A SEMIGROUP APPROACH TO THE ROAD COLORING PROBLEM

Greg Budzban and Arunava Mukherjea

Abstract. The road coloring problem is considered in the context of finite semigroup theory. Certain classical results are reproven using the structure theory of the kernel and the problem itself is generalized.

1. Introduction

Suppose one is given a strongly connected digraph (that is, there is a directed path between any two vertices). One can think of the vertices of the graph as buildings, for example, and the directed arcs as unnamed, one-way roads connecting the buildings. Suppose, further, that in each building there is a person. Under what conditions can one color the roads, so that the same set of instructions allows each person to get to the same building.

This problem, whose precise formulation is given below, was first posed by Adler, Goodwyn, and Weiss [1] in a paper more than twenty years ago. Due to the informal interpretation given above, it has become known as the road coloring problem, and the set of directions which gets everyone to the same building is known as the synchronizing instruction.

Various partial results exist (as our list of references indicates). The techniques employed by these papers vary considerably, but almost all have a heavy combinatorial flavor. The main contribution of this paper is to retranslate the problem into semigroup theory and to use the fundamental theorem of finite semigroups to both generalize the problem and to simplify the proofs of many of the past results. This unification of technique permits the ability to see many diverse results from a common perspective. In particular, the structure theory of the minimal ideal (kernel) of a finite semigroup plays an essential role. We feel that the kernel will eventually play an important role in the complete solution of the problem. All of the semigroup theory used is elementary and can be found, for example, in Clifford and Preston [4].

The structure of this paper will be as follows. After this introduction, we will provide the necessary semigroup theory to state the problem precisely. Next we will include a section that shows how the structure of the kernel allows us to retranslate certain graph theoretic properties into the language of semigroups. In addition, we will generalize the problem in this semigroup context. Finally, we will present new

1991 *Mathematics Subject Classification*. Primary: ; Secondary:.

Key words and phrases. semigroups, kernels, digraph.

The authors are thankful to W. E. Clark and Göran Högnäs for their useful comments.

Typeset by $\mathcal{AMS}$-TEX

semigroup proofs of several of the most well known results. Examples to illustrate various key ideas will be used throughout the paper.

2. Finite Semigroups and the Road Coloring Problem

A finite semigroup is a finite set, S, which is closed under a binary associative operation. For any subset T of S, we will write $E(T)$ to refer to the set of idempotents in T. Let $G = (V, \mathcal{E})$ be a strongly connected digraph with b vertices having adjacency matrix A. We will assume that the outdegree of each vertex of G or, equivalently, the sum of each row of A is some constant d.

Definition 1. A coloring of G is a decomposition of A into d binary (that is, $0-1$) stochastic matrices $R_1, R_2, \ldots, R_d$ such that $A = R_1 + \cdots + R_d$.

Intuitively, one can think of a matrix R_i as assigning the ith of d colors to the edge (j, k) if $(R_i)_{j,k} = 1$. Each $b \times b$ binary stochastic matrix R can also be thought of as a function on the vertices $\{1, 2, \ldots, n\}$ where $R_{j,k} = 1$ iff $jR = k$. As a notational convention, writing functions on the right allows us to be indifferent to whether we consider $jR = k$ as a function mapping j to k or R as a binary stochastic matrix with j a row vector having a one in the jth position and zeros elsewhere.

Let $S = \langle R_1, R_2, \ldots, R_d \rangle$ be the semigroup generated by $R_1, R_2, \ldots, R_d$ under matrix multiplication (or composition). Clearly, S is a finite semigroup. We will refer to S as a coloring semigroup. The following theorem is extremely important in all that follows.

Theorem 1 ([4])**.** *Let S be a finite semigroup. Then S contains a minimal ideal $\mathcal{K}$ called the kernel which is a disjoint union of isomorphic group. In fact, $\mathcal{K}$ is isomorphic to $\mathcal{X} \times \mathcal{G} \times \mathcal{Y}$ where if $e \in E(S)$, then $e\mathcal{K}e$ is a group and*

$$\mathcal{X} = E(\mathcal{K}e) \qquad \mathcal{G} = e\mathcal{K}e \qquad \mathcal{Y} = E(e\mathcal{K})$$

and if (x_1, g_1, y_1), $(x_2, g_2, y_2) \in \mathcal{X} \times \mathcal{G} \times \mathcal{Y}$ then

$$(x_1, g_1, y_1)(x_2, g_2, y_2) = (x_1, g_1(y_1 x_2)g_2, y_2)$$

The product structure $\mathcal{X} \times \mathcal{G} \times \mathcal{Y}$ is sometimes called a Rees product and any semigroup that has a Rees product is called completely simple. Thus the kernel of a finite semigroup is always completely simple.

The next theoem is extremely useful for characterizing the elements of the kernel. It is an elementary implication of a more general result by Clark [3].

Theorem 2. *Let S be a finite semigroup of matrices. Then the kernel of S is the set of matrices with minimal rank.*

Example. Let us reconsider the road coloring problem using the following example. Suppose the adjacency matrix of a graph is given by

$$A = \begin{bmatrix} 0 & 2 & 0 \\ 1 & 0 & 1 \\ 1 & 0 & 1 \end{bmatrix}.$$

Let

$$R_1 = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 1 & 0 & 0 \end{bmatrix} \qquad B_1 = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 1 \end{bmatrix}$$

$$R_2 = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix} \qquad B_2 = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}$$

Then $A = R_1 + B_1 = R_2 + B_2$.

Let $S_1 = \langle R_1, B_1 \rangle$ and $S_2 = \langle R_2, B_2 \rangle$. Notice that both R_2 and B_2 are permutation matrices, thus S_2 is a group and contains only matrices of rank three. However,

$$(B_1)^2 = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 0 & 1 \\ 0 & 0 & 1 \end{bmatrix}.$$

Therefore, the kernel of S_1 is a set of rank one matrices. In particular, $(B_1)^2$ is a synchronizing instruction. Following the blue road twice will take each person to building three. Thus we can make the following observations from this example:

1) Rank one matrices (equivalently, constant functions) have a natural interpretation as synchronizing instructions
2) Each graph will, in general, have many colorings and not every coloring will produce a synchronizing instruction.

The existence of a synchronizing instruction has ramifications for the "period" of a given graph. We first define the period of a vertex.

Definition 2. For each $v \in V$, define the period of v as

$$\text{per}(v) = \gcd\{|W| : W \text{ is a walk from } v \text{ to } v\}.$$

If the $\text{per}(v) = 1$, then v is called aperiodic. It is a well known fact in Markov chain theory that the period of a vertex is a so-called class property. That is, each vertex in a given strongly connected component (irreducible component, in Markov chain terminology) has the same period. Our assumption of strong connectedness for the graph allows us to speak of the period of the graph. The following theorem was originally proven in [1].

Theorem 3. *If G has a synchronizing instruction, then G is aperiodic.*

Proof. Let $S = \langle R_1, R_2, \ldots, R_d \rangle$ be a coloring semigroup for G that contains a synchronizing instruction $W = M_1 M_2 \ldots M_k$ where each M_i is one of the colors R_j. Then W is a rank one binary stochastic matrix with one column, say w, which is nonzero. Then for each vertex v in V, $vW = w$. In particular, W represents a walk of length k from w to itself. Suppose $u = wR_1$. Now $wR_1W = uW = w$, thus

R_1W is a walk of length $k+1$ from w to itself. Since the period of w is $\gcd(k, k+1)$, G is aperiodic. □

Thus aperiodicity is a necessary condition for the existence of a synchronizing instruction. The road coloring problem seeks to determine if aperiodicity is also a sufficient condition.

Road Coloring Conjecture. *Let $G = (V, \mathcal{E})$ be a d-out, strongly connected digraph with adjacency matrix A. Let $\{\{R_{i_1}, R_{i_2}, \ldots, R_{i_d}\} : A = R_{i_1} + R_{i_2} + \cdot s + R_{i_d}\}$ be the set of all colorings of G and let $S_i = \langle R_{i_1}, R_{i_2}, \ldots, R_{i_d}\rangle$ be the associated coloring semigroups. If G is aperiodic, then for some i, S_i contains a synchronizing instruction.*

3. The Kernel of a Coloring Semigroup

Suppose $S = \langle R_1, R_2, \ldots, R_d\rangle$ is a coloring semigroup for some d-out digraph G. Even if G is not strongly connected, S will be a finite semigroup with kernel $\mathcal{K}$. As we stated in the last section, $\mathcal{K} = \mathcal{X} \times \mathcal{G} \times \mathcal{Y}$. Let M, N be elements of $\mathcal{K}$. Then with respect to the Rees product structure $M = (M_1, M_2, M_3)$ and $N = (N_1, N_2, N_3)$. We will consider the structure of $\mathcal{K}M$, $N\mathcal{K}$, and $N\mathcal{K}M$:

1) $\mathcal{K}M = \mathcal{X} \times \mathcal{G} \times \{M_3\}$ is a minimal left ideal in $\mathcal{K}$ whose elements all have the same range, or nonzero columns as M. This type of semigroup is also referred to as a left group.

2) $N\mathcal{K} = \{N_1\} \times \mathcal{G} \times \mathcal{Y}$ is a minimal right ideal in $\mathcal{K}$ whose elements all have the same partition of the vertices as N. An element P_j in the partition can be assigned to each nonzero column of N by

$$P_j = \{i : N_{i,j} = 1\}$$

   A semigroup like $N\mathcal{K}$ is usually called a right group.

3) $N\mathcal{K}M$ is the intersection of $N\mathcal{K}$ and $\mathcal{K}M$ and is a maximal group in $\mathcal{K}$ (an H-class in the language of semigroups). In this instance, it is best thought of as a set of one-to-one functions specified by the partition of N and the range of M. The idempotent of $N\mathcal{K}M$ is the function which is the identity when restricted to the range of M.

The next result establishes the connection between the kernel and the property of strong connectedness.

Theorem 4. *Let $S = \langle R_1, R_2, \ldots, R_d\rangle$ be any coloring semigroup for $G = (V, E)$. Let S have kernel $\mathcal{K}$ and let M be any element of $\mathcal{K}$. Then G is strongly connected iff for all w in V, $wM\mathcal{K} = V$.*

Proof. Notice that $wM\mathcal{K} = V$ implies strong connectedness immediately, since this implies there is a path between any two vertices. Now, given w_1 in V, let M be any element in $\mathcal{K}$ and suppose $w_1M = w_2$. Let w_3 be any vertex in V. There is a T in S such that $w_2T = w_3$, since G is strongly connected. Thus $w_1MT = w_3$. But MT is in $\mathcal{K}$ and has the same partition as M, since $\text{rank}(M) \leq \text{rank}(T)$. Thus MT is in $M\mathcal{K}$. □

Next we seek to demonstrate that it is the structure of the maximal groups in the kernel that determines whether a coloring semigroup contains a synchronizing instruction. This will follow easily from the ensuing result.

Theorem 5. *Let u, v be arbitrary elements of V. If S is any coloring semigroup with kernel $\mathcal{K}$, then for each maximal group $\mathcal{G}$ in $\mathcal{K}$, $u\mathcal{G} = v\mathcal{G}$.*

Proof. By the previous result, within each minimal right ideal $M\mathcal{K}$, there exists a T_1 such that $uT_1 = v$. Now T_1 belongs to the maximal group $T_1\mathcal{K}T_1 = \mathcal{G}_1 \subset M\mathcal{K}$.

For this group

$$v\mathcal{G}_1 = uT_1\mathcal{G}_1 = u\mathcal{G}_1.$$

If $\mathcal{G}_2$ is any other maximal group in $M\mathcal{K}$ and $T_2 \in \mathcal{G}_2$, then $\mathcal{G}_1T_2 = \mathcal{G}_2$ and

$$v\mathcal{G}_2 = v\mathcal{G}_1T_2 = u\mathcal{G}_1T_2 = u\mathcal{G}_2.$$

But $M\mathcal{K}$ was an arbitrary minimal right ideal. Thus for every maximal group $\mathcal{G}$ in $\mathcal{K}$,

$$u\mathcal{G} = v\mathcal{G}.$$

Theorem 6. *A coloring semigroup S with kernel $\mathcal{K}$ contains a synchronizing instruction iff for every idempotent E in $\mathcal{K}$, $E\mathcal{K}E = \{E\}$.*

Proof. Clearly, if S contains a synchronizing instruction E, then $E = E^2$ is an idempotent. Since E is a rank one binary stochastic matrix, $E\mathcal{K}E = \{E\}$.

Now suppose for every idempotent E in $\mathcal{K}$, $E\mathcal{K}E = \{E\}$. Since E is an idempotent function, E is the identity when restricted to its range. Suppose E is not a constant function. Then there exist u, v in the range of E with $u \neq v$. But $uE = u \neq v = vE$. Since $\{E\}$ is a maximal group in $\mathcal{K}$, this contradicts the previous result. □

The maximal groups in the kernel carry a great deal of information. In fact, we believe that the structure of the maximal groups in the kernels of certain coloring semigroups will provide the periodic structure of the graph. Making this idea precise will require the following definition of periodicity that can be shown to be equivalent to the previous one.

Definition 3. A digraph $G = (V, \mathcal{E})$ is periodic of period $t \geq 2$ iff there exists a partition of the vertices $\{P_1, P_2, \ldots, P_t\}$ such that if $(i, j) \in E$ and $i \in P_k$ then $j \in P_{k+1}$ ($i \in P_t$ implies $j \in P_1$). If no such partition exists, then G is aperiodic. In this case, $\pi = \{V\}$ is the "periodic" partition.

The cyclic nature of a periodic graph suggests the following generalization of the road coloring problem.

Conjecture 2. *Let $G = (V, \mathcal{E})$ be a strongly connected d-out digraph. Then G is periodic of period $t \geq 1$ with periodic partition $\pi = \{P_1, \ldots, P_t\}$ iff G has a minimal (with respect to the rank of its kernel) coloring semigroup $S = \langle R_1, \ldots, R_d \rangle$ whose kernel $\mathcal{K}$ is a right group with partition π and whose maximal groups are all cyclic of order t.*

Computer simulations provide evidence for the conjecture. In addition, a closely-related result in the context of Markov chains has been proven in a very interesting paper by Högnäs [6]. It should be mentioned that in Högnäs' result, (many) more than d colors are often required. Also note that in the aperiodic case, the set of constant functions would be the kernel. The constant functions are a right group with partition $\pi = \{V\}$ and whose maximal groups are all order one, thus trivially cyclic.

4. Semigroup Proofs of Selected Results

In this final section we present new proofs of several well-known results. Part one of the next theorem was originally proven by Friedman in [5]. To the best of our knowledge, part two of this theorem is a new result.

Theorem 7. *Let $G = (V, \mathcal{E})$ be a strongly connected, d-out digraph with adjacency matrix A. Suppose $w = (w_1, w_2, \ldots, w_n)$ is such that $wA = dw$ and let $W = \sum_{i=1}^{n} w_i$ be the Friedman weight of G. We can and do assume that each w_i is a positive integer.*

Let $S = \langle R_1, R_2, \ldots, R_d \rangle$ be a coloring semigroup of G with kernel $\mathcal{K}$ having rank k. Then

(1) $k \mid W$
(2) $k \mid |\mathcal{H}|$ *where $\mathcal{H}$ is any maximal group in $\mathcal{K}$.*

Proof. If $S = \langle R_1, R_2, \ldots, R_d \rangle$ then

$$\frac{1}{d}A = \frac{1}{d}\sum_{j=1}^{d} R_j.$$

Notice $\frac{1}{d}A$ is stochastic, and since strongly connected

$$\lim_{m\to\infty} \frac{1}{m}\sum_{k=1}^{m} \left(\frac{1}{d}A\right)^k = A_0,$$

where A_0 is a rank one strictly positive stochastic matrix with each row equal to $w_0 = \left(\frac{1}{W}\right) w$.

Now consider the element in the semigroup algebra of binary stochastic matrices

$$\frac{1}{d}R_1 + \frac{1}{d}R_2 + \cdots + \frac{1}{d}R_d.$$

Since the coloring semigroup is finite, there is an equivalence between powers of this element and convolution powers of the probability measure μ where

$$\mu(R_i) = \frac{1}{d}.$$

It is known that

$$\lim_{m\to\infty}\left(\frac{1}{m}\sum_{k=1}^{m}\mu^k\right) = \lambda$$

where the support of the measure λ is precisely the kernel $\mathcal{K}$ of the coloring semigroup S. (See Högnäs and Mukherjea [7], pages 79 and 92, for more details.) Thus

$$A_0 = \sum_{K\in\mathcal{K}} \lambda(K)K.$$

Now λ is an idempotent probability measure which is well-known to be locally uniform on each maximal group $\mathcal{H}$.

Precisely, let $E \in E(\mathcal{K})$, then since A_0 is a rank one stochastic matrix,

$$EA_0E = A_0E.$$

Also, $\delta_E * \lambda * \delta_E$, which is an idempotent probability measure on its support $E\mathcal{K}E$ (the reason being $\lambda * \delta_E * \lambda = \lambda$, see [7]), is uniform on $E\mathcal{K}E$; thus

$$(*) \qquad A_0E = \sum_{H\in E\mathcal{K}E} \frac{1}{|\mathcal{H}|} H.$$

Since $\text{rank}(E) = k$, renumber the range elements of E to be $\{1, \dots, k\}$. Then

$$E = \left[\begin{array}{c|c} \frac{I_{k\times k}}{T} & 0 \end{array}\right]$$

where T is $(b-k)\times k$. Also, each $H \in \mathcal{H} = E\mathcal{K}E$ has the same zero columns as E, being elements in the same group.

Write $\mathcal{H} = \{H_1, H_2, \dots, H_m\}$ and let $\mathcal{H}_1 = \{H_1, H_2, \dots, H_t\}$ be all the elements such that

$$(H_j)_{1,1} = 1 \qquad 1 \le j \le t;$$

then by $(*)$ above

$$(A_0E)_{1,1} = \frac{t}{|\mathcal{H}|}.$$

But A_0E has identical rows, thus

$$(A_0E)_{2,1} = \frac{t}{|\mathcal{H}|}.$$

Now $\mathcal{H}_1$ is a subgroup of $\mathcal{H}$ that fixes the element 1. Let H_{t+1} be such that

$$(H_{t+1})_{1,2} = 1$$

then $\mathcal{H}_1 H_{t+1} = \{H_{t+1}, \ldots, H_{2t}\}$ is a coset of $\mathcal{H}_1$.

Notice for j such that $t+1 \leq j \leq 2t$

$$\left(H_j^{-1}\right)_{2,1} = 1;$$

thus

$$(A_0 E)_{1,2} = \frac{t}{|\mathcal{H}|}$$

thus,

$$A_0 E = \left[\begin{array}{cccc|c} \frac{t}{|\mathcal{H}|} & \frac{t}{|\mathcal{H}|} & \cdots & \frac{t}{|\mathcal{H}|} & \\ \vdots & & & \vdots & \\ \vdots & & & \vdots & 0 \\ \frac{t}{|\mathcal{H}|} & \cdots & \cdots & \frac{t}{|\mathcal{H}|} & \end{array}\right]$$

Since $A_0 E$ is a stochastic matrix, then

$$\frac{tk}{|\mathcal{H}|} = 1$$

which implies

$$k \Big| \, |\mathcal{H}| \, .$$

Also, since

$$A_0 = \begin{pmatrix} w_0 \\ w_0 \\ \vdots \\ w_0 \end{pmatrix}$$

where

$$w_0 = \left(\frac{w_1}{W}, \frac{w_2}{W}, \cdots, \frac{w_n}{W}\right) \qquad w_i \in Z^+$$

then

$$A_0 E = \left[\begin{array}{cccc|c} \sum\limits_{E_{i,1}=1} \frac{w_i}{W}, & \sum\limits_{E_{i,2}=1} \frac{w_i}{W}, & \cdots, & \sum\limits_{E_{i,k}=1} \frac{w_i}{W} & \\ \vdots & \vdots & \vdots & \vdots & \\ \vdots & \vdots & \vdots & \vdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \end{array}\right]$$

Let

$$\sum_{E_{i,1}=1} w_i = W_0.$$

Then

$$\frac{W_0}{W} = \frac{t}{|\mathcal{H}|};$$

but since $|\mathcal{H}| = tk$, then

$$kW_0 = W$$

and thus,

$$k \mid W. \qquad \square$$

In the remainder of the paper, we will make the simplifying assumption that the out degree of each vertex is two. We are leading up to O'Brien's result, in which he assumes that a cycle of prime length exists within the graph. Under this assumption, O'Brien also showed that the general problem can be reduced to one of out degree two (see [9] for details). The cycle C will, for the purposes of notation, always in the rest of this paper consist of vertices $1 \to 2 \to 3 \cdots \to p \to 1$. If p is assumed to be prime, it will be explicitly stated.

Definition 4. A binary stochastic matrix R will be called a C-matrix for G iff

(1) $A = R + B$
(2) $(R)_{i,i+1} = (R)_{p,1} = 1$ for $i = 1, \ldots, p-1$.
(3) For each $w \in V$, there is an $i \in C$ such that $(R^t)_{w,i} = 1$, for some t sufficiently large.

It is clear from this definition that for t_0 sufficiently large

$$R^{t_0} = \left[\begin{array}{c|c} \frac{I_{p\times p}}{M} & 0 \end{array} \right]$$

where $I_{p\times p}$ is the $p \times p$ identity matrix and M is a binary stochastic $(b-p) \times p$ matrix. In fact, the powers of R generate an abelian semigroup whose kernel is a cyclic group of order p. R^{t_0} is simply the identity element for this cyclic group.

Definition 5. A vertex $w \in V$ is called periodic with respect to a C-matrix R iff whenever $A_{w,u} = A_{w,v} = 1$, then there exists $k \geq 1$ such that for some $i \in C$,

$$\left(R^k\right)_{u,i} = \left(R^k\right)_{v,i} = 1.$$

If w is not periodic with respect to R, then it is called aperiodic.

Theorem 8. *If G is aperiodic and R is any C-matrix of G, then there exists a vertex $w \in V$ which is aperiodic with respect to R.*

Proof. Suppose each $w \in V$ is periodic with respect to a given C-matrix R. Then if u, v are such that

$$A_{w,u} = A_{w,v} = 1.$$

Then for some k $(= k(w))$,

$$\left(R^k\right)_{u,i} = \left(R^k\right)_{v,i} = 1.$$

Thus

$$\left(BR^k\right)_{w,i} = \left(R^{k+1}\right)_{w,i} = 1.$$

But once the w-th row of BR^k and R^{k+1} are equal, they remain equal under additional powers of R. Since this is true for each vertex, there exists a $\bar{k} = \max_w(k(w))$, such that for all $k \geq \bar{k}$

$$BR^k = R^{k+1}.$$

This implies,

$$\left(\frac{1}{2}A\right) R^k = \left(\frac{1}{2}R + \frac{1}{2}B\right) R^k$$
$$= R^{k+1}.$$

Recall that A is irreducible and aperiodic or, equivalently,

$$\left(\frac{1}{2}A\right)^t > 0 \quad \text{for some } t.$$

However, since

$$\left(\frac{1}{2}A\right)^t R^k = R^{k+t}, \quad t \geq 1,$$

the $p \times p$ submatrix of R^{k+t} (corresponding to the cycle) is strictly positive. Since R^{k+t} is a binary stochastic matrix, we have our contradiction. ☐

Theorem 9. *Let R be a C-matrix for G and let $\mathcal{K}$ be the kernel of $S = \langle R, B\rangle$. Then the rank of $\mathcal{K}$ divides p. Here p need not be a prime.*

Proof. Let

$$M = R^t = \left[\begin{array}{ccccc|c} 0 & 1 & 0 & \cdots & 0 & \\ 0 & 0 & 1 & \cdots & \vdots & \\ \vdots & & & & \vdots & \\ 0 & \cdots & \cdots & \cdots & 1 & 0 \\ 1 & 0 & \cdots & \cdots & 0 & \\ -- & -- & -- & -- & -- & \\ & & D & & & \end{array}\right].$$

Let $z \in \mathcal{K}$ and let $\mathcal{G} = zM\mathcal{K}zM$. Suppose $E = E^2$ is the local identity of $\mathcal{G}$. Notice that each zero column of M is a zero column of E.

Suppose that $\operatorname{rank}(E) = k$ and that k does not divide p. Then

$$p = kr + s, \quad 1 \leq s < k.$$

If we can show that, as a result of this assumption, there exists a positive integer m such that

$$\operatorname{rank}(EM^mE) < k,$$

then we are done.

Let the non-zero columns of E be the columns $i_1 < i_2 \cdots < i_k \leq p$ and define

$$P_j := \left\{\ell : E_{\ell, i_j} = 1, 1 \leq \ell \leq p\right\}.$$

Since the P_j's are disjoint and

$$\operatorname{card}\left(\bigcup_{j=1}^{k} P_j\right) = p < (r+1)k$$

there must exist at least one j_0 such that card $(P_{j_0}) \leq r$. With no loss of generality, assume that $j_0 = 1$.

Claim. For some m, $1 \leq m \leq p$,

$$(M^m E)_{i_j, i_1} = 0 \quad 1 \leq j \leq k.$$

Notice that, because of the action of the cycle, if $(M^m E)_{i_j, i_1} = 1$, then $i_j + m$ must be in P_1. Therefore, m has at most r choices for each j. Thus, there are at most rk choices and if m is different from each of these choices so that for this m, $i_j + m$ is not in P_1 for any j, $1 \leq j \leq k$

$$(M^m E)_{i_j, i_1} = 0.$$

It follows that the i_1th column of $EM^m E$ is zero and this implies that

$$\operatorname{rank}(EM^m E) < k. \qquad \square$$

Theorem 10. *Suppose $G = (V, \mathcal{E})$ is aperiodic, has no parallel edges and a simple cycle, C, of prime length p. Then there exists a C-matrix R whose coloring semigroup $S = \langle R, B \rangle$ contains a synchronizing instruction.*

Proof. Let $A = R + B$. Construct the C-matrix R in the following way. If for i not in C, there are j in C and k not in C such that

$$A_{i,j} = A_{i,k} = 1,$$

then we choose so that $R_{i,j} = 1 = B_{i,k}$. Now if there are any vertices outside of C not connected to C by the previous rule, simply connect them to C by the shortest path to define R.

Case 1. Every point in $V - C$ is periodic with respect to R.

Notice that if every point in $V - C$ is periodic with respect to R, then by the assumption of no parallel edges, and by construction the $(V - C) \times C$ block of the matrix B is all zero. (If a vertex in $V - C$ is connected to two distinct vertices in C, it must be aperiodic.) We know that since every point in $V - C$ is periodic, $BR^n = R^{n+1}$, for sufficiently large n, when we restrict the matrices to $V - C$. Notice that because of our convention mentioned earlier, for every positive integer p the $(V - C) \times V$ block of $B^{p+1} R^n$ is equal to the product of the $(V - C) \times (V - C)$ block of B and the $(V - C) \times V$ block of $B^p R^n$. Thus, by induction, it is easy to see that for any word H in B and R of length r,

$$\begin{aligned} &HR^n \text{ restricted to the } (V - C) \times V \text{ block} \\ &= R^{n+r} \text{ restricted to the } (V - C) \times V \text{ block.} \end{aligned}$$

This means that $[(1/2)A]^p (R^n) = R^{n+p}$, when we restrict both matrices to the $(V - C) \times V$ block, for some sufficiently large n, but for all positive integers p. But this is a contradiction as the left side converges as p goes to infinity, but the right side does not unless $p = 1$. The case $p = 1$ is trivial to synchronize.

Case 2. There is at least one aperiodic point outside C with respect to R.

First observation: Let w_1 be aperiodic, w_1 not in C. Consider all those vertices v_k outside C such that

$$v_k R^k = w_1.$$

If there is no such positive k, then we work with w_1; otherwise, let k_0 be the largest such k. If v_{k_0} is aperiodic, then we will replace w_1 by v_{k_0} and we'll still call it w_1. If v_{k_0} is periodic, we will not change anything and still work with our old w_1. Thus, there is no loss of generality in assuming that w_1 is aperiodic, w_1 not in C, and if there is a v_k such that $v_k R^k = w_1$ for positive integer k, then such a v_k must be periodic.

Second observation: Let us consider the shortest path from C to w_1. We consider a word H (in R and B) such that $(C)H = \{w_1, w_2, \ldots, w_p\}$, and for $i > 1$, the H-path from C to w_i does not contain w_1. In other words, if we interchange R and B only at the vertex w_1, then $(C)H$ remains unaffected.

Final observation: Decompose $(C)H = \{w_1\} \cup Y_k \cup Z_k$, where $Y_k = \{w_2, \ldots, w_k\}$ and $Z_k = \{w_{k+1}, \ldots, w_p\}$, such that for $1 < j < k+1$, $w_j R^{s_j - 1} = w_1$ and w_j is periodic, where $s_2, s_3, \ldots, s_k$ are distinct positive integers, and for each $j > k$, there is no positive integer p such that $w_j R^p = w_1$. [Note: There cannot be two different w_i in Y_k leading to w_1 in the same number of R-steps, as otherwise we can easily reduce the rank of the kernel.] Thus, every vertex in Y_k is periodic; and when we apply the map R^{n+1} on $(C)H$, then the vertices in Z_k remain unaffected if we interchange R and B only at w_1.

Suppose Z_k is empty (in this case, recoloring is not needed). Choose n large so that $(V)R^n$ is inside C and $w_1 R^{n+1} = 1$. Then, Y_k is mapped onto $\{2, 3, \ldots, p\}$ by both R^{n+1} and BR^n. However, $w_1 BR^n > 1$.

Suppose Z_k is not empty. Choose n large as before. Let $w_j R^{n+1} = q_j$. Then, $w_1 BR^{n+1} = q_{j_0}$, for some $j_0 > k$. Now we recolor at the vertex w_1 and then again consider $(C)HR^{n+1}$, with the new R. Notice that the image of Z_k remains the same before and after coloring under the map R^{n+1}; however, q_{j_0}, the present image of w_1 after recoloring, creates a contradiction.

Finally, we state a result where the elementary proof is left to the reader. It is included since it dispenses with a large number of examples quite easily. Notice no assumption concerning parallel edges is required.

Theorem 11. *Let $G = (V, E)$ have a simple cycle C of prime length p and adjacency matrix A. Suppose one of the following conditions holds:*

(1) *there exists $j \notin C$ such that*

$$\sum_{i=1}^{p} A_{i,j} \geq 2; \text{ or}$$

(2) *there exists $j \in C$ such that*

$$\sum_{i=1}^{p} A_{i,j} \geq 3.$$

Then G has a coloring semigroup that contains a synchronizing instruction.

References

1. R. L. Adler, L. W. Goodwyn and B. Weiss, *Equivalence of topological Markov shifts*, Israel Journal of Mathematics **27** (1977), 49–63.
2. A. Carbone, *Cycles of Relatively Prime Length and the Road Coloring Problem*, preprint.
3. W. E. Clark, *Remarks on the Kernel of a Matrix Semigroup*, Czechoslovak Math. Journal **15** (1965), 305–310.
4. A. H. Clifford and G. B. Preston, *The Algebraic Theory of Semigroups*, vol. 1, AMS, Providence, 1961.
5. J. Friedman, *On the Colorability Problem*, Proceedings of the AMS **110** (1990), 1133–1135.
6. G. Högnäs, *Random Semigoup Acts on a Finite Set*, J. Australian Math. Society **23** (1977), 481–498.
7. G. Högnäs and A. Mukherjea, *Probability Measures on Semigroups: Convolution Products, Random Walks, and Random Matrices*, Plenum Press, New York, 1995.
8. N. Jonoska and S. Suen, *Monocyclic Decomposition of Graphs and the Road Coloring Problem*, Congressum Numerantium **110** (1995), 201–209.
9. G. L. O'Brien, *The Road Coloring Problem*, Israel Journal of Mathematics **39** (1981), 145–154.
10. D. Perrin and M. P. Schtzenberger, *Synchronizing Prefix Codes and Automata and the Road Coloring Problem*, Symbolic Dynamics and Applications, Contemporary Mathematics, vol. 135, AMS, Providence, 1992, pp. 295–318.

Southern Illinois University at Carbondale, Carbondale, IL 62901-4408
E-mail address: gbudzban@math.siu.edu

University of South Florida, Tampa, FL 33620-5700
E-mail address: arun@math.usf.edu