R of only disjoint cycles (without trees). Then Γ also has another spanning subgraph with exactly one vertex of maximal positive level.*

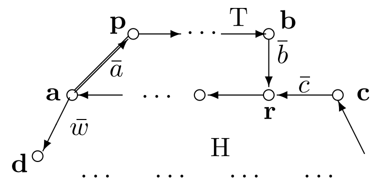
Proof. The spanning subgraph R has only cycles and therefore the levels of all vertices are equal to zero. In view of gcd =1 in the strongly connected graph Γ, not all edges belong to a bunch. Therefore there exist two edges $u = \mathbf{p} \to \mathbf{q} \notin R$ and $v = \mathbf{p} \to \mathbf{s} \in R$ with common first vertex $\mathbf{p}$ but such that $\mathbf{q} \neq \mathbf{s}$. Let us replace the edge $v = \mathbf{p} \to \mathbf{s}$ from R by u. Then only the vertex $\mathbf{s}$ has maximal level $L > 0$ in the new spanning subgraph.

Lemma 7 *Let any vertex of an AGW graph Γ have no two incoming bunches. Then Γ has a spanning subgraph such that all its vertices of maximal positive level belong to one non-trivial tree.*

Proof. Let us consider a spanning subgraph R with a maximal number of vertices [edges] in its cycles. In view of Lemma 6, suppose that R has non-trivial trees and let $L > 0$ be the maximal value of the level of a vertex.

Further consideration is necessary only if at least two vertices of level L belong to distinct trees of R with distinct roots.

Let us consider a tree T from R with vertex $\mathbf{p}$ of maximal level L and edge $\bar{b}$ from vertex $\mathbf{b}$ to the tree root $\mathbf{r} \in T$ on the path of length L from $\mathbf{p}$. Let the root $\mathbf{r}$ belong to the cycle H of R with the edge $\bar{c} = \mathbf{c} \to \mathbf{r} \in H$. There exists also an edge $\bar{a} = \mathbf{a} \to \mathbf{p}$ that does not belong to R because Γ is strongly connected and $\mathbf{p}$ has no incoming edge from R.



Let us consider the path from $\mathbf{p}$ to $\mathbf{r}$ of maximal length L in T. Our aim is to extend the maximal level of the vertex on the extension of the tree T much more than the maximal level of vertex of other trees from R. We plan to use the following three changes:

1) replace the edge $\bar{w}$ from R with first vertex $\mathbf{a}$ by the edge $\bar{a} = \mathbf{a} \to \mathbf{p}$,

2) replace the edge $\bar{b}$ from R by some other outgoing edge of the vertex $\mathbf{b}$,

3) replace the edge $\bar{c}$ from R by some other outgoing edge of the vertex $\mathbf{c}$.

If one of the ways does not succeed let us go to the next assuming the situation in which the previous way fails and excluding the successfully studied cases. So we diminish the considered domain. We can use sometimes two changes together. Let us begin with

1) Suppose first $\mathbf{a} \notin H$. If $\mathbf{a}$ belongs to a path in T from $\mathbf{p}$ to $\mathbf{r}$ then a new cycle with part of the path and edge $\mathbf{a} \to \mathbf{p}$ is added to R extending the number of vertices in its cycles in spite of the choice of R. In opposite case the level of $\mathbf{a}$ in the new spanning subgraph is $L+1$ and the vertex $\mathbf{r}$ is a root of the new tree containing all vertices of maximal level (in particular, the vertex $\mathbf{a}$ or its ancestors in R).

So let us assume $\mathbf{a} \in H$ and suppose $\bar{w} = \mathbf{a} \to \mathbf{d} \in H$. In this case the vertices $\mathbf{p}$, $\mathbf{r}$ and $\mathbf{a}$ belong to a cycle H_1 with new edge $\bar{a}$ of a new spanning subgraph R_1. So we have the cycle $H_1 \in R_1$ instead of $H \in R$. If the length of path from $\mathbf{r}$ to $\mathbf{a}$ in H is r_1 then H_1 has length $L+r_1+1$. A path to $\mathbf{r}$ from the vertex $\mathbf{d}$ of the cycle H remains in R_1. Suppose its length is r_2. So the length of the cycle H is r_1+r_2+1. The length of the cycle H_1 is not greater than the length of H because the spanning subgraph R has maximal number of edges in its cycles. So $r_1+r_2+1 \geq L+r_1+1$, whence $r_2 \geq L$. If $r_2 > L$, then the length r_2 of the path from $\mathbf{d}$ to $\mathbf{r}$ in a tree of R_1 (and the level of $\mathbf{d}$) is greater than L and the level of $\mathbf{d}$ (or of some other ancestor of $\mathbf{r}$ in a tree from R_1) is the desired unique maximal level.

So assume for further consideration $L = r_2$ and $\mathbf{a} \in H$. Analogously, for any vertex of maximal level L with root in the cycle H and incoming edge from a vertex $\mathbf{a}_1$ the proof can be reduced to the case $\mathbf{a}_1 \in H$ and $L = r_2$ for the corresponding new value of r_2.

2) Suppose the set of outgoing edges of the vertex $\mathbf{b}$ is not a bunch. So one can replace in R the edge $\bar{b}$ from the vertex $\mathbf{b}$ by an edge $\bar{v}$ from $\mathbf{b}$ to a vertex $\mathbf{v} \neq \mathbf{r}$.

The vertex $\mathbf{v}$ could not belong to T because in this case a new cycle is added to R and therefore a new spanning subgraph has a number of vertices in the cycles greater than in R.

If the vertex $\mathbf{v}$ belongs to another tree of R but not to cycle, then T is a part of a new tree T_1 with a new root of a new spanning subgraph R_1 and the path from $\mathbf{p}$ to the new root is extended. So only the tree T_1 has states of new maximal level.

If $\mathbf{v}$ belongs to some cycle $H_2 \neq H$ from R, then together with replacing $\bar{b}$ by $\bar{v}$, we replace also the edge $\bar{w}$ by $\bar{a}$. So we extend the path from $\mathbf{p}$ to the new root $\mathbf{v}$ at least by the edge $\bar{a} = \mathbf{a} \to \mathbf{p}$ and by almost all edges of H. Therefore the new maximal level $L_1 > L$ has either the vertex $\mathbf{d}$ or its ancestors from the old spanning subgraph R.

Now there remains only the case when $\mathbf{v}$ belongs to the cycle H. The vertex $\mathbf{p}$ also has level L in new tree T_1 with root $\mathbf{v}$. The only difference between T and T_1 (just as between R and R_1) is the root and the incoming edge of the root. The new spanning subgraph R_1 has also a maximal number of vertices in cycles just as R. Let r_3 be the length of the path from $\mathbf{d}$ to the new root $\mathbf{v} \in H$.

For the spanning subgraph R_1, one can obtain $L = r_3$ just as it was done on the step 1) for R. From $\mathbf{v} \neq \mathbf{r}$ follows $r_3 \neq r_2$, though $L = r_3$ and $L = r_2$.

So for further consideration suppose that the set of outgoing edges of the vertex $\mathbf{b}$ is a bunch to $\mathbf{r}$.

3) The set of outgoing edges of the vertex $\mathbf{c}$ is not a bunch to $\mathbf{r}$ because $\mathbf{r}$ has another bunch from $\mathbf{b}$.

Let us replace in R the edge $\bar{c}$ by an edge $\bar{u} = \mathbf{c} \to \mathbf{u}$ such that $\mathbf{u} \neq \mathbf{r}$. The vertex $\mathbf{u}$ could not belong to the tree T because in this case the cycle H is replaced by a cycle with all vertices from H and some vertices of T whence its length is greater than $|H|$. Therefore the new spanning subgraph has a number of vertices in its cycles greater than in spanning subgraph R in spite of the choice of R.

So remains the case $\mathbf{u} \notin T$. Then the tree T is a part of a new tree with a new root and the path from $\mathbf{p}$ to the new root is extended at least by a part of H from the former root $\mathbf{r}$. The new level of $\mathbf{p}$ therefore is maximal and greater than the level of any vertex in some another tree.

Thus anyway there exists a spanning subgraph with vertices of maximal level in one non-trivial tree.

Theorem 3 *Any AGW graph* Γ *has a coloring with stable couples.*

Proof. By Lemma 4, in the case of vertex with two incoming bunches Γ has a coloring with stable couples. In opposite case, by Lemma 7, Γ has a spanning subgraph R such that the vertices of maximal positive level L belong to one tree of R.

Let us give to the edges of R the color α and denote by C the set of all vertices from the cycles of R. Then let us color the remaining edges of Γ by other colors arbitrarily.

By Lemma 2, in a strongly connected graph Γ for every word s and F-clique F of size $|F| > 1$, the set Fs also is an F-clique (of the same size by Lemma 1) and for any state $\mathbf{p}$ there exists an F-clique F such that $\mathbf{p} \in F$.

In particular, some F has non-empty intersection with the set N of vertices of maximal level L. The set N belongs to one tree, whence by Lemma 5 this intersection has only one vertex. The word α^{L-1} maps F on an F-clique F_1 of size $|F|$. One has $|F_1 \setminus C| = 1$ because the sequence of edges of color α from any tree of R leads to the root of the tree, the root belongs to a cycle colored by α from C and only for the set N with vertices of maximal level holds $N\alpha^{L-1} \not\subseteq C$. So $|N\alpha^{L-1} \cap F_1| = |F_1 \setminus C| = 1$ and $|C \cap F_1| = |F_1| - 1$.

Let the integer m be a common multiple of the lengths of all considered cycles from C colored by α. So for any $\mathbf{p}$ from C as well as from $F_1 \cap C$ holds $\mathbf{p}\alpha^m = \mathbf{p}$. Therefore for an F-clique $F_2 = F_1\alpha^m$ holds $F_2 \subseteq C$ and $C \cap F_1 = F_1 \cap F_2$.

Thus two F-cliques F_1 and F_2 of size $|F_1| > 1$ have $|F_1| - 1$ common vertices. So $|F_1 \setminus (F_1 \cap F_2)| = 1$. Consequently, in view of Lemma 3, there exists a stable couple in the considered coloring.

Theorem 4 *Every AGW graph Γ has synchronizing coloring.*

The proof follows from Theorems 3 and 2.

References

[1] R.L. Adler, L.W. Goodwyn, B. Weiss. *Equivalence of topological Markov shifts*, Israel J. of Math. 27(1977), 49-63.

[2] R.L. Adler, B. Weiss. *Similarity of automorphisms of the torus*, Memoirs of the Amer. Math. Soc., Providence, RI, 98(1970).

[3] G. Budzban, A. Mukherjea. *A semigroup approach to the Road Coloring Problem*, Probability on Algebraic Structures. Contemporary Mathematics, 261(2000), 195-207.

[4] A. Carbone. *Cycles of relatively prime length and the road coloring problem*, Israel J. of Math., 123(2001), 303-316.

[5] K. Culik II, J. Karhumaki, J. Kari. *A note on synchronized automata and Road Coloring Problem*, Developments in Language Theory (5th Int. Conf., Vienna, 2001), Lecture Notes in Computer Science, 2295(2002), 175-185.

[6] J. Friedman. *On the road coloring problem*, Proc. of the Amer. Math. Soc. 110(1990), 1133-1135.

[7] E. Gocka, W. Kirchherr, E. Schmeichel, *A note on the road-coloring conjecture*. Ars Combin. 49(1998), 265-270.

[8] R. Hegde, K. Jain, *Min-Max theorem about the Road Coloring Conjecture* EuroComb 2005, DMTCS proc., AE, 2005, 279 - 284.

[9] N. Jonoska, S. Suen. *Monocyclic decomposition of graphs and the road coloring problem*, Congressum numerantium, 110(1995), 201-209.

[10] J. Kari. *Synchronizing finite automata on Eulerian digraphs*, Springer, Lect. Notes in Comp. Sci., 2136(2001), 432-438.

[11] D. Lind, B. Marcus. *An Introduction of Symbolic Dynamics and Coding*, Cambridge Univ. Press, 1995.

[12] A. Mateescu, A. Salomaa, *Many-Valued Truth Functions, Černy's Conjecture and Road Coloring*, Bull. of European Ass. for TCS, 68(1999), 134-148.

[13] G.L. O'Brien. *The road coloring problem*, Israel J. of Math., 39(1981), 145-154.

[14] D. Perrin, M.P. Schŭtzenberger. *Synchronizing prefix codes and automata, and the road coloring problem*, In Symbolic Dynamics and Appl., Contemp. Math., 135(1992), 295-318.

[15] J.E. Pin. *On two combinatorial problems arising from automata theory*, Annals of Discrete Math., 17(1983), 535-548.

[16] A.N. Trahtman. *Notable trends concerning the synchronization of graphs and automata*, CTW06, El. Notes in Discrete Math., 25(2006), 173-175.