Synchronizing Finite Automata

Lecture V. Expansion Method

Mikhail Volkov

Ural Federal University

Spring of 2021

Deterministic finite automata: $\mathscr{A} = \langle Q, \Sigma, \delta \rangle$.

- Q the state set
- Σ the input alphabet
- $\delta : Q \times \Sigma \to Q$ the transition function

Deterministic finite automata: $\mathscr{A} = \langle Q, \Sigma, \delta \rangle$.

- Q the state set
- Σ the input alphabet
- $\delta : Q \times \Sigma \to Q$ the transition function

$\mathscr{A}$ is called synchronizing if there exists a word $w \in \Sigma^*$ whose action resets $\mathscr{A}$, that is, leaves the automaton in one particular state no matter which state in Q it started at: $\delta(q, w) = \delta(q', w)$ for all $q, q' \in Q$.

Deterministic finite automata: $\mathscr{A} = \langle Q, \Sigma, \delta \rangle$.

- Q the state set
- Σ the input alphabet
- $\delta : Q \times \Sigma \to Q$ the transition function

$\mathscr{A}$ is called synchronizing if there exists a word $w \in \Sigma^*$ whose action resets $\mathscr{A}$, that is, leaves the automaton in one particular state no matter which state in Q it started at: $\delta(q, w) = \delta(q', w)$ for all $q, q' \in Q$.
$|Q \, . \, w| = 1$. Here $Q \, . \, v = \{\delta(q, v) \mid q \in Q\}$.

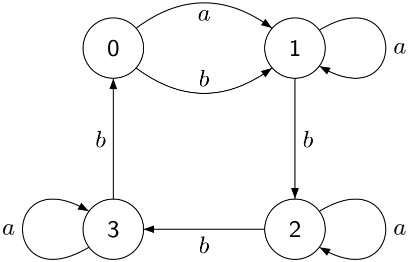
1. Recap

Deterministic finite automata: $\mathscr{A} = \langle Q, \Sigma, \delta \rangle$.

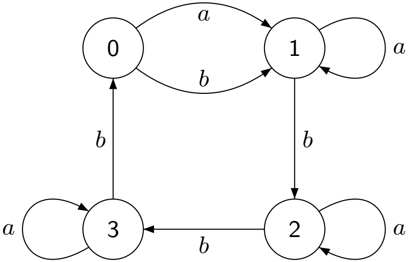
- Q the state set
- Σ the input alphabet
- $\delta : Q \times \Sigma \to Q$ the transition function

$\mathscr{A}$ is called synchronizing if there exists a word $w \in \Sigma^*$ whose action resets $\mathscr{A}$, that is, leaves the automaton in one particular state no matter which state in Q it started at: $\delta(q, w) = \delta(q', w)$ for all $q, q' \in Q$.
$|Q \,.\, w| = 1$. Here $Q \,.\, v = \{\delta(q, v) \mid q \in Q\}$.

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

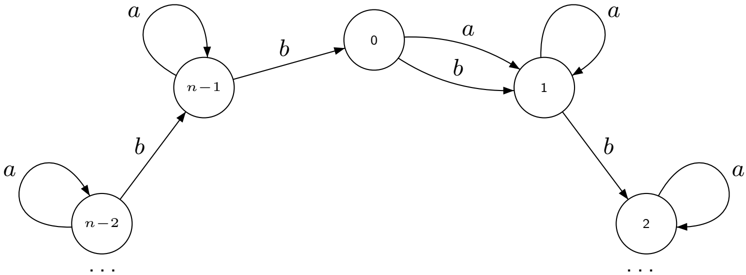


0
1
2
3
a
b

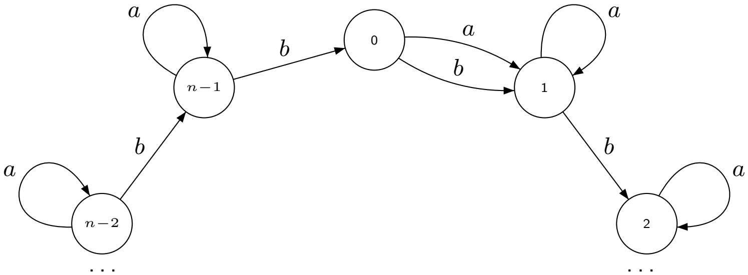


A reset word is $abbbabbba$. In fact, we have verified that this is the shortest reset word for this automaton.

In his 1964 paper Jan Černý constructed a series $\mathscr{C}_n$, $n = 2, 3, \ldots$, of synchronizing automata over 2 letters. Here is a generic automaton from the Černý series:



In his 1964 paper Jan Černý constructed a series $\mathscr{C}_n$, $n = 2, 3, \dots,$ of synchronizing automata over 2 letters. Here is a generic automaton from the Černý series:



Černý has proved that the shortest reset word for $\mathscr{C}_n$ is $(ab^{n-1})^{n-2}a$ of length $(n-1)^2$.

Define the Černý function $C(n)$ as the maximum reset threshold of all synchronizing automata with n states. The above property of the series $\{\mathscr{C}_n\}$, $n = 2, 3, \dots$, yields the inequality $C(n) \geq (n-1)^2$.

Define the Černý function $C(n)$ as the maximum reset threshold of all synchronizing automata with n states. The above property of the series $\{\mathscr{C}_n\}$, $n = 2, 3, \ldots$, yields the inequality $C(n) \geq (n-1)^2$.

The Černý conjecture is the claim that in fact the equality $C(n) = (n-1)^2$ holds true.

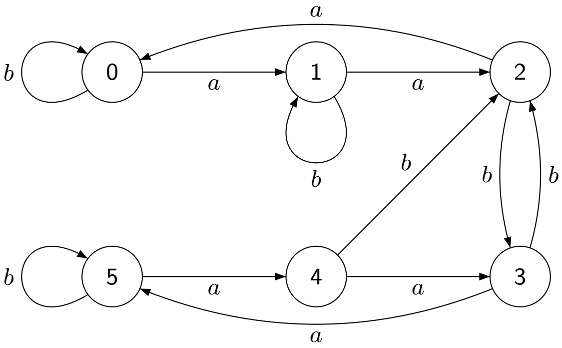
Define the Černý function $C(n)$ as the maximum reset threshold of all synchronizing automata with n states. The above property of the series $\{\mathscr{C}_n\}$, $n = 2, 3, \ldots$, yields the inequality $C(n) \geq (n-1)^2$.

The Černý conjecture is the claim that in fact the equality $C(n) = (n-1)^2$ holds true.
Everything we know about the conjecture in general can be summarized in one line:

$$(n-1)^2 \leq C(n) \leq \frac{\min\{\frac{85059n^3+90024n^2+196504n-10648}{85184}, n^3-n\}}{6}.$$

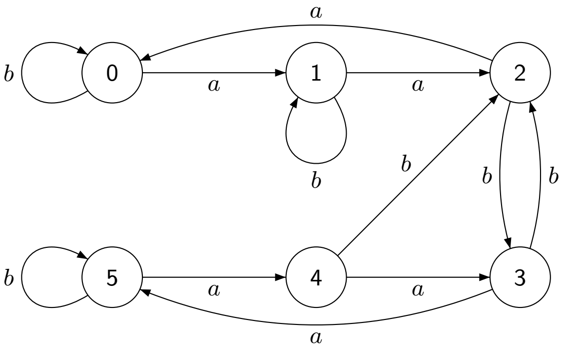
Beyond the Černý series, the largest automaton that reaches the Černý bound is the 6-state automaton $\mathscr{K}_6$ found by Jarkko Kari (A counter example to a conjecture concerning synchronizing words in finite automata, EATCS Bull., 73, 146 (2001)).

Beyond the Černý series, the largest automaton that reaches the Černý bound is the 6-state automaton $\mathscr{K}_6$ found by Jarkko Kari (A counter example to a conjecture concerning synchronizing words in finite automata, EATCS Bull., 73, 146 (2001)).



5. Kari's Automaton

Beyond the Černý series, the largest automaton that reaches the Černý bound is the 6-state automaton $\mathscr{K}_6$ found by Jarkko Kari (A counter example to a conjecture concerning synchronizing words in finite automata, EATCS Bull., 73, 146 (2001)).



It has refuted several conjectures.

In particular, Kari's example has refuted the extensibility conjecture.

In particular, Kari's example has refuted the extensibility conjecture.
Let $\mathscr{A} = \langle Q, \Sigma, \delta \rangle$ be a DFA. For $P \subseteq Q$ and $w \in \Sigma^*$,

$$Pw^{-1} := \{q \in Q \mid q\,.\,w \in P\}.$$

In particular, Kari's example has refuted the extensibility conjecture.
Let $\mathscr{A} = \langle Q, \Sigma, \delta \rangle$ be a DFA. For $P \subseteq Q$ and $w \in \Sigma^*$,

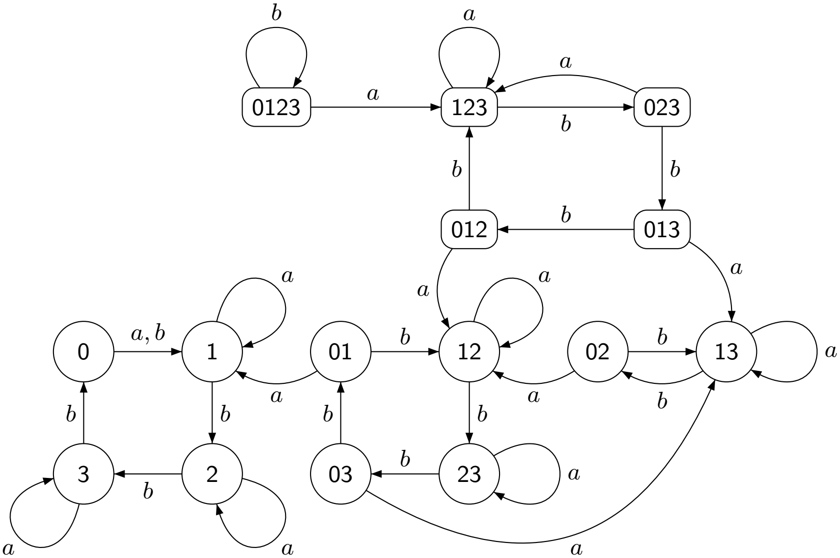
$$Pw^{-1} := \{q \in Q \mid q\,.\,w \in P\}.$$

A subset $P \subset Q$ is extensible if there exists a word $w \in \Sigma^*$ of length at most $n = |Q|$ such that $|Pw^{-1}| > |P|$.

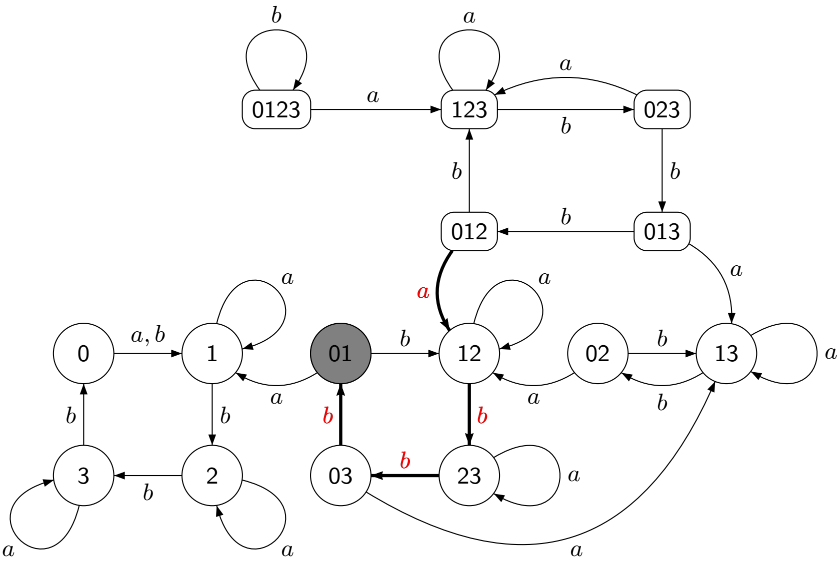
In particular, Kari's example has refuted the extensibility conjecture.
Let $\mathscr{A} = \langle Q, \Sigma, \delta \rangle$ be a DFA. For $P \subseteq Q$ and $w \in \Sigma^*$,

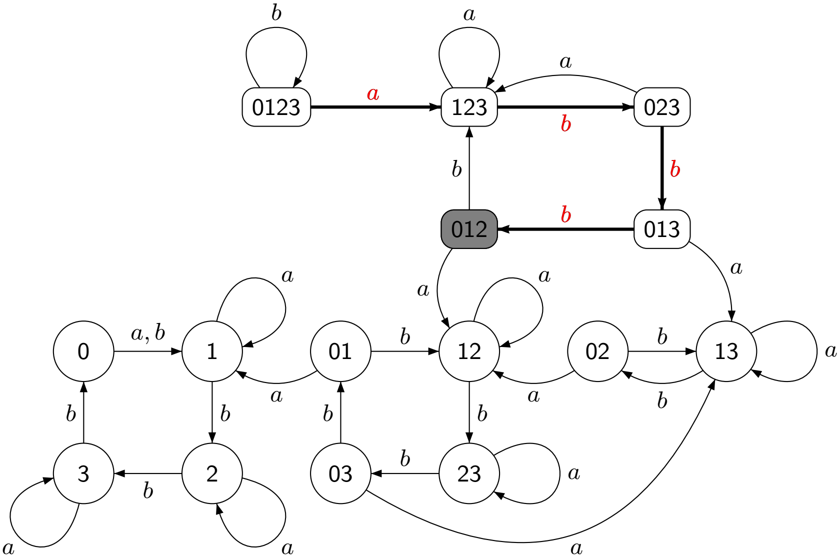
$$Pw^{-1} := \{q \in Q \mid q \,.\, w \in P\}.$$

A subset $P \subset Q$ is extensible if there exists a word $w \in \Sigma^*$ of length at most $n = |Q|$ such that $|Pw^{-1}| > |P|$.
It was conjectured that in synchronizing automata every proper non-singleton subset is extensible.


0123
123
023
012
013
0
1
01
12
02
13
3
2
03
23
a
b
a, b

7. Example





b
a
a
0123
a
123
023
b
b
b
012
b
013
a
a
a
a
a, b
0
1
01
b
12
02
b
13
a
a
a
b
b
b
b
b
3
b
2
03
b
23
a
a
a
a

Observe that the extensibility conjecture implies the Černý conjecture.

Observe that the extensibility conjecture implies the Černý conjecture. Indeed, if $\mathscr{A} = \langle Q, \Sigma, \delta \rangle$ with $|Q| = n$ is synchronizing, then some letter $a \in \Sigma$ should send two states $q, q' \in Q$ to the same state p.

Observe that the extensibility conjecture implies the Černý conjecture.
Indeed, if $\mathscr{A} = \langle Q, \Sigma, \delta \rangle$ with $|Q| = n$ is synchronizing, then some letter $a \in \Sigma$ should send two states $q, q' \in Q$ to the same state p.
Let $P_0 = \{q, q'\}$ and, for $i > 0$, let P_i be such that $|P_i| > |P_{i-1}|$ and $P_i = P_{i-1} w_i^{-1}$ for some word w_i of length $\leq n$.

Observe that the extensibility conjecture implies the Černý conjecture.
Indeed, if $\mathscr{A} = \langle Q, \Sigma, \delta\rangle$ with $|Q| = n$ is synchronizing, then some letter $a \in \Sigma$ should send two states $q, q' \in Q$ to the same state p.
Let $P_0 = \{q, q'\}$ and, for $i > 0$, let P_i be such that $|P_i| > |P_{i-1}|$ and $P_i = P_{i-1}w_i^{-1}$ for some word w_i of length $\leq n$.
Then in at most $n-2$ steps the sequence $P_0, P_1, P_2, \ldots$ reaches Q and

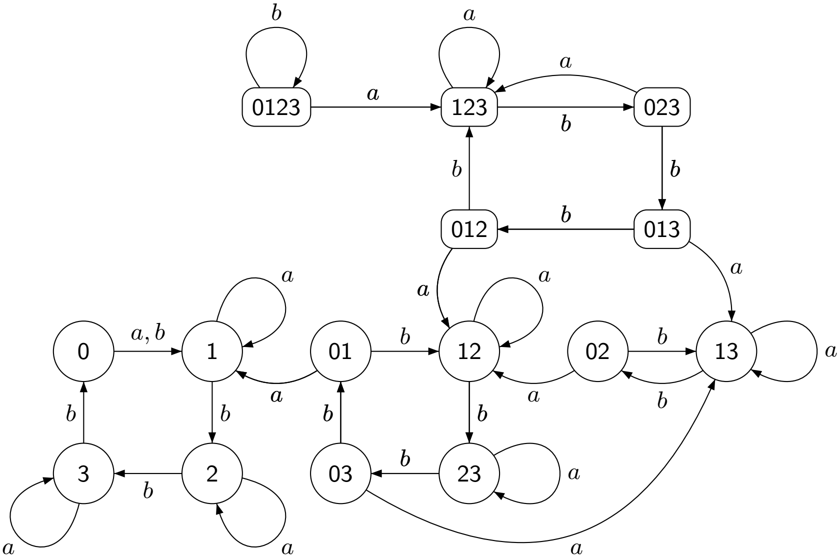
$$Q \,.\, w_{n-2}w_{n-3}\cdots w_1 a = \{p\},$$

that is, $w_{n-2}w_{n-3}\cdots w_1 a$ is a reset word.

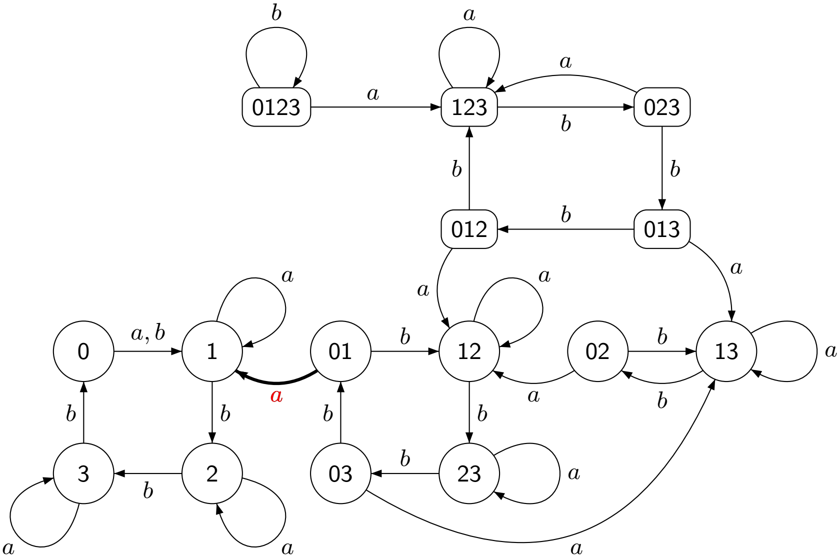
Observe that the extensibility conjecture implies the Černý conjecture.
Indeed, if $\mathscr{A} = \langle Q, \Sigma, \delta \rangle$ with $|Q| = n$ is synchronizing, then some letter $a \in \Sigma$ should send two states $q, q' \in Q$ to the same state p.
Let $P_0 = \{q, q'\}$ and, for $i > 0$, let P_i be such that $|P_i| > |P_{i-1}|$ and $P_i = P_{i-1} w_i^{-1}$ for some word w_i of length $\leq n$.
Then in at most $n - 2$ steps the sequence $P_0, P_1, P_2, \ldots$ reaches Q and

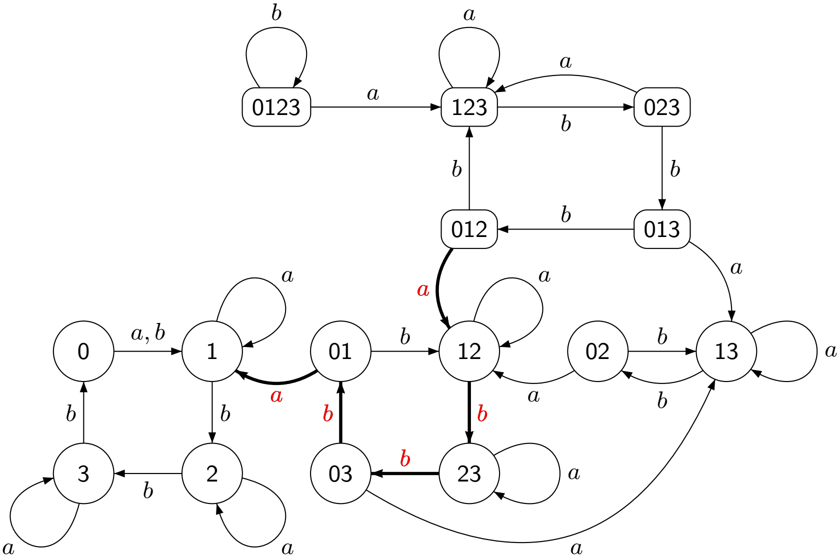
$$Q \,.\, w_{n-2} w_{n-3} \cdots w_1 a = \{p\},$$

that is, $w_{n-2} w_{n-3} \cdots w_1 a$ is a reset word.
The length of this reset word is at most $n(n-2) + 1 = (n-1)^2$.

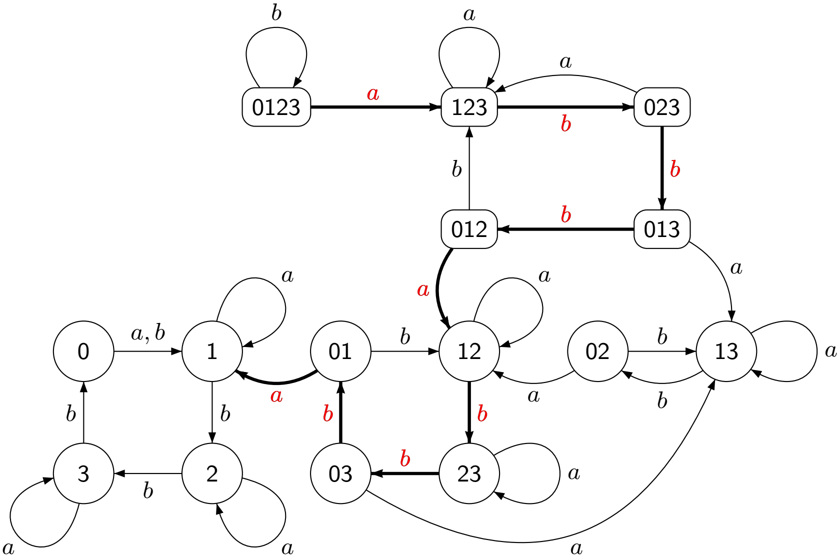

0123
123
023
012
013
0
1
01
12
02
13
3
2
03
23
a
b
a, b

9. Example




0123
123
023
012
013
0
1
01
12
02
13
3
2
03
23
a
b
a, b

9. Example



b
a
a
0123
a
123
023
b
b
b
b
012
013
a
a
a
a
a
0
a, b
1
01
b
12
02
b
13
a
a
a
b
b
b
b
b
b
3
b
2
03
b
23
a
a
a
a

Several important results confirming the Černý conjecture for various partial cases have been proved by verifying the extensibility conjecture for the corresponding automata. This includes:

Several important results confirming the Černý conjecture for various partial cases have been proved by verifying the extensibility conjecture for the corresponding automata. This includes:

• Louis Dubuc's result for automata in which a letter acts on the state set Q as a cyclic permutation of order $|Q|$ (Sur le automates circulaires et la conjecture de Černý, RAIRO Inform. Theor. Appl., 32, 21–34 (1998) [in French]).

Several important results confirming the Černý conjecture for various partial cases have been proved by verifying the extensibility conjecture for the corresponding automata. This includes:

• Louis Dubuc's result for automata in which a letter acts on the state set Q as a cyclic permutation of order $|Q|$ (Sur le automates circulaires et la conjecture de Černý, RAIRO Inform. Theor. Appl., 32, 21–34 (1998) [in French]).
• Jarkko Kari's result for automata with Eulerian digraphs (Synchronizing finite automata on Eulerian digraphs, Theoret. Comput. Sci., 295, 223–232 (2003).)

Several important results confirming the Černý conjecture for various partial cases have been proved by verifying the extensibility conjecture for the corresponding automata. This includes:

• Louis Dubuc's result for automata in which a letter acts on the state set Q as a cyclic permutation of order $|Q|$ (Sur le automates circulaires et la conjecture de Černý, RAIRO Inform. Theor. Appl., 32, 21–34 (1998) [in French]).
• Jarkko Kari's result for automata with Eulerian digraphs (Synchronizing finite automata on Eulerian digraphs, Theoret. Comput. Sci., 295, 223–232 (2003).)
• Benjamin Steinberg's result for automata in which a letter labels only one cycle (one-cluster automata) and this cycle is of prime length (The Černý conjecture for one-cluster automata with prime length cycle. Theoret. Comput. Sci., 412, 5487–5491 (2011)).

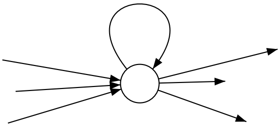
In this lecture, we present Kari's result.

In this lecture, we present Kari's result.

A (directed) graph is strongly connected if for every pair of its vertices, there exists a (directed) path from one to the other.

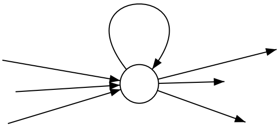
In this lecture, we present Kari's result.

A (directed) graph is strongly connected if for every pair of its vertices, there exists a (directed) path from one to the other.
A graph is Eulerian if it is strongly connected and each of its vertices serves as the tail and as the head for the same number of edges.



In this lecture, we present Kari's result.

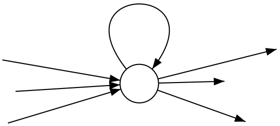
A (directed) graph is strongly connected if for every pair of its vertices, there exists a (directed) path from one to the other.
A graph is Eulerian if it is strongly connected and each of its vertices serves as the tail and as the head for the same number of edges.



A DFA is said to be Eulerian if so is its underlying graph.

In this lecture, we present Kari's result.

A (directed) graph is strongly connected if for every pair of its vertices, there exists a (directed) path from one to the other.
A graph is Eulerian if it is strongly connected and each of its vertices serves as the tail and as the head for the same number of edges.



A DFA is said to be Eulerian if so is its underlying graph.
Since in any DFA the number of edges starting at a given state is the same (the cardinality of the input alphabet), in an Eulerian DFA the number of edges ending at any state is the same.

Now suppose that $\mathscr{A} = \langle Q, \Sigma, \delta \rangle$ is an Eulerian synchronizing automaton with $|Q| = n$ and $|\Sigma| = k$.

Now suppose that $\mathscr{A} = \langle Q, \Sigma, \delta \rangle$ is an Eulerian synchronizing automaton with $|Q| = n$ and $|\Sigma| = k$. Then for every $P \subseteq Q$, the equality

$$\sum_{a \in \Sigma} |Pa^{-1}| = k|P| \qquad (*)$$

holds true since the left-hand side is the number of edges in the underlying graph of $\mathscr{A}$ with ends in P.

Now suppose that $\mathscr{A} = \langle Q, \Sigma, \delta \rangle$ is an Eulerian synchronizing automaton with $|Q| = n$ and $|\Sigma| = k$. Then for every $P \subseteq Q$, the equality

$$\sum_{a \in \Sigma} |Pa^{-1}| = k|P| \qquad (*)$$

holds true since the left-hand side is the number of edges in the underlying graph of $\mathscr{A}$ with ends in P.

The equality (*) readily implies that for each $P \subseteq Q$, exactly one of the following alternatives takes place:
either

$$|Pa^{-1}| = |P| \text{ for all letters } a \in \Sigma$$

or

$$|Pb^{-1}| > |P| \text{ for some letter } b \in \Sigma.$$

Assume that a subset $S \subseteq Q$ and a word $u \in \Sigma^+$ are such that $|Su^{-1}| \neq |S|$ and u is a word of minimum length with this property.

Assume that a subset $S \subseteq Q$ and a word $u \in \Sigma^+$ are such that $|Su^{-1}| \neq |S|$ and u is a word of minimum length with this property. We write $u = aw$ for some $a \in \Sigma$ and $w \in \Sigma^*$ and let $P = Sw^{-1}$.

Assume that a subset $S \subseteq Q$ and a word $u \in \Sigma^+$ are such that $|Su^{-1}| \neq |S|$ and u is a word of minimum length with this property. We write $u = aw$ for some $a \in \Sigma$ and $w \in \Sigma^*$ and let $P = Sw^{-1}$. Then $|P| = |S|$ by the choice of u and $Pa^{-1} = (Sw^{-1})a^{-1} = S(aw)^{-1} = Su^{-1}$ whence $|Pa^{-1}| \neq |P|$.

Assume that a subset $S \subseteq Q$ and a word $u \in \Sigma^+$ are such that $|Su^{-1}| \neq |S|$ and u is a word of minimum length with this property. We write $u = aw$ for some $a \in \Sigma$ and $w \in \Sigma^*$ and let $P = Sw^{-1}$. Then $|P| = |S|$ by the choice of u and $Pa^{-1} = (Sw^{-1})a^{-1} = S(aw)^{-1} = Su^{-1}$ whence $|Pa^{-1}| \neq |P|$.

Thus, P must fall into the second of the above alternatives and so $|Pb^{-1}| > |P|$ for some $b \in \Sigma$.

Assume that a subset $S \subseteq Q$ and a word $u \in \Sigma^+$ are such that $|Su^{-1}| \neq |S|$ and u is a word of minimum length with this property. We write $u = aw$ for some $a \in \Sigma$ and $w \in \Sigma^*$ and let $P = Sw^{-1}$. Then $|P| = |S|$ by the choice of u and $Pa^{-1} = (Sw^{-1})a^{-1} = S(aw)^{-1} = Su^{-1}$ whence $|Pa^{-1}| \neq |P|$.

Thus, P must fall into the second of the above alternatives and so $|Pb^{-1}| > |P|$ for some $b \in \Sigma$. The word $v = bw$ has the same length as u and has the property that $|Sv^{-1}| > |S|$.

Assume that a subset $S \subseteq Q$ and a word $u \in \Sigma^+$ are such that $|Su^{-1}| \neq |S|$ and u is a word of minimum length with this property. We write $u = aw$ for some $a \in \Sigma$ and $w \in \Sigma^*$ and let $P = Sw^{-1}$. Then $|P| = |S|$ by the choice of u and $Pa^{-1} = (Sw^{-1})a^{-1} = S(aw)^{-1} = Su^{-1}$ whence $|Pa^{-1}| \neq |P|$.

Thus, P must fall into the second of the above alternatives and so $|Pb^{-1}| > |P|$ for some $b \in \Sigma$. The word $v = bw$ has the same length as u and has the property that $|Sv^{-1}| > |S|$. Having this in mind, we now aim to prove that *for every proper subset $S \subset Q$, there exists a word $u \in \Sigma^*$ of length at most $n-1$ such that $|Su^{-1}| \neq |S|$.*

Assume that a subset $S \subseteq Q$ and a word $u \in \Sigma^+$ are such that $|Su^{-1}| \neq |S|$ and u is a word of minimum length with this property. We write $u = aw$ for some $a \in \Sigma$ and $w \in \Sigma^*$ and let $P = Sw^{-1}$. Then $|P| = |S|$ by the choice of u and $Pa^{-1} = (Sw^{-1})a^{-1} = S(aw)^{-1} = Su^{-1}$ whence $|Pa^{-1}| \neq |P|$.

Thus, P must fall into the second of the above alternatives and so $|Pb^{-1}| > |P|$ for some $b \in \Sigma$. The word $v = bw$ has the same length as u and has the property that $|Sv^{-1}| > |S|$. Having this in mind, we now aim to prove that *for every proper subset* $S \subset Q$, *there exists a word* $u \in \Sigma^*$ *of length at most* $n - 1$ *such that* $|Su^{-1}| \neq |S|$. (This does not use the premise that $\mathscr{A}$ is Eulerian!)

Assume that a subset $S \subseteq Q$ and a word $u \in \Sigma^+$ are such that $|Su^{-1}| \neq |S|$ and u is a word of minimum length with this property. We write $u = aw$ for some $a \in \Sigma$ and $w \in \Sigma^*$ and let $P = Sw^{-1}$. Then $|P| = |S|$ by the choice of u and $Pa^{-1} = (Sw^{-1})a^{-1} = S(aw)^{-1} = Su^{-1}$ whence $|Pa^{-1}| \neq |P|$.

Thus, P must fall into the second of the above alternatives and so $|Pb^{-1}| > |P|$ for some $b \in \Sigma$. The word $v = bw$ has the same length as u and has the property that $|Sv^{-1}| > |S|$. Having this in mind, we now aim to prove that *for every proper subset $S \subset Q$, there exists a word $u \in \Sigma^*$ of length at most $n - 1$ such that $|Su^{-1}| \neq |S|$.* (This does not use the premise that $\mathscr{A}$ is Eulerian!) Then every proper subset can be extended by a word of length at most $n - 1$ whence $\mathscr{A}$ has a reset word of length at most

$$(n-2)(n-1) + 1 = n^2 - 3n + 3 < (n-1)^2.$$

Assume that $Q = \{1, 2, \ldots, n\}$. Assign to each subset $P \subseteq Q$ its characteristic vector $[P]$ in the linear space $\mathbb{R}^n$ of n-dimensional row vectors over $\mathbb{R}$ as follows: i-th entry of $[P]$ is 1 if $i \in P$, otherwise it is equal to 0.

Assume that $Q = \{1, 2, \ldots, n\}$. Assign to each subset $P \subseteq Q$ its characteristic vector $[P]$ in the linear space $\mathbb{R}^n$ of n-dimensional row vectors over $\mathbb{R}$ as follows: i-th entry of $[P]$ is 1 if $i \in P$, otherwise it is equal to 0.
For instance, $[Q]$ is the all ones row vector and the vectors $[1], \ldots, [n]$ form the standard basis of $\mathbb{R}^n$.

Assume that $Q = \{1, 2, \dots, n\}$. Assign to each subset $P \subseteq Q$ its characteristic vector $[P]$ in the linear space $\mathbb{R}^n$ of n-dimensional row vectors over $\mathbb{R}$ as follows: i-th entry of $[P]$ is 1 if $i \in P$, otherwise it is equal to 0.
For instance, $[Q]$ is the all ones row vector and the vectors $[1], \dots, [n]$ form the standard basis of $\mathbb{R}^n$.
Observe that for any vector $x \in \mathbb{R}^n$, the inner product $\langle x, [Q] \rangle$ is equal to the sum of all entries of x. In particular, for each subset $P \subseteq Q$, we have $\langle [P], [Q] \rangle = |P|$.

Assume that $Q = \{1, 2, \dots, n\}$. Assign to each subset $P \subseteq Q$ its characteristic vector $[P]$ in the linear space $\mathbb{R}^n$ of n-dimensional row vectors over $\mathbb{R}$ as follows: i-th entry of $[P]$ is 1 if $i \in P$, otherwise it is equal to 0.
For instance, $[Q]$ is the all ones row vector and the vectors $[1], \dots, [n]$ form the standard basis of $\mathbb{R}^n$.
Observe that for any vector $x \in \mathbb{R}^n$, the inner product $\langle x, [Q]\rangle$ is equal to the sum of all entries of x. In particular, for each subset $P \subseteq Q$, we have $\langle [P], [Q]\rangle = |P|$.

Assign to each word $w \in \Sigma^*$ the linear operator φ_w on $\mathbb{R}^n$ defined by $\varphi_w([i]) := [iw^{-1}]$ for each $i \in Q$.

Assume that $Q = \{1, 2, \dots, n\}$. Assign to each subset $P \subseteq Q$ its characteristic vector $[P]$ in the linear space $\mathbb{R}^n$ of n-dimensional row vectors over $\mathbb{R}$ as follows: i-th entry of $[P]$ is 1 if $i \in P$, otherwise it is equal to 0.
For instance, $[Q]$ is the all ones row vector and the vectors $[1], \dots, [n]$ form the standard basis of $\mathbb{R}^n$.
Observe that for any vector $x \in \mathbb{R}^n$, the inner product $\langle x, [Q] \rangle$ is equal to the sum of all entries of x. In particular, for each subset $P \subseteq Q$, we have $\langle [P], [Q] \rangle = |P|$.

Assign to each word $w \in \Sigma^*$ the linear operator φ_w on $\mathbb{R}^n$ defined by $\varphi_w([i]) := [iw^{-1}]$ for each $i \in Q$. Then for each $P \subseteq Q$, we get

$$\varphi_w([P]) = \varphi_w(\sum_{i \in P}[i]) = \sum_{i \in P} \varphi_w[i] = \sum_{i \in P}[iw^{-1}] = [Pw^{-1}].$$

The inequality $|Su^{-1}| \neq |S|$ that we look for can be rewritten as $\langle\varphi_u([S]), [Q]\rangle \neq \langle[S], [Q]\rangle$ or $\langle\varphi_u([S]) - [S], [Q]\rangle \neq 0$.

The inequality $|Su^{-1}| \neq |S|$ that we look for can be rewritten as $\langle \varphi_u([S]), [Q] \rangle \neq \langle [S], [Q] \rangle$ or $\langle \varphi_u([S]) - [S], [Q] \rangle \neq 0$.
Let $x = [S] - \frac{|S|}{n}[Q]$. Then $x \neq 0$ as $S \neq Q$ and $\langle x, [Q] \rangle = 0$. Since $Qu^{-1} = Q$ for every word u, we have $\varphi_u([Q]) = [Q]$.

The inequality $|Su^{-1}| \neq |S|$ that we look for can be rewritten as $\langle \varphi_u([S]), [Q]\rangle \neq \langle [S], [Q]\rangle$ or $\langle \varphi_u([S]) - [S], [Q]\rangle \neq 0$.
Let $x = [S] - \frac{|S|}{n}[Q]$. Then $x \neq 0$ as $S \neq Q$ and $\langle x, [Q]\rangle = 0$. Since $Qu^{-1} = Q$ for every word u, we have $\varphi_u([Q]) = [Q]$. Hence

$$\langle \varphi_u([S]) - [S], [Q]\rangle = \langle \varphi_u(x + \frac{|S|}{n}[Q]) - (x + \frac{|S|}{n}[Q]), [Q]\rangle =$$

The inequality $|Su^{-1}| \neq |S|$ that we look for can be rewritten as $\langle\varphi_u([S]), [Q]\rangle \neq \langle[S], [Q]\rangle$ or $\langle\varphi_u([S]) - [S], [Q]\rangle \neq 0$.
Let $x = [S] - \frac{|S|}{n}[Q]$. Then $x \neq 0$ as $S \neq Q$ and $\langle x, [Q]\rangle = 0$. Since $Qu^{-1} = Q$ for every word u, we have $\varphi_u([Q]) = [Q]$. Hence

$$\langle\varphi_u([S]) - [S], [Q]\rangle = \langle\varphi_u(x + \frac{|S|}{n}[Q]) - (x + \frac{|S|}{n}[Q]), [Q]\rangle =$$
$$\langle\varphi_u(x) + \frac{|S|}{n}[Q] - x - \frac{|S|}{n}[Q], [Q]\rangle = \langle\varphi_u(x) - x, [Q]\rangle = \langle\varphi_u(x), [Q]\rangle.$$

The inequality $|Su^{-1}| \neq |S|$ that we look for can be rewritten as $\langle \varphi_u([S]), [Q] \rangle \neq \langle [S], [Q] \rangle$ or $\langle \varphi_u([S]) - [S], [Q] \rangle \neq 0$.
Let $x = [S] - \frac{|S|}{n}[Q]$. Then $x \neq 0$ as $S \neq Q$ and $\langle x, [Q] \rangle = 0$. Since $Qu^{-1} = Q$ for every word u, we have $\varphi_u([Q]) = [Q]$. Hence

$$\langle \varphi_u([S]) - [S], [Q] \rangle = \langle \varphi_u(x + \frac{|S|}{n}[Q]) - (x + \frac{|S|}{n}[Q]), [Q] \rangle =$$
$$\langle \varphi_u(x) + \frac{|S|}{n}[Q] - x - \frac{|S|}{n}[Q], [Q] \rangle = \langle \varphi_u(x) - x, [Q] \rangle = \langle \varphi_u(x), [Q] \rangle.$$

Thus, u satisfies $|Su^{-1}| \neq |S|$ if and only if $\langle \varphi_u(x), [Q] \rangle \neq 0$.

The inequality $|Su^{-1}| \neq |S|$ that we look for can be rewritten as $\langle\varphi_u([S]), [Q]\rangle \neq \langle[S], [Q]\rangle$ or $\langle\varphi_u([S]) - [S], [Q]\rangle \neq 0$.
Let $x = [S] - \frac{|S|}{n}[Q]$. Then $x \neq 0$ as $S \neq Q$ and $\langle x, [Q]\rangle = 0$. Since $Qu^{-1} = Q$ for every word u, we have $\varphi_u([Q]) = [Q]$. Hence

$$\langle\varphi_u([S]) - [S], [Q]\rangle = \langle\varphi_u(x + \frac{|S|}{n}[Q]) - (x + \frac{|S|}{n}[Q]), [Q]\rangle =$$
$$\langle\varphi_u(x) + \frac{|S|}{n}[Q] - x - \frac{|S|}{n}[Q], [Q]\rangle = \langle\varphi_u(x) - x, [Q]\rangle = \langle\varphi_u(x), [Q]\rangle.$$

Thus, u satisfies $|Su^{-1}| \neq |S|$ if and only if $\langle\varphi_u(x), [Q]\rangle \neq 0$.
Let U be the subspace of all vectors orthogonal to the vector $[Q]$.

The inequality $|Su^{-1}| \neq |S|$ that we look for can be rewritten as $\langle \varphi_u([S]), [Q] \rangle \neq \langle [S], [Q] \rangle$ or $\langle \varphi_u([S]) - [S], [Q] \rangle \neq 0$.
Let $x = [S] - \frac{|S|}{n}[Q]$. Then $x \neq 0$ as $S \neq Q$ and $\langle x, [Q] \rangle = 0$. Since $Qu^{-1} = Q$ for every word u, we have $\varphi_u([Q]) = [Q]$. Hence

$$\langle \varphi_u([S]) - [S], [Q] \rangle = \langle \varphi_u(x + \frac{|S|}{n}[Q]) - (x + \frac{|S|}{n}[Q]), [Q] \rangle =$$
$$\langle \varphi_u(x) + \frac{|S|}{n}[Q] - x - \frac{|S|}{n}[Q], [Q] \rangle = \langle \varphi_u(x) - x, [Q] \rangle = \langle \varphi_u(x), [Q] \rangle.$$

Thus, u satisfies $|Su^{-1}| \neq |S|$ if and only if $\langle \varphi_u(x), [Q] \rangle \neq 0$.
Let U be the subspace of all vectors orthogonal to the vector $[Q]$. Then $x \in U$ and the inequality $\langle \varphi_u(x), [Q] \rangle \neq 0$ means that $\varphi_u(x) \notin U$.

The inequality $|Su^{-1}| \neq |S|$ that we look for can be rewritten as $\langle \varphi_u([S]), [Q] \rangle \neq \langle [S], [Q] \rangle$ or $\langle \varphi_u([S]) - [S], [Q] \rangle \neq 0$.
Let $x = [S] - \frac{|S|}{n}[Q]$. Then $x \neq 0$ as $S \neq Q$ and $\langle x, [Q] \rangle = 0$. Since $Qu^{-1} = Q$ for every word u, we have $\varphi_u([Q]) = [Q]$. Hence

$$\langle \varphi_u([S]) - [S], [Q] \rangle = \langle \varphi_u(x + \frac{|S|}{n}[Q]) - (x + \frac{|S|}{n}[Q]), [Q] \rangle =$$
$$\langle \varphi_u(x) + \frac{|S|}{n}[Q] - x - \frac{|S|}{n}[Q], [Q] \rangle = \langle \varphi_u(x) - x, [Q] \rangle = \langle \varphi_u(x), [Q] \rangle.$$

Thus, u satisfies $|Su^{-1}| \neq |S|$ if and only if $\langle \varphi_u(x), [Q] \rangle \neq 0$.
Let U be the subspace of all vectors orthogonal to the vector $[Q]$. Then $x \in U$ and the inequality $\langle \varphi_u(x), [Q] \rangle \neq 0$ means that $\varphi_u(x) \notin U$. We aim to bound the minimum length of such word u but first we explain why words sending x beyond U exist.

Since the automaton $\mathscr{A}$ is synchronizing and strongly connected, there exists a word $w \in \Sigma^*$ such that $Q\,.\,w \subseteq S$—one can first synchronize $\mathscr{A}$ to a state q and then move q into S by applying a word that labels a path from q to a state in S.

Since the automaton $\mathscr{A}$ is synchronizing and strongly connected, there exists a word $w \in \Sigma^*$ such that $Q\,.\,w \subseteq S$—one can first synchronize $\mathscr{A}$ to a state q and then move q into S by applying a word that labels a path from q to a state in S. Then we have $\varphi_w([S]) = [Q]$ whence

$$\varphi_w(x) = \varphi_w([S] - \frac{|S|}{n}[Q]) = \varphi_w([S]) - \frac{|S|}{n}\varphi_w([Q]) = (1 - \frac{|S|}{n})[Q] \neq 0.$$

Since the automaton $\mathscr{A}$ is synchronizing and strongly connected, there exists a word $w \in \Sigma^*$ such that $Q\,.\,w \subseteq S$—one can first synchronize $\mathscr{A}$ to a state q and then move q into S by applying a word that labels a path from q to a state in S. Then we have $\varphi_w([S]) = [Q]$ whence

$$\varphi_w(x) = \varphi_w([S] - \frac{|S|}{n}[Q]) = \varphi_w([S]) - \frac{|S|}{n}\varphi_w([Q]) = (1 - \frac{|S|}{n})[Q] \neq 0.$$

Now consider the chain of subspaces $U_0 \subseteq U_1 \subseteq \dots$, where U_j is spanned by all vectors of the form $\varphi_w(x)$ with $|w| \leq j$.

Since the automaton $\mathscr{A}$ is synchronizing and strongly connected, there exists a word $w \in \Sigma^*$ such that $Q\,.\,w \subseteq S$—one can first synchronize $\mathscr{A}$ to a state q and then move q into S by applying a word that labels a path from q to a state in S. Then we have $\varphi_w([S]) = [Q]$ whence

$$\varphi_w(x) = \varphi_w([S] - \frac{|S|}{n}[Q]) = \varphi_w([S]) - \frac{|S|}{n}\varphi_w([Q]) = (1 - \frac{|S|}{n})[Q] \neq 0.$$

Now consider the chain of subspaces $U_0 \subseteq U_1 \subseteq \dots$, where U_j is spanned by all vectors of the form $\varphi_w(x)$ with $|w| \leq j$. Clearly, if $U_{j+1} = U_j$ for some j, then $\varphi_a(U_j) \subseteq U_j$ for all $a \in \Sigma$ whence $U_i = U_j$ for every $i \geq j$.

Since the automaton $\mathscr{A}$ is synchronizing and strongly connected, there exists a word $w \in \Sigma^*$ such that $Q\,.\,w \subseteq S$—one can first synchronize $\mathscr{A}$ to a state q and then move q into S by applying a word that labels a path from q to a state in S. Then we have $\varphi_w([S]) = [Q]$ whence

$$\varphi_w(x) = \varphi_w([S] - \frac{|S|}{n}[Q]) = \varphi_w([S]) - \frac{|S|}{n}\varphi_w([Q]) = (1 - \frac{|S|}{n})[Q] \neq 0.$$

Now consider the chain of subspaces $U_0 \subseteq U_1 \subseteq \ldots$, where U_j is spanned by all vectors of the form $\varphi_w(x)$ with $|w| \leq j$. Clearly, if $U_{j+1} = U_j$ for some j, then $\varphi_a(U_j) \subseteq U_j$ for all $a \in \Sigma$ whence $U_i = U_j$ for every $i \geq j$. Let ℓ be the least number such that $\varphi_u(x) \notin U$ for some word u of length ℓ, that is, the smallest ℓ such that $U_\ell \nsubseteq U$. Then in the chain $U_0 \subset U_1 \subset \cdots \subset U_\ell$ all inclusions are strict.

Hence

$$1 = \dim U_0 < \dim U_1 < \cdots < \dim U_{\ell-1} < \dim U_\ell$$

and, in particular, $\dim U_{\ell-1} \geq \ell$.

Hence

$$1 = \dim U_0 < \dim U_1 < \cdots < \dim U_{\ell-1} < \dim U_\ell$$

and, in particular, $\dim U_{\ell-1} \geq \ell$. But by our choice of ℓ we have $U_{\ell-1} \subseteq U$ whence $\dim U_{\ell-1} \leq \dim U$.

Hence

$$1 = \dim U_0 < \dim U_1 < \cdots < \dim U_{\ell-1} < \dim U_\ell$$

and, in particular, $\dim U_{\ell-1} \geq \ell$. But by our choice of ℓ we have $U_{\ell-1} \subseteq U$ whence $\dim U_{\ell-1} \leq \dim U$. Since U is the orthogonal complement of a 1-dimensional subspace, $\dim U = n - 1$, and we conclude that $\ell \leq n - 1$.

Hence

$$1 = \dim U_0 < \dim U_1 < \cdots < \dim U_{\ell-1} < \dim U_\ell$$

and, in particular, $\dim U_{\ell-1} \geq \ell$. But by our choice of ℓ we have $U_{\ell-1} \subseteq U$ whence $\dim U_{\ell-1} \leq \dim U$. Since U is the orthogonal complement of a 1-dimensional subspace, $\dim U = n - 1$, and we conclude that $\ell \leq n - 1$.

Thus, we have proved that for every proper subset $S \subset Q$, there exists a word $u \in \Sigma^*$ with $|u| \leq n - 1$ such that $|Su^{-1}| \neq |S|$.

Hence

$$1 = \dim U_0 < \dim U_1 < \cdots < \dim U_{\ell-1} < \dim U_\ell$$

and, in particular, $\dim U_{\ell-1} \geq \ell$. But by our choice of ℓ we have $U_{\ell-1} \subseteq U$ whence $\dim U_{\ell-1} \leq \dim U$. Since U is the orthogonal complement of a 1-dimensional subspace, $\dim U = n-1$, and we conclude that $\ell \leq n-1$.

Thus, we have proved that for every proper subset $S \subset Q$, there exists a word $u \in \Sigma^*$ with $|u| \leq n-1$ such that $|Su^{-1}| \neq |S|$.
Recall that for Eulerian automata this implies that every proper subset can be extended by a word of length at most $n-1$

Hence

$$1 = \dim U_0 < \dim U_1 < \cdots < \dim U_{\ell-1} < \dim U_\ell$$

and, in particular, $\dim U_{\ell-1} \geq \ell$. But by our choice of ℓ we have $U_{\ell-1} \subseteq U$ whence $\dim U_{\ell-1} \leq \dim U$. Since U is the orthogonal complement of a 1-dimensional subspace, $\dim U = n-1$, and we conclude that $\ell \leq n-1$.

Thus, we have proved that for every proper subset $S \subset Q$, there exists a word $u \in \Sigma^*$ with $|u| \leq n-1$ such that $|Su^{-1}| \neq |S|$.
Recall that for Eulerian automata this implies that every proper subset can be extended by a word of length at most $n-1$ whence $\mathscr{A}$ has a reset word of length at most

$$(n-2)(n-1)+1 = n^2 - 3n + 3 < (n-1)^2.$$

Kari's upper bound $n^2 - 3n + 3$ is far from being tight.

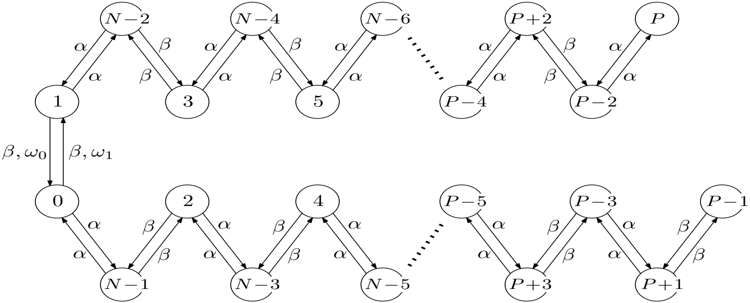
Kari's upper bound $n^2 - 3n + 3$ is far from being tight.
The best theoretical lower bounds for the restriction of the Černý function to the class of Eulerian synchronizing automata known so far are of magnitude $\frac{n^2}{2}$ (Pavel Martyugin, Vladimir Gusev, Marek Szykuła, Vojtěch Vorel).

Martyugin found a series of Eulerian synchronizing automata with n states and 2 letters whose reset threshold is $\lfloor \frac{n^2-5}{2} \rfloor$.

Martyugin found a series of Eulerian synchronizing automata with n states and 2 letters whose reset threshold is $\lfloor\frac{n^2-5}{2}\rfloor$. Szykuła and Vorel (An extremal series of Eulerian synchronizing automata, DLT 2016, LNCS 9840, 380–392 (2016)) constructed a series of Eulerian synchronizing automata with $N = 4m + 1$ states and 4 letters $\alpha, \beta, \omega_0, \omega_1$ whose reset threshold is $\frac{N^2-3}{2}$.

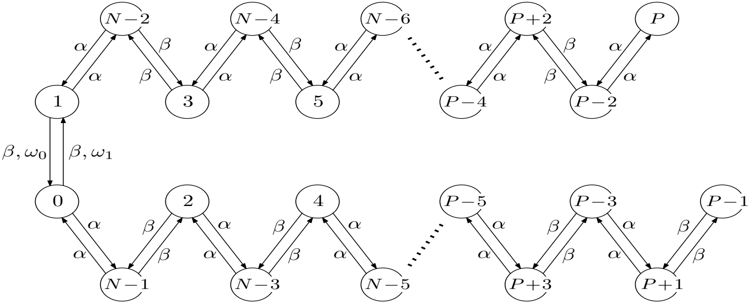
18. Open Problem

Martyugin found a series of Eulerian synchronizing automata with n states and 2 letters whose reset threshold is $\lfloor\frac{n^2-5}{2}\rfloor$. Szykuła and Vorel (An extremal series of Eulerian synchronizing automata, DLT 2016, LNCS 9840, 380–392 (2016)) constructed a series of Eulerian synchronizing automata with $N = 4m + 1$ states and 4 letters $\alpha, \beta, \omega_0, \omega_1$ whose reset threshold is $\frac{N^2-3}{2}$.



$P = \frac{N+1}{2}$, loops are not shown.

Martyugin found a series of Eulerian synchronizing automata with n states and 2 letters whose reset threshold is $\lfloor\frac{n^2-5}{2}\rfloor$. Szykuła and Vorel (An extremal series of Eulerian synchronizing automata, DLT 2016, LNCS 9840, 380–392 (2016)) constructed a series of Eulerian synchronizing automata with $N = 4m + 1$ states and 4 letters $\alpha, \beta, \omega_0, \omega_1$ whose reset threshold is $\frac{N^2-3}{2}$.



$P = \frac{N+1}{2}$, loops are not shown. The proof is quite non-trivial.

Gusev (Lower bounds for the length of reset words in Eulerian automata, Reachability Problems, LNCS 6945, 180–190 (2011)) has constructed another series of Eulerian synchronizing automata with n states and 2 input letters whose reset threshold is $\frac{n^2-3n+4}{2}$.

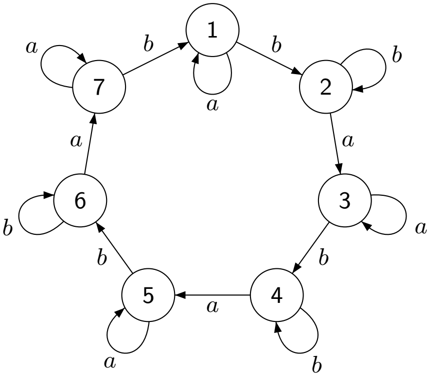
Gusev (Lower bounds for the length of reset words in Eulerian automata, Reachability Problems, LNCS 6945, 180–190 (2011)) has constructed another series of Eulerian synchronizing automata with n states and 2 input letters whose reset threshold is $\frac{n^2-3n+4}{2}$. The construction and the proof are rather elegant.

Define the automaton $\mathscr{M}_n$ (from Matricaria) on the state set $\{1, 2, \dots, n\}$, where $n \geq 5$ is odd, in which a and b act as follows:

$$k \, . \, a = \begin{cases} k & \text{if } k \text{ is odd,} \\ k+1 & \text{if } k \text{ is even;} \end{cases} \quad k \, . \, b = \begin{cases} k+1 & \text{if } k \neq n \text{ is odd,} \\ k & \text{if } k \text{ is even,} \\ 1 & \text{if } k = n. \end{cases}$$

Define the automaton $\mathscr{M}_n$ (from Matricaria) on the state set $\{1, 2, \dots, n\}$, where $n \geq 5$ is odd, in which a and b act as follows:

$$k\,.\,a = \begin{cases} k & \text{if } k \text{ is odd,} \\ k+1 & \text{if } k \text{ is even;} \end{cases} \qquad k\,.\,b = \begin{cases} k+1 & \text{if } k \neq n \text{ is odd,} \\ k & \text{if } k \text{ is even,} \\ 1 & \text{if } k = n. \end{cases}$$



Observe that $\mathscr{M}_n$ is Eulerian.

Observe that $\mathscr{M}_n$ is Eulerian. One can verify that the word $b(b(ab)^{\frac{n-1}{2}})^{\frac{n-3}{2}}b$ of length $\frac{n^2-3n+4}{2}$ is a reset word for $\mathscr{M}_n$.

Observe that $\mathscr{M}_n$ is Eulerian. One can verify that the word $b(b(ab)^{\frac{n-1}{2}})^{\frac{n-3}{2}}b$ of length $\frac{n^2-3n+4}{2}$ is a reset word for $\mathscr{M}_n$.

Now let w be a reset word of minimum length for $\mathscr{M}_n$.

Observe that $\mathscr{M}_n$ is Eulerian. One can verify that the word $b(b(ab)^{\frac{n-1}{2}})^{\frac{n-3}{2}}b$ of length $\frac{n^2-3n+4}{2}$ is a reset word for $\mathscr{M}_n$.

Now let w be a reset word of minimum length for $\mathscr{M}_n$. The action of aa is the same as the action of a. Therefore aa could not be a factor of w. (Otherwise reducing this factor to just a results in a shorter reset word.)

Observe that $\mathscr{M}_n$ is Eulerian. One can verify that the word $b(b(ab)^{\frac{n-1}{2}})^{\frac{n-3}{2}}b$ of length $\frac{n^2-3n+4}{2}$ is a reset word for $\mathscr{M}_n$.

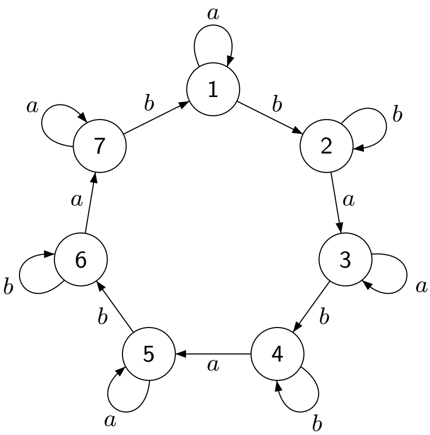
Now let w be a reset word of minimum length for $\mathscr{M}_n$. The action of aa is the same as the action of a. Therefore aa could not be a factor of w. (Otherwise reducing this factor to just a results in a shorter reset word.) So every occurrence of a, maybe except the last one, is followed by b.

Observe that $\mathscr{M}_n$ is Eulerian. One can verify that the word $b(b(ab)^{\frac{n-1}{2}})^{\frac{n-3}{2}}b$ of length $\frac{n^2-3n+4}{2}$ is a reset word for $\mathscr{M}_n$.

Now let w be a reset word of minimum length for $\mathscr{M}_n$. The action of aa is the same as the action of a. Therefore aa could not be a factor of w. (Otherwise reducing this factor to just a results in a shorter reset word.) So every occurrence of a, maybe except the last one, is followed by b. If we let $c = ab$, then either w or wb (if w ends with a) can be rewritten into a word u over the alphabet $\{b, c\}$.

Observe that $\mathscr{M}_n$ is Eulerian. One can verify that the word $b(b(ab)^{\frac{n-1}{2}})^{\frac{n-3}{2}}b$ of length $\frac{n^2-3n+4}{2}$ is a reset word for $\mathscr{M}_n$.

Now let w be a reset word of minimum length for $\mathscr{M}_n$. The action of aa is the same as the action of a. Therefore aa could not be a factor of w. (Otherwise reducing this factor to just a results in a shorter reset word.) So every occurrence of a, maybe except the last one, is followed by b. If we let $c = ab$, then either w or wb (if w ends with a) can be rewritten into a word u over the alphabet $\{b, c\}$. The actions of b and c induce a new automaton on the state set of $\mathscr{M}_n$ and u is easily seen to be a reset word for this new automaton.



The automaton $\mathscr{M}_7$ and the automaton induced by the actions of b and $c = ab$

After applying the first letter of u it remains to synchronize the subautomaton on the set of states $S = \{1\} \cup \{2k \mid 1 \leq k \leq \frac{n-1}{2}\}$, and this subautomaton is isomorphic to $\mathscr{C}_{\frac{n+1}{2}}$.

After applying the first letter of u it remains to synchronize the subautomaton on the set of states $S = \{1\} \cup \{2k \mid 1 \leq k \leq \frac{n-1}{2}\}$, and this subautomaton is isomorphic to $\mathscr{C}_{\frac{n+1}{2}}$. Thus, if $u = xu'$ for some letter x, then u' is a reset word for $\mathscr{C}_{\frac{n+1}{2}}$ and it can be shown that u' has at least $(\frac{n+1}{2})^2 - 3(\frac{n+1}{2}) + 2 = \frac{n^2-4n+3}{4}$ occurrences of c and at least $\frac{n-1}{2}$ occurrences of b.

After applying the first letter of u it remains to synchronize the subautomaton on the set of states $S = \{1\} \cup \{2k \mid 1 \leq k \leq \frac{n-1}{2}\}$, and this subautomaton is isomorphic to $\mathscr{C}_{\frac{n+1}{2}}$. Thus, if $u = xu'$ for some letter x, then u' is a reset word for $\mathscr{C}_{\frac{n+1}{2}}$ and it can be shown that u' has at least $(\frac{n+1}{2})^2 - 3(\frac{n+1}{2}) + 2 = \frac{n^2-4n+3}{4}$ occurrences of c and at least $\frac{n-1}{2}$ occurrences of b. Since each occurrence of c in u' corresponds to an occurrence of the factor ab in w, we conclude that the length of w is at least $1 + 2\frac{n^2-4n+3}{4} + \frac{n-1}{2} = \frac{n^2-3n+4}{2}$.

After applying the first letter of u it remains to synchronize the subautomaton on the set of states $S = \{1\} \cup \{2k \mid 1 \leq k \leq \frac{n-1}{2}\}$, and this subautomaton is isomorphic to $\mathscr{C}_{\frac{n+1}{2}}$. Thus, if $u = xu'$ for some letter x, then u' is a reset word for $\mathscr{C}_{\frac{n+1}{2}}$ and it can be shown that u' has at least $(\frac{n+1}{2})^2 - 3(\frac{n+1}{2}) + 2 = \frac{n^2-4n+3}{4}$ occurrences of c and at least $\frac{n-1}{2}$ occurrences of b. Since each occurrence of c in u' corresponds to an occurrence of the factor ab in w, we conclude that the length of w is at least $1 + 2\frac{n^2-4n+3}{4} + \frac{n-1}{2} = \frac{n^2-3n+4}{2}$.

Thus, if $C_E(n)$ is the restriction of the Černý function to the class of Eulerian automata, then

After applying the first letter of u it remains to synchronize the subautomaton on the set of states $S = \{1\} \cup \{2k \mid 1 \leq k \leq \frac{n-1}{2}\}$, and this subautomaton is isomorphic to $\mathscr{C}_{\frac{n+1}{2}}$. Thus, if $u = xu'$ for some letter x, then u' is a reset word for $\mathscr{C}_{\frac{n+1}{2}}$ and it can be shown that u' has at least $(\frac{n+1}{2})^2 - 3(\frac{n+1}{2}) + 2 = \frac{n^2-4n+3}{4}$ occurrences of c and at least $\frac{n-1}{2}$ occurrences of b. Since each occurrence of c in u' corresponds to an occurrence of the factor ab in w, we conclude that the length of w is at least $1 + 2\frac{n^2-4n+3}{4} + \frac{n-1}{2} = \frac{n^2-3n+4}{2}$.

Thus, if $C_E(n)$ is the restriction of the Černý function to the class of Eulerian automata, then

$$\text{(Szykuła and Vorel, 2016)} \quad \frac{n^2-3}{2} \leq C_E(n)$$

After applying the first letter of u it remains to synchronize the subautomaton on the set of states $S = \{1\} \cup \{2k \mid 1 \le k \le \frac{n-1}{2}\}$, and this subautomaton is isomorphic to $\mathscr{C}_{\frac{n+1}{2}}$. Thus, if $u = xu'$ for some letter x, then u' is a reset word for $\mathscr{C}_{\frac{n+1}{2}}$ and it can be shown that u' has at least $(\frac{n+1}{2})^2 - 3(\frac{n+1}{2}) + 2 = \frac{n^2-4n+3}{4}$ occurrences of c and at least $\frac{n-1}{2}$ occurrences of b. Since each occurrence of c in u' corresponds to an occurrence of the factor ab in w, we conclude that the length of w is at least $1 + 2\frac{n^2-4n+3}{4} + \frac{n-1}{2} = \frac{n^2-3n+4}{2}$.

Thus, if $C_E(n)$ is the restriction of the Černý function to the class of Eulerian automata, then

(Szykuła and Vorel, 2016) $\dfrac{n^2-3}{2} \le C_E(n) \le n^2 - 3n + 3$ (Kari, 2003).

Back to extensibility, in $\mathscr{K}_6$ there exists a 2-subset that cannot be extended to a larger subset by any word of length 6 (and even by any word of length 7).

23. Extensibility vs Kari's Example

Back to extensibility, in $\mathscr{K}_6$ there exists a 2-subset that cannot be extended to a larger subset by any word of length 6 (and even by any word of length 7). Thus, the extensibility conjecture fails, and the approach based on it cannot prove the Černý conjecture in general.

23. Extensibility vs Kari's Example

Back to extensibility, in $\mathscr{K}_6$ there exists a 2-subset that cannot be extended to a larger subset by any word of length 6 (and even by any word of length 7). Thus, the extensibility conjecture fails, and the approach based on it cannot prove the Černý conjecture in general.

However, studying the extensibility phenomenon in synchronizing automata appears to be worthwhile: if there is a linear bound on the minimum length of words extending non-singleton proper subsets of a synchronizing automaton, then there is a quadratic bound on the minimum length of reset words for the automaton.

24. Extension Algorithm

GREEDYEXTENSTION($\mathscr{A}$)

if $|qa^{-1}| = 1$ for all $q \in Q$ and $a \in \Sigma$ **then**
  return Failure
else
  $w \leftarrow a$ such that $|qa^{-1}| > 1$ ▷ Initializing the current word
  $P \leftarrow qa^{-1}$ such that $|qa^{-1}| > 1$ ▷ Initializing the current set
while $|P| < |Q|$ **do**
  if $|Pu^{-1}| \leq |P|$ for all $u \in \Sigma^*$ **then**
    return Failure
  else
    take a word $v \in \Sigma^*$ of minimum length with $|Pv^{-1}| > |P|$
  $w \leftarrow vw$ ▷ Updating the current word
  $P \leftarrow Pv^{-1}$ ▷ Updating the current set
return w

In contrast to Compression Algorithm, it is not clear whether Extension Algorithm admits a polynomial-time implementation.

In contrast to Compression Algorithm, it is not clear whether Extension Algorithm admits a polynomial-time implementation. Moreover, in general we know no non-trivial bound on the length of the words v that the main loop of Extension Algorithm appends to the current word.

In contrast to Compression Algorithm, it is not clear whether Extension Algorithm admits a polynomial-time implementation. Moreover, in general we know no non-trivial bound on the length of the words v that the main loop of Extension Algorithm appends to the current word. However, one can isolate some cases in which rather strong bounds on $|v|$ do exist.

In contrast to Compression Algorithm, it is not clear whether Extension Algorithm admits a polynomial-time implementation. Moreover, in general we know no non-trivial bound on the length of the words v that the main loop of Extension Algorithm appends to the current word. However, one can isolate some cases in which rather strong bounds on $|v|$ do exist.

Let α be a positive real number. An automaton $\mathscr{A} = \langle Q, \Sigma, \delta \rangle$ is α-extensible if for any subset $P \subset Q$ there is $w \in \Sigma^*$ of length at most $\alpha|Q|$ such that $|Pw^{-1}| > |P|$.

In contrast to Compression Algorithm, it is not clear whether Extension Algorithm admits a polynomial-time implementation. Moreover, in general we know no non-trivial bound on the length of the words v that the main loop of Extension Algorithm appends to the current word. However, one can isolate some cases in which rather strong bounds on $|v|$ do exist.

Let α be a positive real number. An automaton $\mathscr{A} = \langle Q, \Sigma, \delta \rangle$ is α-extensible if for any subset $P \subset Q$ there is $w \in \Sigma^*$ of length at most $\alpha|Q|$ such that $|Pw^{-1}| > |P|$.

An α-extensible automaton with n states has a reset word of length $\alpha n^2 + O(n)$.

In contrast to Compression Algorithm, it is not clear whether Extension Algorithm admits a polynomial-time implementation. Moreover, in general we know no non-trivial bound on the length of the words v that the main loop of Extension Algorithm appends to the current word. However, one can isolate some cases in which rather strong bounds on $|v|$ do exist.

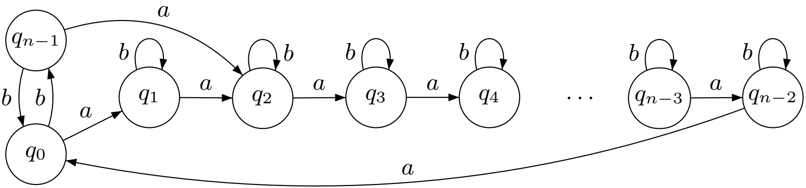
Let α be a positive real number. An automaton $\mathscr{A} = \langle Q, \Sigma, \delta \rangle$ is α-extensible if for any subset $P \subset Q$ there is $w \in \Sigma^*$ of length at most $\alpha|Q|$ such that $|Pw^{-1}| > |P|$.

An α-extensible automaton with n states has a reset word of length $\alpha n^2 + O(n)$.

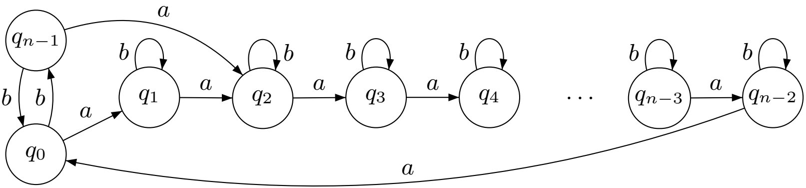
Several important classes of synchronizing automata are known to be 2-extensible, for instance, one-cluster automata (Marie-Pierre Béal, Mikhail Berlinkov, Dominique Perrin, A quadratic upper bound on the size of a synchronizing word in one-cluster automata, Int. J. Found. Comput. Sci., 22, 277–288 (2011)).

On the other hand, for any $\alpha < 2$ Mikhail Berlinkov (On a conjecture by Carpi and D'Alessandro, Int. J. Found. Comput. Sci. 22, 1565–1576 (2011)) constructed a synchronizing one-cluster automaton that is not α-extensible.

On the other hand, for any $\alpha < 2$ Mikhail Berlinkov (On a conjecture by Carpi and D'Alessandro, Int. J. Found. Comput. Sci. 22, 1565–1576 (2011)) constructed a synchronizing one-cluster automaton that is not α-extensible.

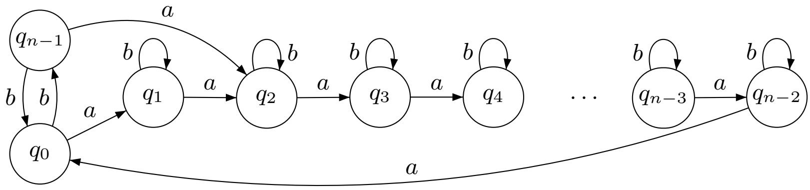


On the other hand, for any $\alpha < 2$ Mikhail Berlinkov (On a conjecture by Carpi and D'Alessandro, Int. J. Found. Comput. Sci. 22, 1565–1576 (2011)) constructed a synchronizing one-cluster automaton that is not α-extensible.



For $n > \frac{3}{2-\alpha}$, this automaton is not α-extensible.

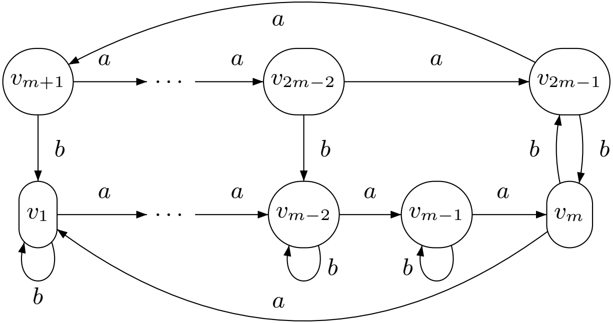
On the other hand, for any $\alpha < 2$ Mikhail Berlinkov (On a conjecture by Carpi and D'Alessandro, Int. J. Found. Comput. Sci. 22, 1565–1576 (2011)) constructed a synchronizing one-cluster automaton that is not α-extensible.



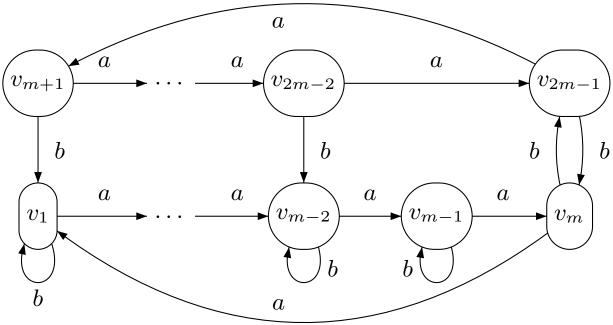
For $n > \frac{3}{2-\alpha}$, this automaton is not α-extensible. In fact, the shortest word that extends the set $\{q_0, q_{n-1}\}$ is $a^{n-2}ba^{n-2}$.

Finally, Andrzej Kisielewicz and Marek Szykuła (Synchronizing automata with extremal properties, MFCS 2015, LNCS 9234, 331–343 (2015)) constructed a series of synchronizing automata that are not α-extensible for any α.

Finally, Andrzej Kisielewicz and Marek Szykuła (Synchronizing automata with extremal properties, MFCS 2015, LNCS 9234, 331–343 (2015)) constructed a series of synchronizing automata that are not α-extensible for any α.



Finally, Andrzej Kisielewicz and Marek Szykuła (Synchronizing automata with extremal properties, MFCS 2015, LNCS 9234, 331–343 (2015)) constructed a series of synchronizing automata that are not α-extensible for any α.



The automata in the series have subsets that require words of length as big as $m^2 + O(m)$ in order to be extended.

Open problem: to investigate the worst-case/average-case behaviour of the greedy extension algorithm.

Open problem: to investigate the worst-case/average-case behaviour of the greedy extension algorithm.

Some experimental work that can be used in this direction has been done by Adam Roman and Marek Szykuła (Forward and backward synchronizing algorithms, Expert Systems with Applications, 42, 9512–9527 (2015)).