On synchronizing colorings of digraphs

Vladimir V. Gusev

Université Catholique de Loivain, Belgium

Ural Federal University, Russia

November 28, 2016

1. Outline of the talk

- Introduction to synchronizing automata
- The Road Coloring Theorem
- Conjectured generalizations of the Road Coloring Theorem
- How do the eigenvectors of digraphs aid us to tackle them

2. Notation

We consider only complete deterministic finite automata:

$$\mathscr{A} = \langle Q, \Sigma, \delta \rangle$$

- Q is the set of states
- Σ is the input alphabet of letters
- $\delta : Q \times \Sigma \to Q$ is the transition function

We need neither initial nor final states

We will write $q \cdot w$ for $\delta(q, w)$

and $P \cdot w$ for $\{\delta(q, w) \mid q \in P\}$

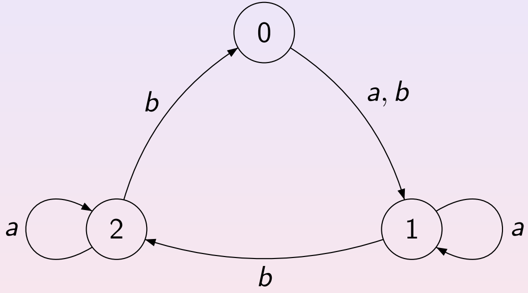
3. Definitions and terminology

An automaton $\mathscr{A}$ is synchronizing if there exists a word $w \in \Sigma^*$ and a state f such that for all $q \in Q$ we have $q \cdot w = f$

We can also write this as $|Q \cdot w| = 1$

Any word w with this property is a reset word or synchronizing word for $\mathscr{A}$

4. An example



The word *abba* is synchronizing

It resets the automaton to the state 1

5. Applications of synchronizing automata

1. Engineering and industrial automation
2. Combinatorial matrix theory (related to primitive and scrambling sets of matrices)
3. Synchronizing codes
4. Algebra (synchronizing groups)
5. Combinatorics on words (non-complete sets of words)

6. The Černý Conjecture

The length of the shortest reset word is called reset threshold

How does the reset threshold depend on the number of states of automata?

Conjecture (Černý, 1964)

Every synchronizing automaton has a reset word of length at most $(n-1)^2$, where n is the number of states

Theorem (Pin, Frankl, 1983)

Every synchronizing automaton with n states has a reset word of length at most $\frac{n^3-n}{6}$

Confirmed in special cases: aperidic, eulerian, with zero, with a cyclic letter, etc.

6. The Černý Conjecture

The length of the shortest reset word is called reset threshold

How does the reset threshold depend on the number of states of automata?

Conjecture (Černý, 1964)

Every synchronizing automaton has a reset word of length at most $(n-1)^2$, where n is the number of states

Theorem (Pin, Frankl, 1983)

Every synchronizing automaton with n states has a reset word of length at most $\frac{n^3-n}{6}$

Confirmed in special cases: aperidic, eulerian, with zero, with a cyclic letter, etc.

6. The Černý Conjecture

The length of the shortest reset word is called reset threshold

How does the reset threshold depend on the number of states of automata?

Conjecture (Černý, 1964)

Every synchronizing automaton has a reset word of length at most $(n-1)^2$, where n is the number of states

Theorem (Pin, Frankl, 1983)

Every synchronizing automaton with n states has a reset word of length at most $\frac{n^3-n}{6}$

Confirmed in special cases: aperidic, eulerian, with zero, with a cyclic letter, etc.

7. Babai's conjecture

Conjecture (the Babai conjecture for S_n, 1992)

There exists a polynomial $f(n)$ such that for any set of generators A of the full permutation group S_n, then for each $\pi \in S_n$ there is a product of at most $f(n)$ elements from A equal to π

Theorem (Helfgott, Seress, 2011)

The full permutation group S_n can be generated in $\exp(O(\log^4 n \log\log n))$ *steps, i.e.,* $\approx n^{\log^C(n)}$

7. Babai's conjecture

Conjecture (the Babai conjecture for S_n, 1992)

There exists a polynomial $f(n)$ such that for any set of generators A of the full permutation group S_n, then for each $\pi \in S_n$ there is a product of at most $f(n)$ elements from A equal to π

Theorem (Helfgott, Seress, 2011)

The full permutation group S_n can be generated in $\exp(O(\log^4 n \log\log n))$ steps, i.e., $\approx n^{\log^C(n)}$

8. Hybrid Černý-Babai's problem

A mapping t from the full transormation semigroup T_n is a constant, if there exists c such that $\forall i \; t(i) = c$

Conjecture (Černý, 1964)

For any set of generators A from the transformation semigroup T_n, if $\langle A \rangle$ contains a constant, then there exists a constant representable as a product of at most $(n-1)^2$ elements from A

Theorem (G., Gonze, Gerencsér, Jungers, Volkov, 2016)

For any set of generators A of the full transformation semigroup T_n, there exists a constant representable as a product of at most $2n^2 - 6n + 5$ elements from A

Open: improve the bound!

8. Hybrid Černý-Babai's problem

A mapping t from the full transormation semigroup T_n is a constant, if there exists c such that $\forall i \, t(i) = c$

Conjecture (Černý, 1964)

For any set of generators A from the transformation semigroup T_n, if $\langle A \rangle$ contains a constant, then there exists a constant representable as a product of at most $(n-1)^2$ elements from A

Theorem (G., Gonze, Gerencsér, Jungers, Volkov, 2016)

For any set of generators A of the full transformation semigroup T_n, there exists a constant representable as a product of at most $2n^2 - 6n + 5$ elements from A

Open: improve the bound!

8. Hybrid Černý-Babai's problem

A mapping t from the full transormation semigroup T_n is a constant, if there exists c such that $\forall i \, t(i) = c$

Conjecture (Černý, 1964)

For any set of generators A from the transformation semigroup T_n, if $\langle A \rangle$ contains a constant, then there exists a constant representable as a product of at most $(n-1)^2$ elements from A

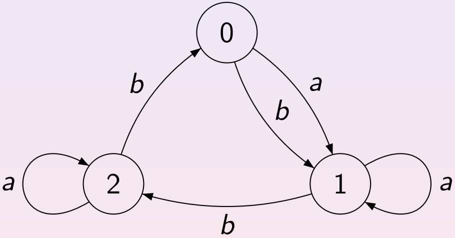
Theorem (G., Gonze, Gerencsér, Jungers, Volkov, 2016)

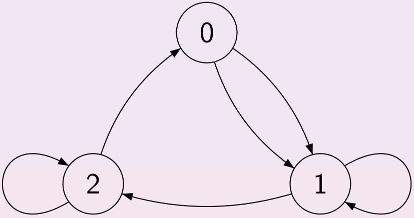
For any set of generators A of the full transformation semigroup T_n, there exists a constant representable as a product of at most $2n^2 - 6n + 5$ elements from A

Open: improve the bound!

What are the properties of the underlying digraph G of a synchronizing automaton $\mathscr{A}$?

Automaton and its underlying digraph





Digraph and its coloring

We consider only k-out-regular digraphs!

9. Primitive matrices and digraphs

A digraph G is primitive if it is strongly connected and the greatest common divisor of lengths of its cycles is equal to 1

Primitive digraphs are related to:

- mixing (or ergodic) Markov chains
- primitive matrices in Perron-Frobenius theory (non-negative square matrix A is primitive if $A^t > 0$ for some t)

Lemma (folklore)

If $\mathscr{A}$ is a strongly connected synchronizing automaton then its underlying digraph is primitive

Is this conditions sufficient?

9. Primitive matrices and digraphs

A digraph G is primitive if it is strongly connected and the greatest common divisor of lengths of its cycles is equal to 1

Primitive digraphs are related to:

- mixing (or ergodic) Markov chains
- primitive matrices in Perron-Frobenius theory (non-negative square matrix A is primitive if $A^t > 0$ for some t)

Lemma (folklore)

If $\mathscr{A}$ is a strongly connected synchronizing automaton then its underlying digraph is primitive

Is this conditions sufficient?

Road Coloring Problem (Ader, Goodwyn and Weiss, 1977)

Does every primitive digraph have a synchronizing coloring?

Motivation: topological Markov shifts in symbolic dynamics

Theorem (Trahtman, 2007)

Every primitive digraph has a synchronizing coloring.

After a crucial observation by Culik II, Karhumäki and Kari in 2001

Theorem (Béal, Perrin, 2008)

There is an $O(kn^2)$-time algorithm to find a synchronizing coloring, where n is the number of states and k is the number of letters.

10. Road Coloring Theorem

Road Coloring Problem (Ader, Goodwyn and Weiss, 1977)

Does every primitive digraph have a synchronizing coloring?

Motivation: topological Markov shifts in symbolic dynamics

Theorem (Trahtman, 2007)

Every primitive digraph has a synchronizing coloring.

After a crucial observation by Culik II, Karhumäki and Kari in 2001

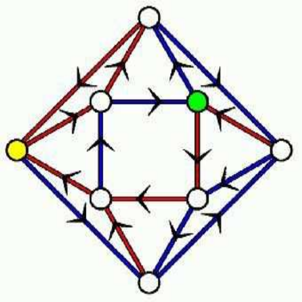
Theorem (Béal, Perrin, 2008)

There is an $O(kn^2)$-time algorithm to find a synchronizing coloring, where n is the number of states and k is the number of letters.

11. Road Coloring Illustration

Edges correspond to one-way roads

Vertices correspond to crossroads



To Yellow:

blue-red-red-blue-red-red-blue-red-red

To Green:

blue-blue-red-blue-blue-red-blue-blue-red

Robust and simple approach for a network of autonomous agents

12. Generalizations of the RCP

Let G be a k-out-regular strongly connected digraph with n vertices

The synchronizing ratio of a digraph G is equal to

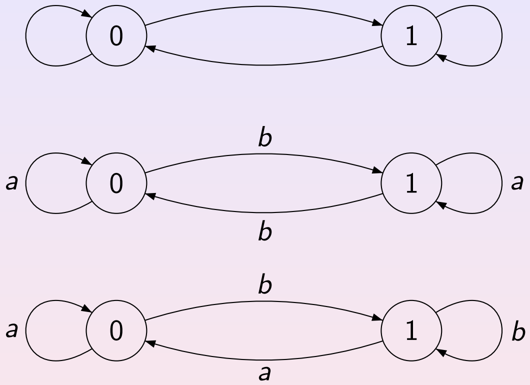
$$\mathrm{SynRatio}(G) = \frac{\text{the number of synchronizing colorings of } G}{\text{the number of all possible colorings of } G}$$

Theorem (Road coloring theorem)

The synchronizing ratio of G is not equal to 0 if and only if G is primitive

What is the worst and average case behaviour of $SynRatio(G)$?

13. Basic example



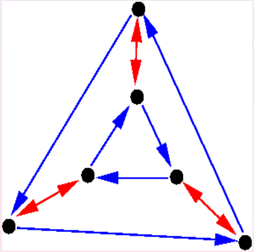
There are 4 colorings and 2 of them are synchronizing

The synchronizing ratio is $\frac{2}{4}$

14. Synchronizing ratio conjecture

Conjecture (G., Szyluła, 2015)

The synchronizing ratio (the fraction of synchronizing automata among all possible colorings) of a primitive k-out-regular digraph G is at least $\frac{k-1}{k}$ with a single exception



only 30 of 64 automata are synchronizing

15. Totally synchronizing digraphs conjecture

A digraph G is called totally synchronizing if its synchronizing ratio is equal to 1

Conjecture (G., Szyluła, 2015)

For every $k \geq 2$, the probability that a random primitive k-out regular digraph is totally synchronizing goes to 1 as n goes to infinity.

Theorem (Berlinkov, 2013; Nicaud 2014)

For every $k \geq 2$, the probability that a random n-state automaton with k letters is synchronizing goes to 1 as n goes to infinity.

Random automaton $\approx$ a random digraph with a random coloring

Question: Do you see totally-synchronizing digraphs in your field?

15. Totally synchronizing digraphs conjecture

A digraph G is called totally synchronizing if its synchronizing ratio is equal to 1

Conjecture (G., Szyluła, 2015)

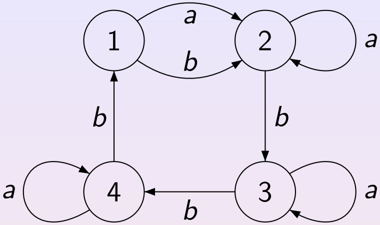
For every $k \geq 2$, the probability that a random primitive k-out regular digraph is totally synchronizing goes to 1 as n goes to infinity.

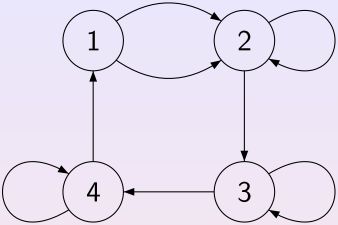
Theorem (Berlinkov, 2013; Nicaud 2014)

For every $k \geq 2$, the probability that a random n-state automaton with k letters is synchronizing goes to 1 as n goes to infinity.

Random automaton $\approx$ a random digraph with a random coloring

Question: Do you see totally-synchronizing digraphs in your field?





Digraph of the automaton

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

The adjacency matrix of the digraph:

At position (i, j) has the number of edges from i to j

17. The eigenvector of a digraph

Theorem

Let A be the adjacency matrix of a primitive k-out-regular digraph G. There exists positive integer eigenvector $\vec{w}$ of A such that $\vec{w}A = k\vec{w}$.

We say that $\vec{w}$ is the eigenvector of G

The eigenvector of $\mathscr{A}$ is the eigenvector of its underlying digraph

Note 1 : entries of $\vec{w}$ are positive by the Perron-Frobenius theorem

Note 2 : $\vec{w}$ is proportional to the stationary distribution of the random walk on G when each edge is taken with the uniform probability $\frac{1}{k}$

Let $Q = \{1, \dots, n\}$, and $\vec{w}[i]$ be the ith entry of $\vec{w}$

The weight of a subset $S \subseteq Q$ is given by $\mathrm{wg}(S) = \sum_{i \in S} \vec{w}[i]$, where $\vec{w}$ is the eigenvector of the automaton

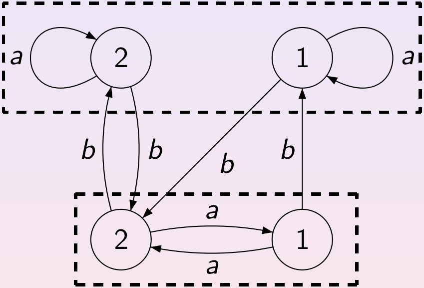
A subset $S \subseteq Q$ is synchronizing if there exists a word u such that $|S \cdot u| = 1$

Theorem (Friedman, 1990)

Every coloring $\mathscr{A}$ of G has a partition of vertices into synchronizing subsets $Q_1, \dots, Q_\ell$ such that $\mathrm{wg}(Q_1) = \dots = \mathrm{wg}(Q_\ell)$ and for any other synchronizing subset S we have $\mathrm{wg}(S) \leq \mathrm{wg}(Q_1)$.

19. Example of a partition

The selected subsets are synchronized by b^2



The eigenvector is equal to $\vec{w} = (2, 1, 2, 1)$

The partition of the states gives rise to the partition of the coordinates $\vec{w} = (\{2, 1\}, \{2, 1\})$

20. Totally-synchronizing digraphs

A vector $\vec{w}$ is partitionable if there exists a partition of entries of $\vec{w}$ into blocks of equal weight b, i.e., a partition $Q_1, \ldots, Q_\ell$ of Q with $\ell > 1$ such that $\sum_{i \in Q_1} \vec{w}[i] = \ldots = \sum_{i \in Q_\ell} \vec{w}[i] = b$

For example :

$(2,1,2,1)$ is partitionable as $(\{2,1\},\{2,1\})$

$(2,2,2,1)$ is not partitionable

Corollary

If the eigenvector of a digraph G is not partitionable then G is totally-synchronizing.

What about the converse statement?

21. Totally-synchronizing digraphs

Denote by $\mathcal{G}(\vec{w})$ the class of out-regular digraphs with the eigenvector $\vec{w}$ (the number of states is fixed, the outdegree is not)

Theorem (G., Pribavkina, 2016)

An entrywise positive integer vector $\vec{w}$ is not partitionable if and only if all digraphs from $\mathcal{G}(\vec{w})$ are totally synchronizing.

Conjecture (G., Pribavkina, 2016)

The eigenvector of a random primitive k-out-regular digraph with n vertices is not partitionable with probability 1 as n goes to infinity.

This conjecture is stronger than totally-synchronizing digraphs conjecture

21. Totally-synchronizing digraphs

Denote by $\mathcal{G}(\vec{w})$ the class of out-regular digraphs with the eigenvector $\vec{w}$ (the number of states is fixed, the outdegree is not)

Theorem (G., Pribavkina, 2016)

An entrywise positive integer vector $\vec{w}$ is not partitionable if and only if all digraphs from $\mathcal{G}(\vec{w})$ are totally synchronizing.

Conjecture (G., Pribavkina, 2016)

The eigenvector of a random primitive k-out-regular digraph with n vertices is not partitionable with probability 1 as n goes to infinity.

This conjecture is stronger than totally-synchronizing digraphs conjecture

22. Unique partitions and the synchronizing ratios

A partition $Q_1, \dots, Q_\ell$ of $\vec{w}$ into blocks of weight b is unique if for every partition $Q'_1, \dots, Q'_\ell$ of weight b there exists a permutation of $1, \dots, \ell$ such that $Q_i = Q'_{\sigma(i)}$ for all i

$(1, 4, 6, 9, 10)$ has two unique partitions:

$(1, 4, 6, 9, 10)$ of weight 10

$(1, 4, 6, 9, 10)$ of weight 15

Theorem (G., Pribavkina, 2016)

If all partitions of the eigenvector $\vec{w}$ are unique and their number is equal to s, then the synchronizing ratio of every k-out-regular digraph in $\mathcal{G}(\vec{w})$ is at least $\frac{k-s}{k}$.

Note, in the case of $s = 1$ we have the conjectured bound: it includes all Eulerian digraphs with a prime number of states, i.e., digraphs with the eigenvector $(1, 1, \dots, 1)$

22. Unique partitions and the synchronizing ratios

A partition $Q_1, \ldots, Q_\ell$ of $\vec{w}$ into blocks of weight b is unique if for every partition $Q'_1, \ldots, Q'_\ell$ of weight b there exists a permutation of $1, \ldots, \ell$ such that $Q_i = Q'_{\sigma(i)}$ for all i

$(1, 4, 6, 9, 10)$ has two unique partitions:

$(1, 4, 6, 9, 10)$ of weight 10

$(1, 4, 6, 9, 10)$ of weight 15

Theorem (G., Pribavkina, 2016)

If all partitions of the eigenvector $\vec{w}$ are unique and their number is equal to s, then the synchronizing ratio of every k-out-regular digraph in $\mathcal{G}(\vec{w})$ is at least $\frac{k-s}{k}$.

Note, in the case of $s = 1$ we have the conjectured bound: it includes all Eulerian digraphs with a prime number of states, i.e., digraphs with the eigenvector $(1, 1, \ldots, 1)$

23. Main idea of the proof

Lemma (G., Pribavkina, 2016)

Let $\mathscr{A}$ be a non-synchronizing automaton with the eigenvector $\vec{w}$. A partition into synchronizing subsets of maximal weight is unique if and only if it is a congruence.

Rough scheme of the proof:

1. every non-synchronizing coloring $\mathscr{A}$ is associated to a partition $\beta(\mathscr{A})$ of states
2. $\beta(\mathscr{A})$ has to be a congruence on $\mathscr{A}$
3. $\beta(\mathscr{A})$ is a congruence for at most $\frac{1}{k} \cdot k^n$ colorings

24. Conjectures on the complexity of RCP

Given a primitive k-ot-regular digraph G with n states

Conjecture

The problem of deciding whether G has a non-synchronizing coloring is NP-complete.

Conjecture

The problem of counting the number of synchronizing colorings is $\#P$-complete.

25. Conclusions

Main ideas: there are many open problems related to synchronizing colorings of digraphs; the eigenvectors of digraphs tell us a lot about synchronizing properties of automata

Open problems:

1. the Černý conjecture
2. the synchronizing ratio is bounded by $\frac{k-1}{k}$
3. w.h.p. random primitive digraph is totally synchronizing
4. Hybrid Černý-Babai's problem
5. characterization of totally synchronizing digraphs (is it an NP-complete problem?)

26. Hybrid Conjecture

Conjecture (Hybrid Černý–Road Coloring Problem, Volkov)

Every primitive k-out-regular digraph with n vertices has a synchronizing coloring with the reset threshold at most $n^2 - 3n + 3$.

Theorem (Steinberg, 2011)

Every primitive digraph with n vertices containing a cycle of prime length admits a coloring with the reset threshold at most $(n-1)^2$.

Theorem (Carpi, D'Alessandro, 2011)

Every digraph having a Hamiltonian cycle admit a coloring with the reset threshold at most $2n^2 - 4n + 1 - 2(n-1)\ln(\frac{n}{2})$.

Given an object that can have certain spacial orientations, e.g. a mushroom on a conveyor belt

Given a list of actions that we can apply to our object, e.g. bumps and guiding lines

Design a sequence of actions that will bring the object to a desired spacial orientation, e.g. a conveyor belt forcing an object into the right orientation

So, we look for a synchronizing sequence for the automaton with the orientations as its states and the actions as its letters

28. The eigenvectors and the reset thresholds

Theorem (Kari, 2003)

The reset threshold of an Eulerian automaton with n states is at most $n^2 - 3n + 3$.

Theorem (Berlinkov, 2012)

Let W be the sum of the coordinates of the eigenvector of a strongly connected automaton $\mathscr{A}$. If $\mathscr{A}$ is synchronizing, then the reset threshold of $\mathscr{A}$ is at most $1 + (n-1)(W-2)$.

For Eulerian automaton $W = n$

Theorem

Let W be the sum of the coordinates of the eigenvector of a strongly connected automaton $\mathscr{A}$. If $\mathscr{A}$ is synchronizing, then there exists a synchronizing Eulerian automaton $\mathscr{B}$ with W states such that $\mathscr{A}$ is the factor automaton of $\mathscr{B}$ and $\mathrm{rt}(\mathscr{A}) \leq \mathrm{rt}(\mathscr{B}) \leq \mathrm{rt}(\mathscr{A}) + 1$. Thus, $\mathrm{rt}(\mathscr{A}) \leq W^2 - 3W + 3$.

28. The eigenvectors and the reset thresholds

Theorem (Kari, 2003)

The reset threshold of an Eulerian automaton with n states is at most $n^2 - 3n + 3$.

Theorem (Berlinkov, 2012)

Let W be the sum of the coordinates of the eigenvector of a strongly connected automaton $\mathscr{A}$. If $\mathscr{A}$ is synchronizing, then the reset threshold of $\mathscr{A}$ is at most $1 + (n-1)(W-2)$.

For Eulerian automaton $W = n$

Theorem

Let W be the sum of the coordinates of the eigenvector of a strongly connected automaton $\mathscr{A}$. If $\mathscr{A}$ is synchronizing, then there exists a synchronizing Eulerian automaton $\mathscr{B}$ with W states such that $\mathscr{A}$ is the factor automaton of $\mathscr{B}$ and $\mathrm{rt}(\mathscr{A}) \leq \mathrm{rt}(\mathscr{B}) \leq \mathrm{rt}(\mathscr{A}) + 1$. Thus, $\mathrm{rt}(\mathscr{A}) \leq W^2 - 3W + 3$.

28. The eigenvectors and the reset thresholds

Theorem (Kari, 2003)

The reset threshold of an Eulerian automaton with n states is at most $n^2 - 3n + 3$.

Theorem (Berlinkov, 2012)

Let W be the sum of the coordinates of the eigenvector of a strongly connected automaton $\mathscr{A}$. If $\mathscr{A}$ is synchronizing, then the reset threshold of $\mathscr{A}$ is at most $1 + (n-1)(W-2)$.

For Eulerian automaton $W = n$

Theorem

Let W be the sum of the coordinates of the eigenvector of a strongly connected automaton $\mathscr{A}$. If $\mathscr{A}$ is synchronizing, then there exists a synchronizing Eulerian automaton $\mathscr{B}$ with W states such that $\mathscr{A}$ is the factor automaton of $\mathscr{B}$ and $\mathrm{rt}(\mathscr{A}) \leq \mathrm{rt}(\mathscr{B}) \leq \mathrm{rt}(\mathscr{A}) + 1$. *Thus,* $\mathrm{rt}(\mathscr{A}) \leq W^2 - 3W + 3$.