Synchronizing Automata – II

M. V. Volkov

Ural State University, Ekaterinburg, Russia

Synchronizing automata – Recap

We consider DFA: $\mathscr{A} = \langle Q, \Sigma, \delta \rangle$.

Synchronizing automata – Recap

We consider DFA: $\mathscr{A} = \langle Q, \Sigma, \delta \rangle$.

The DFA $\mathscr{A}$ 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.

Synchronizing automata – Recap

We consider DFA: $\mathscr{A} = \langle Q, \Sigma, \delta \rangle$.

The DFA $\mathscr{A}$ 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.
$|Q \,.\, w| = 1$. Here $Q \,.\, v = \{\delta(q, v) \mid q \in Q\}$.

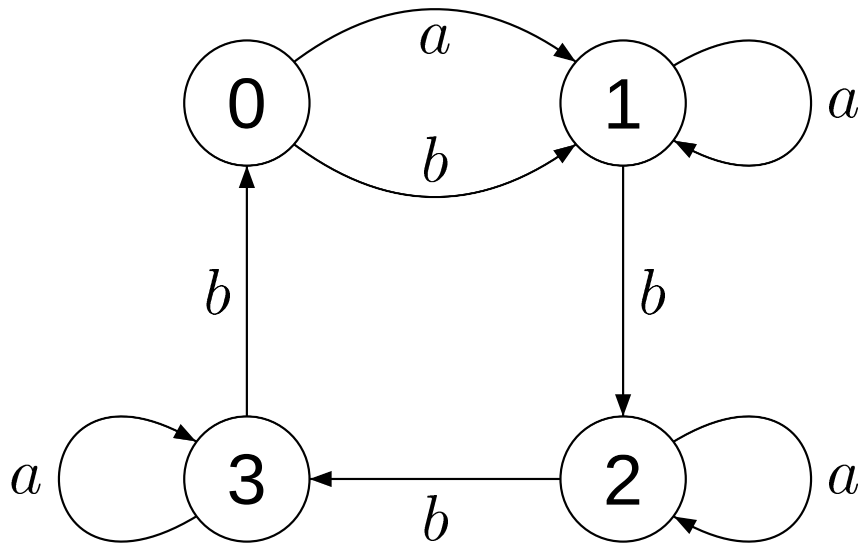
Synchronizing automata – Recap

We consider DFA: $\mathscr{A} = \langle Q, \Sigma, \delta \rangle$.

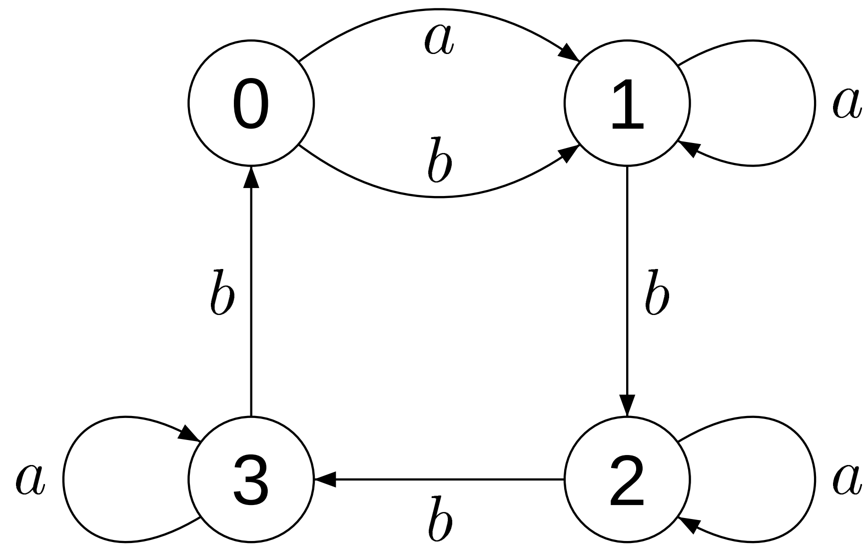
The DFA $\mathscr{A}$ is called *synchronizing* if there exists a word $w \in \Sigma^*$ whose action resets $\mathscr{A}$, that is, leaves the automaton in one particular state no matter which state in Q it started at.
$|Q\,.\,w| = 1$. Here $Q\,.\,v = \{\delta(q, v) \mid q \in Q\}$.

Any w with this property is said to be a *reset word* for the automaton.

Synchronizing automata – Recap



Synchronizing automata – Recap



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

The Černý automata

Suppose a synchronizing automaton has n states.
What is the length of its shortest reset word?

The Černý automata

Suppose a synchronizing automaton has n states. What is the length of its shortest reset word?

We know an upper bound: there always exists a reset word of length $\frac{n^3-n}{6}$. What about a lower bound?

The Černý automata

Suppose a synchronizing automaton has n states. What is the length of its shortest reset word?
We know an upper bound: there always exists a reset word of length $\frac{n^3-n}{6}$. What about a lower bound?

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

The Černý automata

Suppose a synchronizing automaton has n states. What is the length of its shortest reset word?
We know an upper bound: there always exists a reset word of length $\frac{n^3-n}{6}$. What about a lower bound?
In his 1964 paper Jan Černý constructed a series $\mathscr{C}_n$, $n = 2, 3, \ldots$, of synchronizing automata over 2 letters.
The states of $\mathscr{C}_n$ are the residues modulo n, and the input letters a and b act as follows:

$$\delta(0,a) = 1,\ \delta(m,a) = m \text{ for } 0 < m < n,\ \delta(m,b) = m+1 \pmod n$$

The Černý automata

Suppose a synchronizing automaton has n states. What is the length of its shortest reset word? We know an upper bound: there always exists a reset word of length $\frac{n^3-n}{6}$. What about a lower bound?

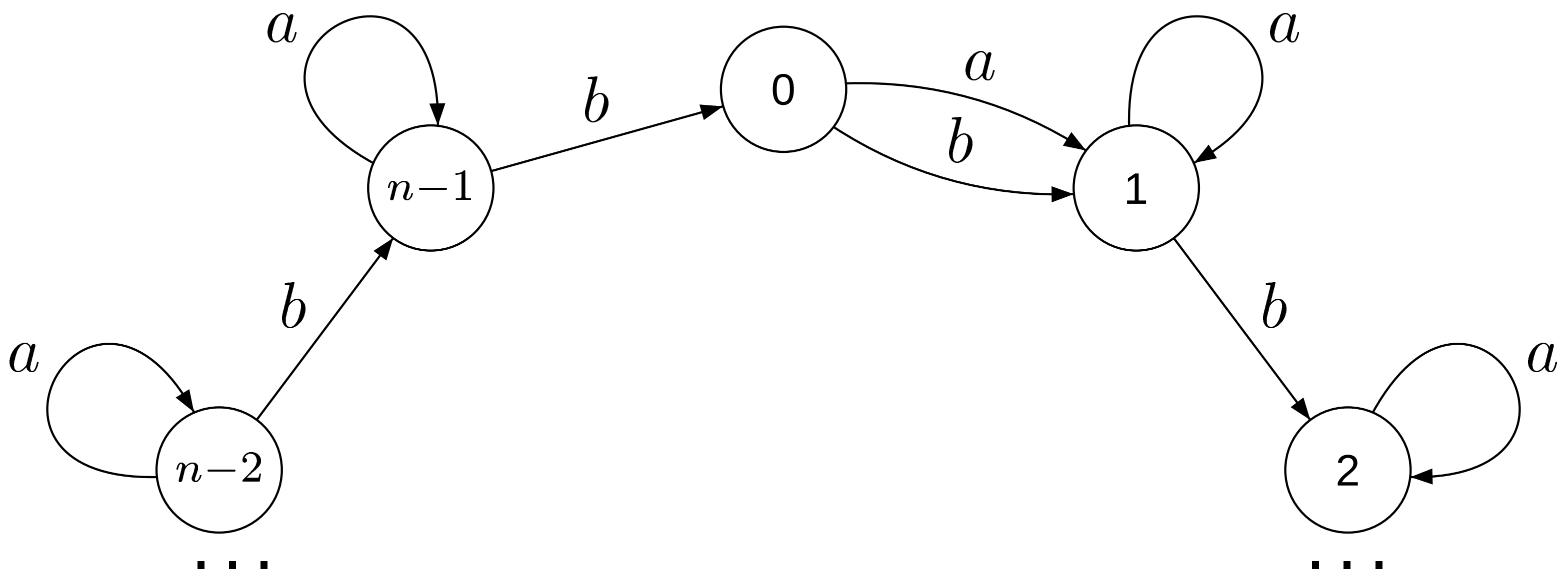
In his 1964 paper Jan Černý constructed a series $\mathscr{C}_n$, $n = 2, 3, \dots$, of synchronizing automata over 2 letters. The states of $\mathscr{C}_n$ are the residues modulo n, and the input letters a and b act as follows:

$$\delta(0, a) = 1,\ \delta(m, a) = m \text{ for } 0 < m < n,\ \delta(m, b) = m+1 \pmod{n}$$

The automaton in the previous slide is $\mathscr{C}_4$.

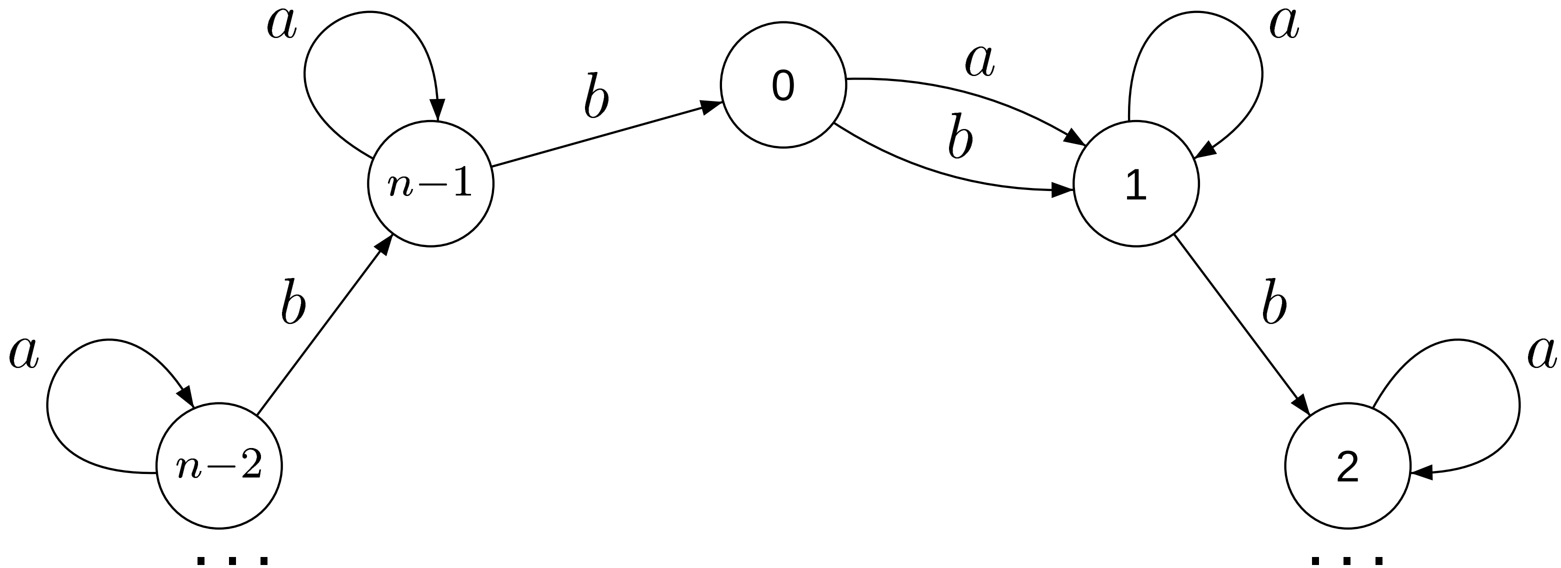
The Černý automata

Here is a generic automaton from the Černý series:



The Černý automata

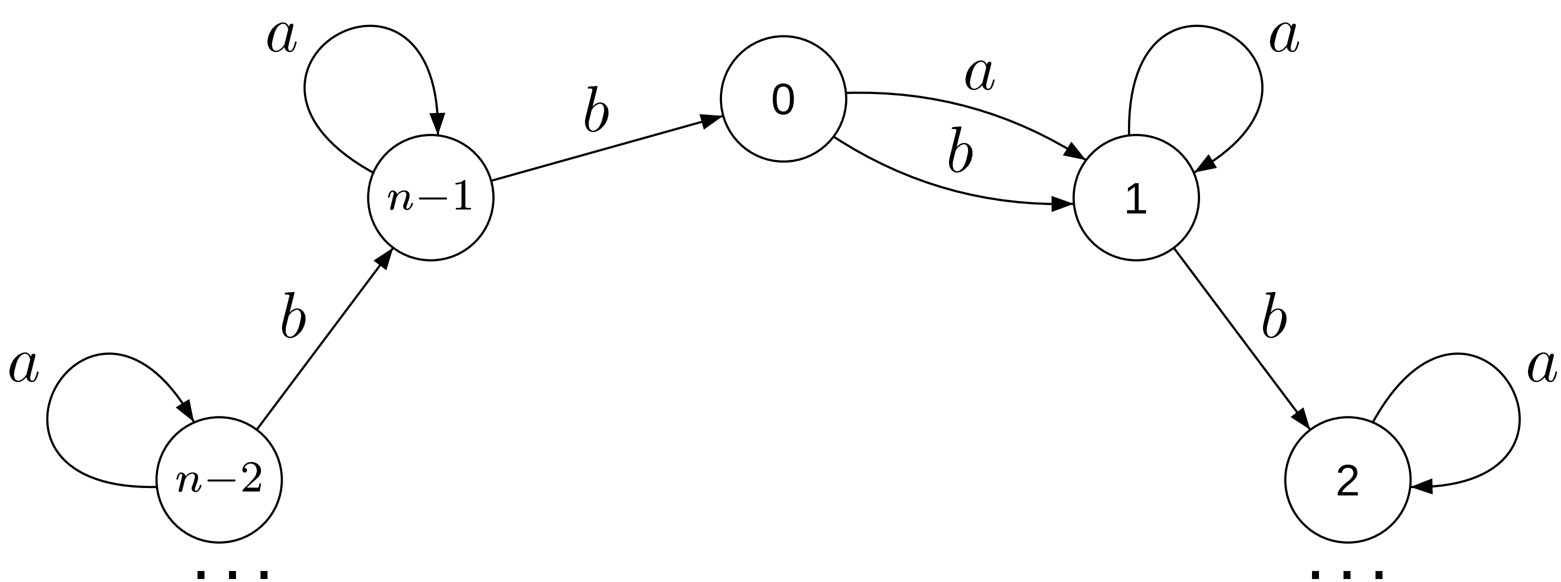
Here is a generic automaton from the Černý series:



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

The Černý automata

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 $(n-1)^2$. As other results from Černý's paper of 1964, this nice series of automata has been rediscovered many times, see references in the pre-proceedings.

The Černý automata

We present a proof of this result using a solitaire-like game:

The Černý automata

We present a proof of this result using a solitaire-like game:

- The digraph of $\mathscr{C}_n$ — the game-board.

The Černý automata

We present a proof of this result using a solitaire-like game:

- The digraph of $\mathscr{C}_n$ — the game-board.
- The initial position — each state holds a coin, all coins are pairwise distinct.

The Černý automata

We present a proof of this result using a solitaire-like game:

- The digraph of $\mathscr{C}_n$ — the game-board.
- The initial position — each state holds a coin, all coins are pairwise distinct.
- Each letter $c \in \{a, b\}$ defines a move — coins slide along the arrows labelled c and, whenever two coins meet at the state 1, the coin arriving from 0 is removed.

The Černý automata

We present a proof of this result using a solitaire-like game:

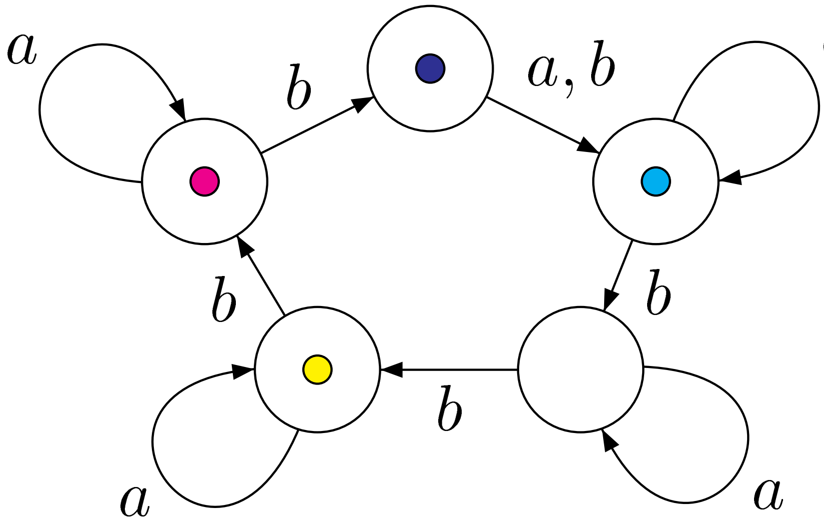
- The digraph of $\mathscr{C}_n$ — the game-board.
- The initial position — each state holds a coin, all coins are pairwise distinct.
- Each letter $c \in \{a, b\}$ defines a move — coins slide along the arrows labelled c and, whenever two coins meet at the state 1, the coin arriving from 0 is removed.
- The goal — to free all but one states.

The Černý automata

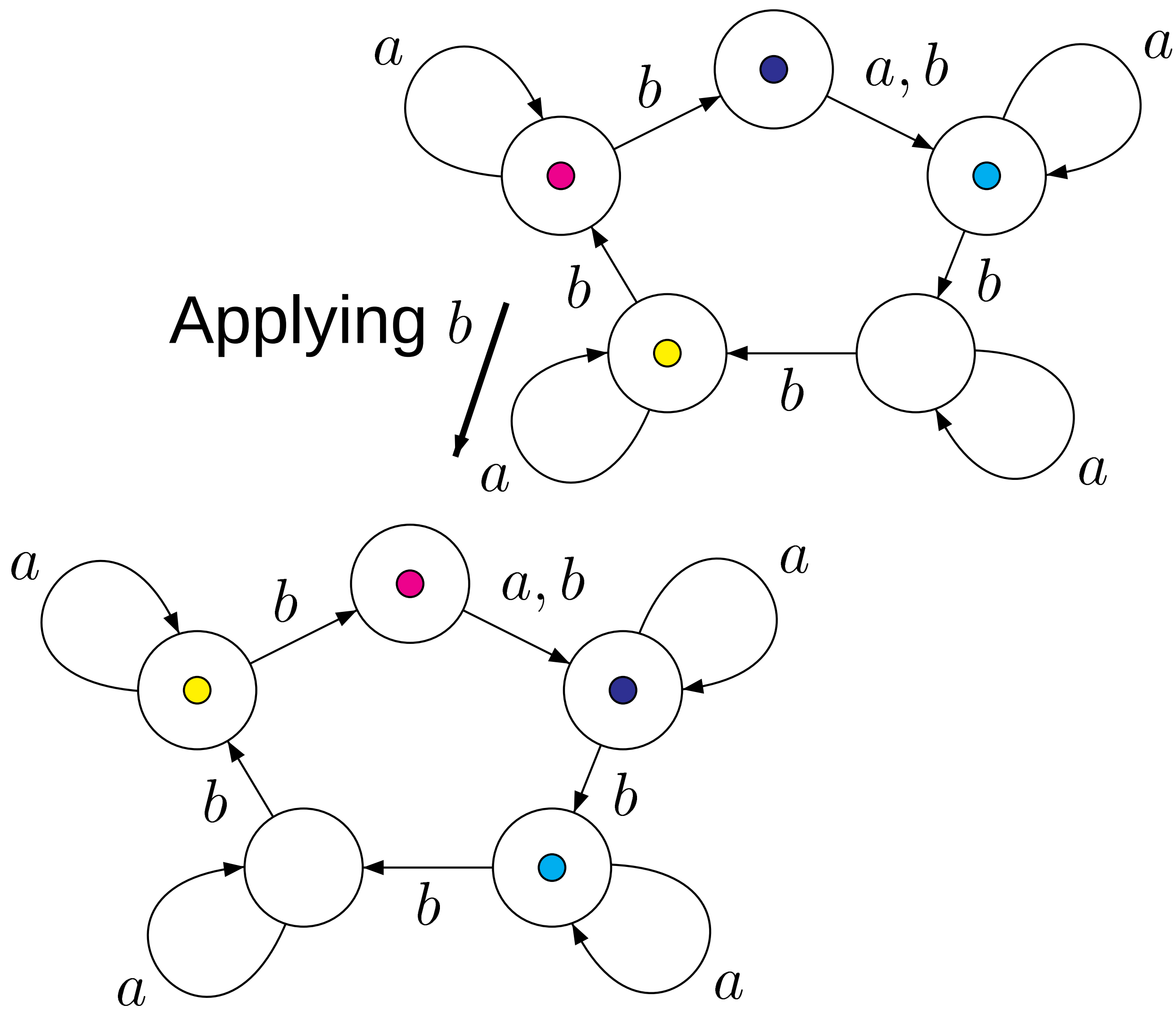
We present a proof of this result using a solitaire-like game:

- The digraph of $\mathscr{C}_n$ — the game-board.
- The initial position — each state holds a coin, all coins are pairwise distinct.
- Each letter $c \in \{a, b\}$ defines a move — coins slide along the arrows labelled c and, whenever two coins meet at the state 1, the coin arriving from 0 is removed.
- The goal — to free all but one states.
- The only coin that remains at the end of the game is the golden coin G.

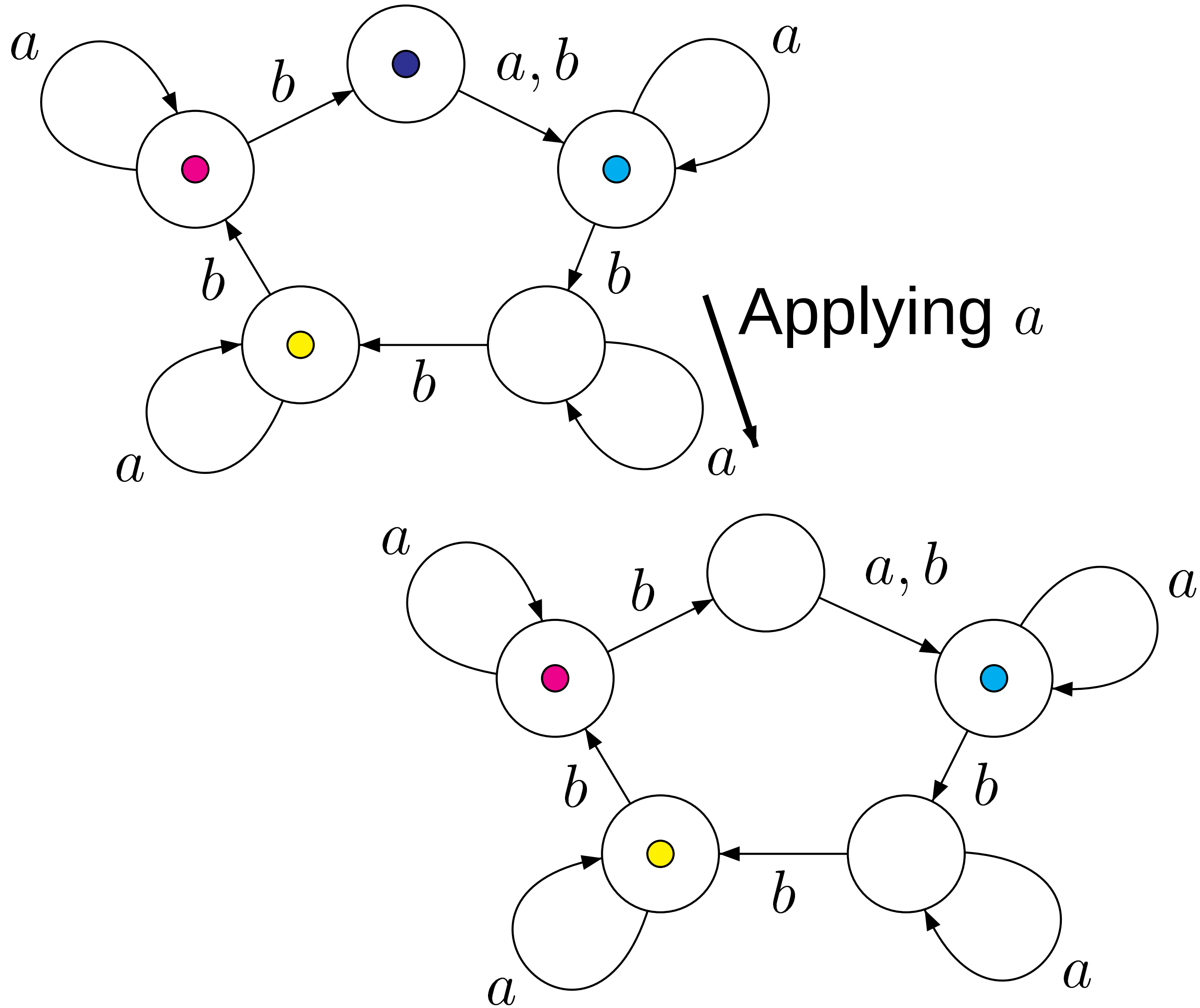
The Černý automata



The Černý automata



The Černý automata



The Černý automata

Let P_0 be an initial distribution of coins, w a reset word.

The Černý automata

Let P_0 be an initial distribution of coins, w a reset word. Denote by P_i the position that arises when we apply the prefix of w of length i to the position P_0.

The Černý automata

Let P_0 be an initial distribution of coins, w a reset word. Denote by P_i the position that arises when we apply the prefix of w of length i to the position P_0. We want to define the weight $\mathrm{wg}(P_i)$ of the position such that

The Černý automata

Let P_0 be an initial distribution of coins, w a reset word. Denote by P_i the position that arises when we apply the prefix of w of length i to the position P_0. We want to define the weight $\mathrm{wg}(P_i)$ of the position such that

(i) $\mathrm{wg}(P_0) \geq n(n-1)$ and $\mathrm{wg}(P_{|w|}) \leq n-1$;

(ii) for each $i = 1, \ldots, |w|$, the action of the i^{th} letter of w decreases the weight by 1 at most, that is, $1 \geq \mathrm{wg}(P_{i-1}) - \mathrm{wg}(P_i)$.

Let P_0 be an initial distribution of coins, w a reset word. Denote by P_i the position that arises when we apply the prefix of w of length i to the position P_0. We want to define the weight $\mathrm{wg}(P_i)$ of the position such that

(i) $\mathrm{wg}(P_0) \geq n(n-1)$ and $\mathrm{wg}(P_{|w|}) \leq n-1$;

(ii) for each $i = 1, \ldots, |w|$, the action of the i^{th} letter of w decreases the weight by 1 at most, that is, $1 \geq \mathrm{wg}(P_{i-1}) - \mathrm{wg}(P_i)$.

Then $$|w| = \sum_{i=1}^{|w|} 1 \geq \sum_{i=1}^{|w|} \big(\mathrm{wg}(P_{i-1}) - \mathrm{wg}(P_i)\big) =$$

$$\mathrm{wg}(P_0) - \mathrm{wg}(P_{|w|}) \geq n(n-1) - (n-1) = (n-1)^2.$$

The Černý automata

The trick consists in letting the weight of each coin depend on its relative location w.r.t. the golden coin.

The Černý automata

The trick consists in letting the weight of each coin depend on its relative location w.r.t. the golden coin. If a coin C is present in a position P_i, let $s_i(C)$ be the state covered with C in this position. We define the *weight of C in the position P_i* as

$$\mathrm{wg}(C, P_i) = n \cdot d_i(C) + m_i(C)$$

where $m_i(C)$ is the residue of $n - s_i(C)$ modulo n and $d_i(C)$ is the number of steps from $s_i(C)$ to $s_i(G)$ in the 'main circle' of our automaton. (Recall that G stands for the golden coin G which is present in all positions.)

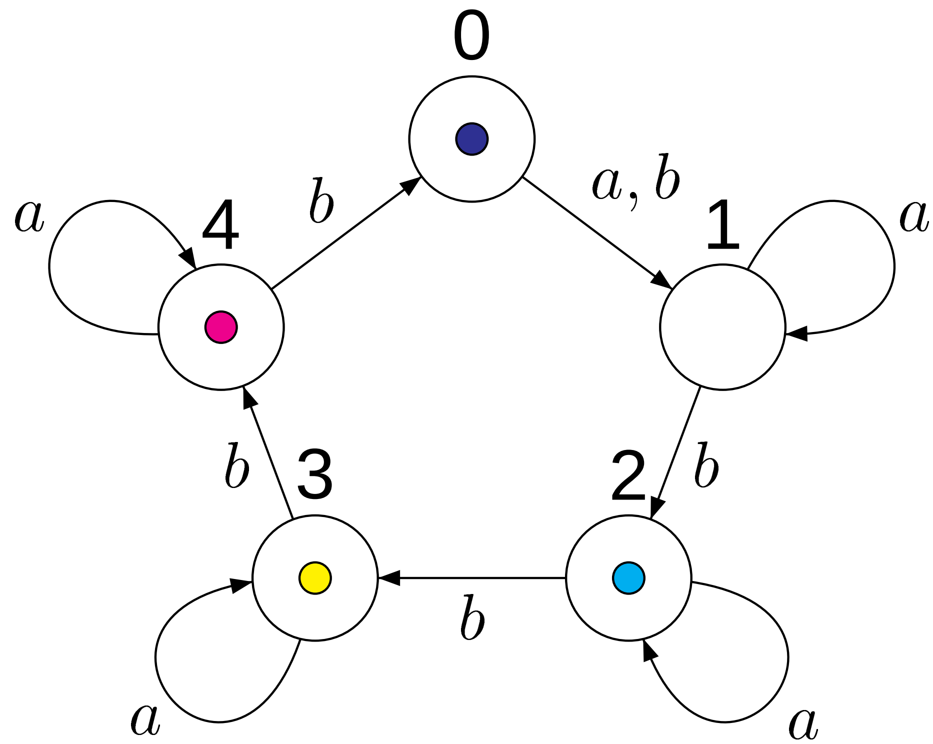
The Černý automata

The trick consists in letting the weight of each coin depend on its relative location w.r.t. the golden coin. If a coin C is present in a position P_i, let $s_i(C)$ be the state covered with C in this position. We define the *weight of C in the position P_i* as

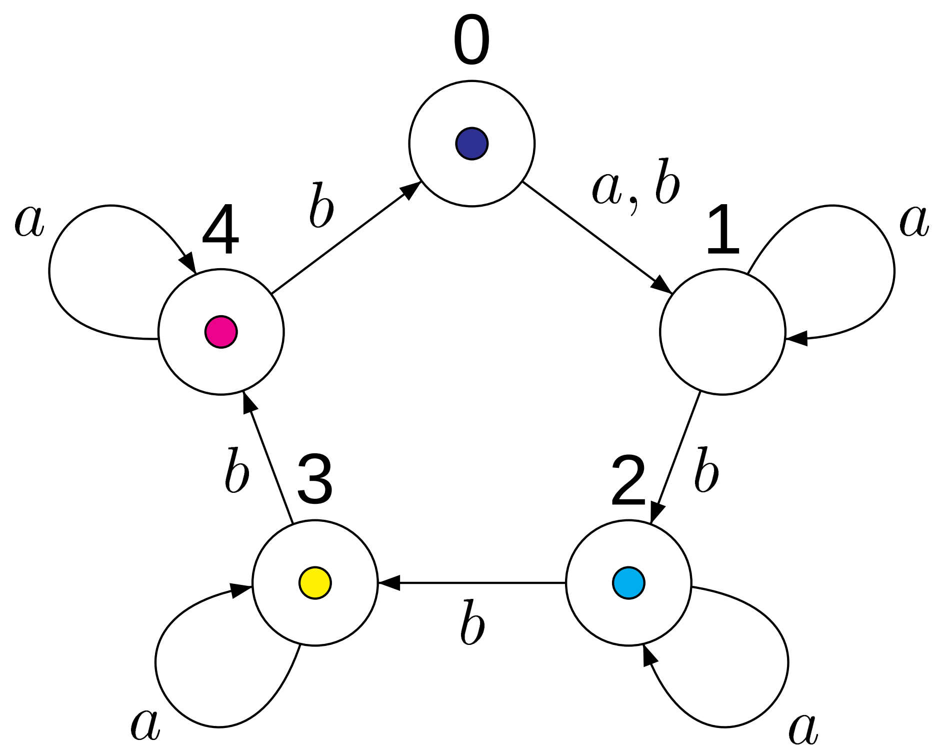
$$\mathrm{wg}(C, P_i) = n \cdot d_i(C) + m_i(C)$$

where $m_i(C)$ is the residue of $n - s_i(C)$ modulo n and $d_i(C)$ is the number of steps from $s_i(C)$ to $s_i(G)$ in the 'main circle' of our automaton. (Recall that G stands for the golden coin G which is present in all positions.) The weight of P_i is the maximum weight of the coins present in this position.

The Černý automata

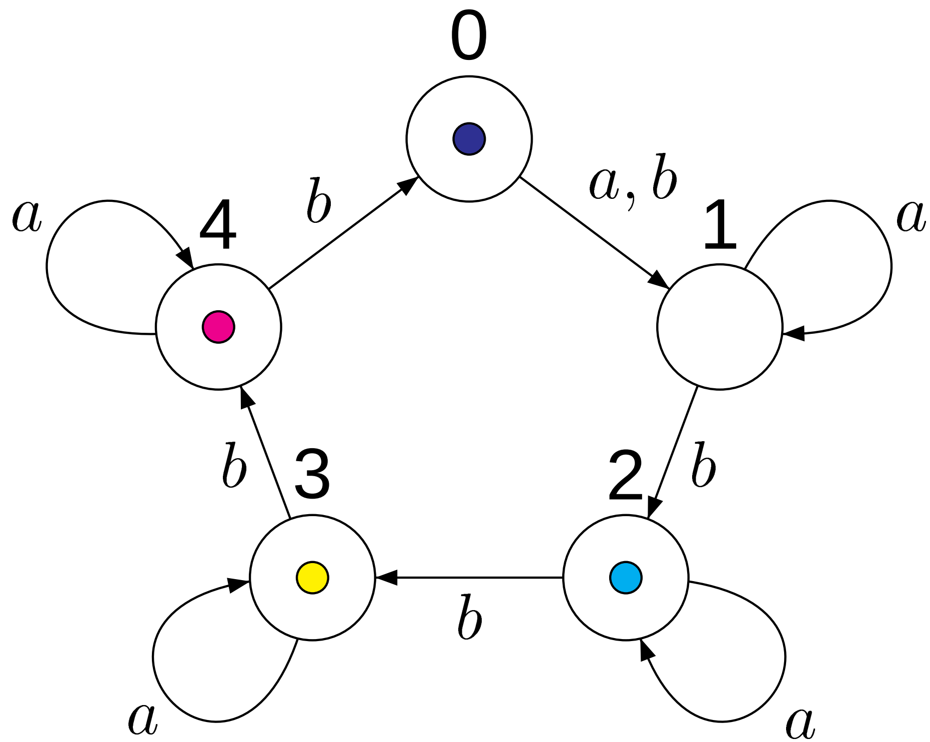


The Černý automata



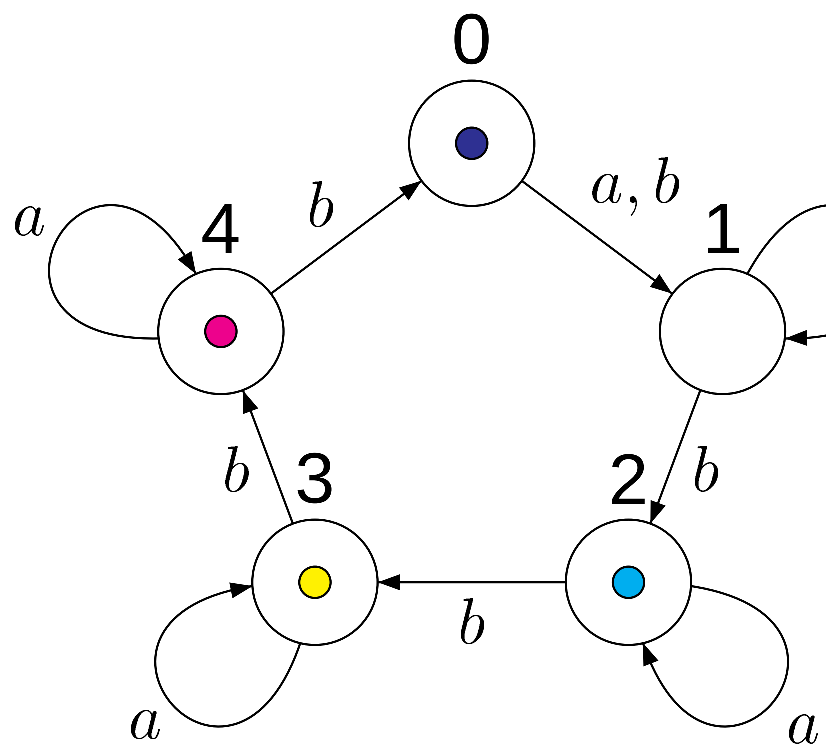
Assume that the yellow coin is the golden one.

The Černý automata



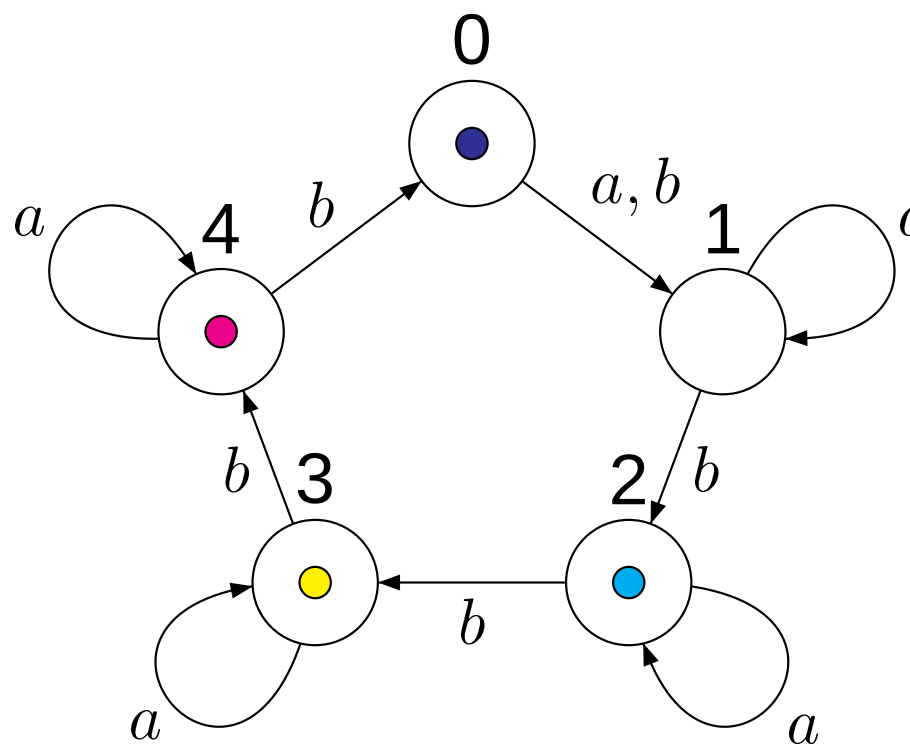
Assume that the yellow coin is the golden one. Then its weight is $5 - 3 = 2$.

The Černý automata



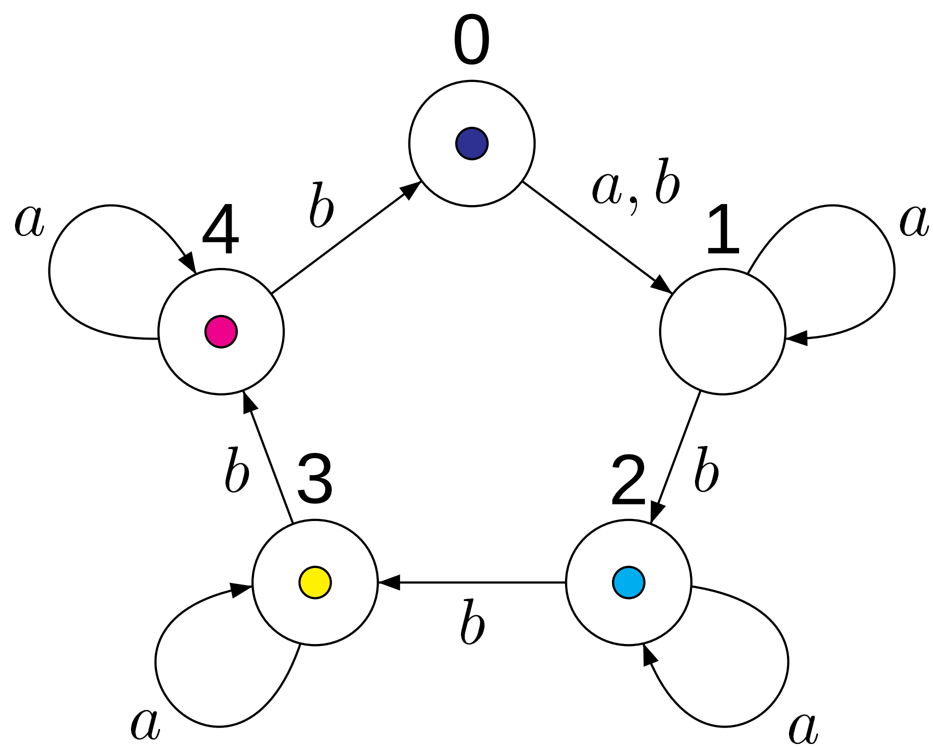
Assume that the yellow coin is the golden one. Then its weight is $5-3=2$. The weight of the cyan coin is $5\cdot 1+(5-2)=8$.

The Černý automata



Assume that the yellow coin is the golden one. Then its weight is $5 - 3 = 2$. The weight of the cyan coin is $5 \cdot 1 + (5 - 2) = 8$. The weight of the blue coin is $5 \cdot 3 + 0 = 15$.

The Černý automata



Assume that the yellow coin is the golden one. Then its weight is $5 - 3 = 2$. The weight of the cyan coin is $5 \cdot 1 + (5 - 2) = 8$. The weight of the blue coin is $5 \cdot 3 + 0 = 15$. The weight of the magenta coin is $5 \cdot 4 + (5 - 4) = 21$, and this is the weight of the position.

The Černý automata

We have to check that our weight function satisfies the conditions

(i) $\mathrm{wg}(P_0) \geq n(n-1)$ and $\mathrm{wg}(P_{|w|}) \leq n-1$;

(ii) $1 \geq \mathrm{wg}(P_{i-1}) - \mathrm{wg}(P_i)$ for each $i = 1, \ldots, |w|$.

The Černý automata

We have to check that our weight function satisfies the conditions

(i) $\mathrm{wg}(P_0) \geq n(n-1)$ and $\mathrm{wg}(P_{|w|}) \leq n-1$;

(ii) $1 \geq \mathrm{wg}(P_{i-1}) - \mathrm{wg}(P_i)$ for each $i = 1, \dots, |w|$.

In the initial position all states are covered with coins. Consider the coin C that covers the state $s_0(G) + 1 \pmod{n}$, that is the state in one step clockwise after the state covered with the golden coin. Then $d_0(C) = n - 1$ whence $\mathrm{wg}(C, P_0) = n \cdot (n-1) + m_0(C) \geq n(n-1)$. Since the weight of a position is not less that the weight of any coin in this position, we have $\mathrm{wg}(P_0) \geq n(n-1)$.

The Černý automata

In the final position only the golden coin G remains, whence the weight of $P_{|w|}$ is the weight of G. Clearly, $\mathrm{wg}(G, P_i) = m_i(G) \leq n-1$ for any position P_i.

The Černý automata

In the final position only the golden coin G remains, whence the weight of $P_{|w|}$ is the weight of G. Clearly, $\mathrm{wg}(G, P_i) = m_i(G) \leq n - 1$ for any position P_i.

Let C be a coin of maximum weight in P_{i-1}. If the transition from P_{i-1} to P_i is caused by b, then $d_i(C) = d_{i-1}(C)$ (because the relative location of the coins does not change) and $m_i(C) = m_{i-1}(C) - 1$ if $m_{i-1}(C) > 0$, otherwise $m_i(C) = n - 1$.

The Černý automata

In the final position only the golden coin G remains, whence the weight of $P_{|w|}$ is the weight of G. Clearly, $\mathrm{wg}(G, P_i) = m_i(G) \leq n-1$ for any position P_i.

Let C be a coin of maximum weight in P_{i-1}. If the transition from P_{i-1} to P_i is caused by b, then $d_i(C) = d_{i-1}(C)$ (because the relative location of the coins does not change) and $m_i(C) = m_{i-1}(C) - 1$ if $m_{i-1}(C) > 0$, otherwise $m_i(C) = n-1$. We see that

$$\mathrm{wg}(P_i) \geq \mathrm{wg}(C, P_i) = n \cdot d_i(C) + m_i(C) \geq$$

$$n \cdot d_{i-1}(C) + m_{i-1}(C) - 1 = \mathrm{wg}(C, P_{i-1}) - 1 = \mathrm{wg}(P_{i-1}) - 1.$$

The Černý automata

Suppose the transition from P_{i-1} to P_i is caused by a. If $s_{i-1}(C) \neq 0$, then $m_i(C) = m_{i-1}(C)$ and $d_i(C) = d_{i-1}(C)$ if $s_{i-1}(G) \neq 0$, otherwise $d_i(C) = d_{i-1}(C) + 1$.

The Černý automata

Suppose the transition from P_{i-1} to P_i is caused by a. If $s_{i-1}(C) \neq 0$, then $m_i(C) = m_{i-1}(C)$ and $d_i(C) = d_{i-1}(C)$ if $s_{i-1}(G) \neq 0$, otherwise $d_i(C) = d_{i-1}(C) + 1$. Thus, the transition from P_{i-1} to P_i cannot decrease the weight.

The Černý automata

Suppose the transition from P_{i-1} to P_i is caused by a. If $s_{i-1}(C) \neq 0$, then $m_i(C) = m_{i-1}(C)$ and $d_i(C) = d_{i-1}(C)$ if $s_{i-1}(G) \neq 0$, otherwise $d_i(C) = d_{i-1}(C) + 1$. Thus, the transition from P_{i-1} to P_i cannot decrease the weight.

Assume that C covers 0 in P_{i-1}. Then in P_i the state 1 holds a coin C' (which may or may not coincide with C). In P_{i-1} the golden coin G does not cover 0 whence it does not move and $d_i(C') = d_{i-1}(C) - 1$.

The Černý automata

Suppose the transition from P_{i-1} to P_i is caused by a. If $s_{i-1}(C) \neq 0$, then $m_i(C) = m_{i-1}(C)$ and $d_i(C) = d_{i-1}(C)$ if $s_{i-1}(G) \neq 0$, otherwise $d_i(C) = d_{i-1}(C) + 1$. Thus, the transition from P_{i-1} to P_i cannot decrease the weight.

Assume that C covers 0 in P_{i-1}. Then in P_i the state 1 holds a coin C' (which may or may not coincide with C). In P_{i-1} the golden coin G does not cover 0 whence it does not move and $d_i(C') = d_{i-1}(C) - 1$. Therefore

$$\mathrm{wg}(P_i) \geq \mathrm{wg}(C', P_i) = n \cdot d_i(C') + n - 1 = n \cdot (d_{i-1}(C) - 1) + n - 1$$

$$= n \cdot d_{i-1}(C) - 1 = \mathrm{wg}(C, P_{i-1}) - 1 = \mathrm{wg}(P_{i-1}) - 1.$$

The Černý conjecture

Define the *Černý function* $C(n)$ as the maximum length of shortest reset words for 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

Define the *Černý function* $C(n)$ as the maximum length of shortest reset words for 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.

The Černý conjecture

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

The Černý conjecture is the claim that in fact the equality $C(n) = (n-1)^2$ holds true. This simply looking conjecture is arguably the most longstanding open problem in the combinatorial theory of finite automata, see the pre-proceedings for a discussion of the history of the conjecture.

The Černý conjecture

Define the *Černý function* $C(n)$ as the maximum length of shortest reset words for 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. This simply looking conjecture is arguably the most longstanding open problem in the combinatorial theory of finite automata, see the pre-proceedings for a discussion of the history of the conjecture. Everything we know about the conjecture in general can be summarized in one line:

$$(n-1)^2 \leq C(n) \leq \frac{n^3 - n}{6}.$$

The Černý conjecture

Why is the problem so surprisingly difficult?

The Černý conjecture

Why is the problem so surprisingly difficult?

We saw two reasons in Lecture I:

The Černý conjecture

Why is the problem so surprisingly difficult?

We saw two reasons in Lecture I:

- non-locality: prefixes of optimal solutions need not be optimal (that's why the greedy algorithm fails;

The Černý conjecture

Why is the problem so surprisingly difficult?

We saw two reasons in Lecture I:

• non-locality: prefixes of optimal solutions need not be optimal (that's why the greedy algorithm fails;

• combinatorics of finite sets is encoded in the problem.

The Černý conjecture

Why is the problem so surprisingly difficult?

We saw two reasons in Lecture I:
• non-locality: prefixes of optimal solutions need not be optimal (that's why the greedy algorithm fails;
• combinatorics of finite sets is encoded in the problem.

Yet another reason: “slowly” synchronizing automata turn out to be extremely rare.

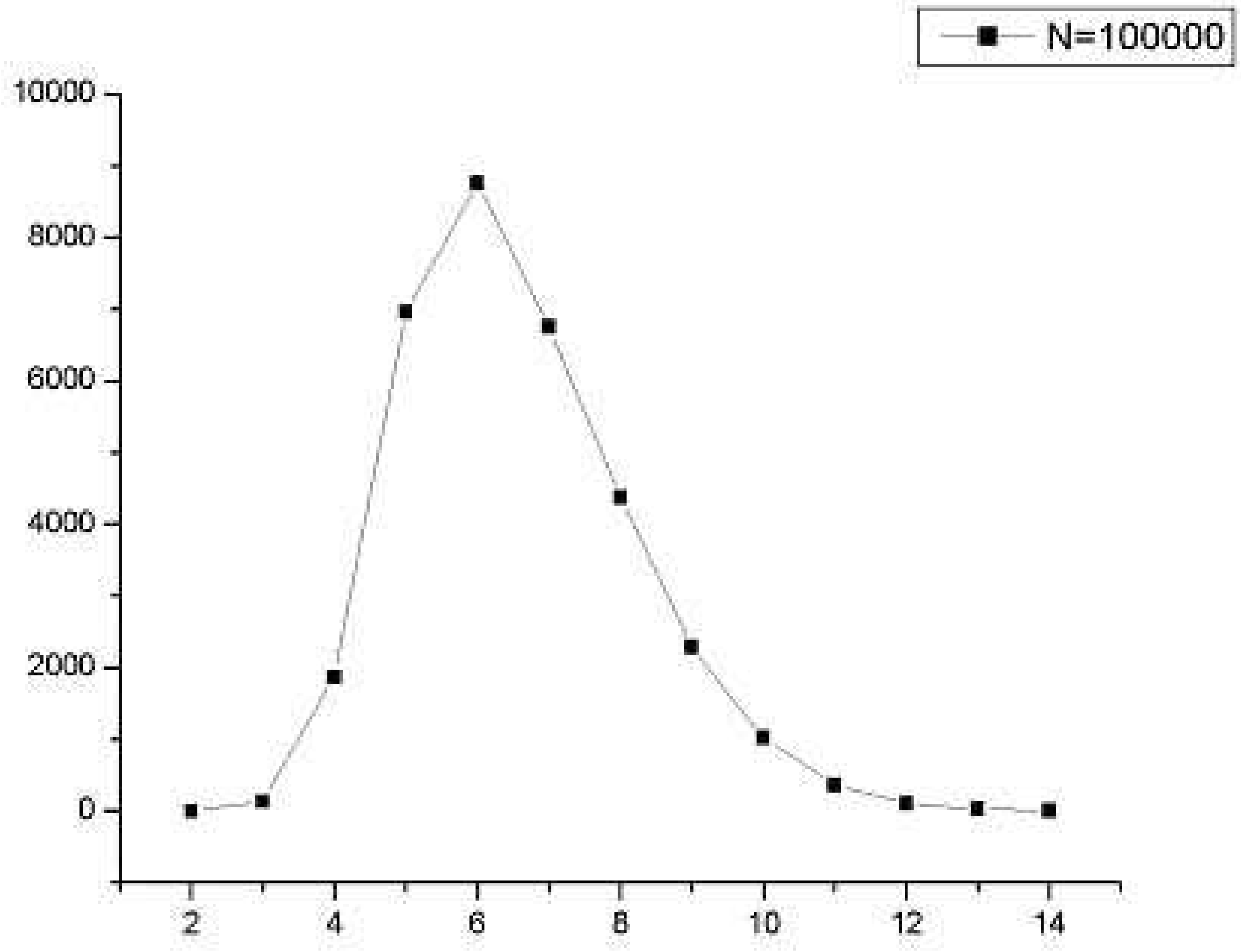
Why is the problem so surprisingly difficult?

We saw two reasons in Lecture I:

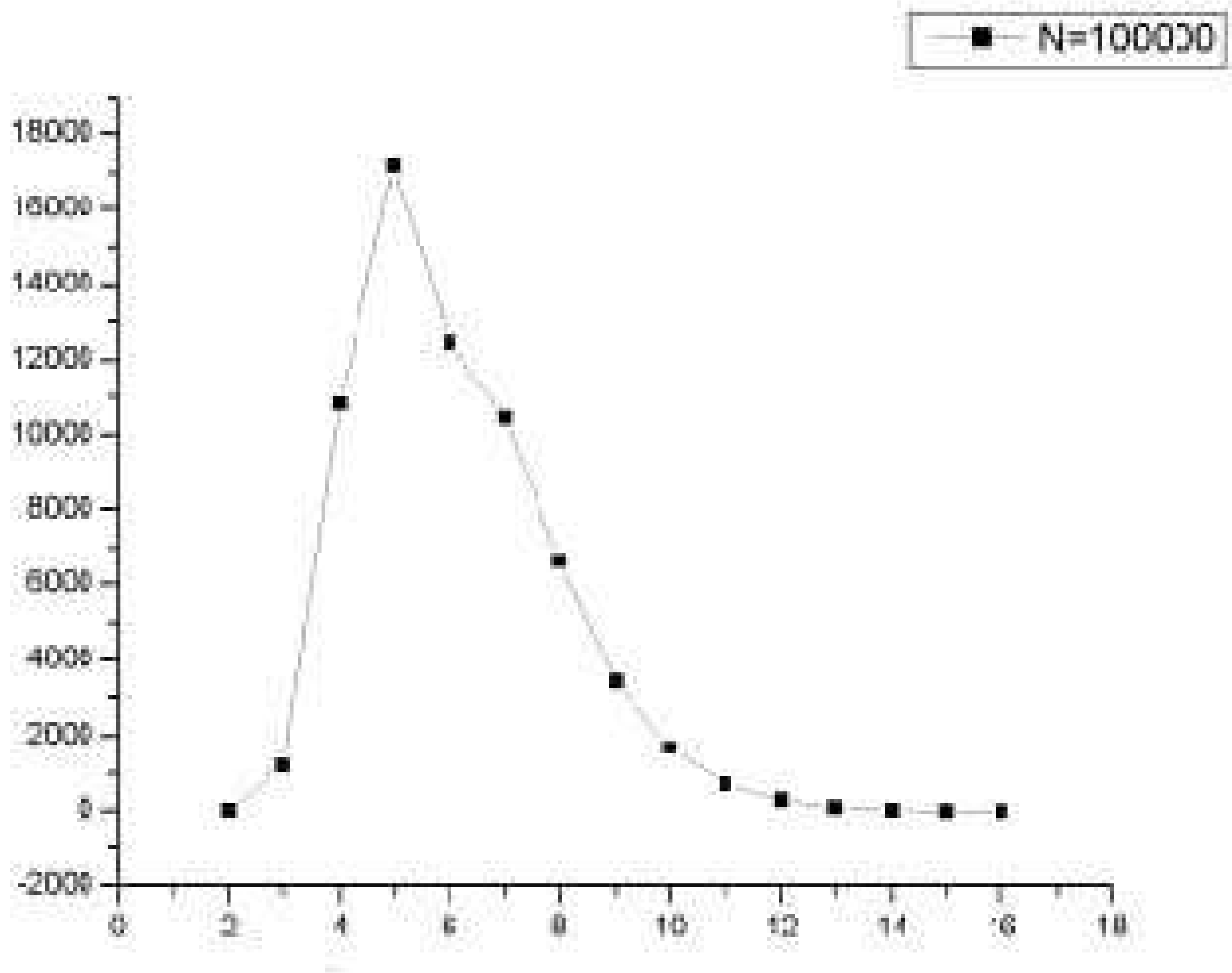
- non-locality: prefixes of optimal solutions need not be optimal (that's why the greedy algorithm fails;
- combinatorics of finite sets is encoded in the problem.

Yet another reason: "slowly" synchronizing automata turn out to be extremely rare. The only known infinite series of n-state synchronizing automata with shortest reset words of length $(n-1)^2$ is the Černý series $\mathscr{C}_n$, $n = 2, 3, \dots$, with a few sporadic examples for $n \leq 6$.

20-State Experiment



30-State Experiment



Random Automata

A (partial) explanation of these experimental observations:

Random Automata

A (partial) explanation of these experimental observations: if Q is an n-set (with n large enough), then, on average, any product of $2n$ randomly chosen transformations of Q is a constant map (Peter Higgins, The range order of a product of i transformations from a finite full transformation semigroup, Semigroup Forum, 37 (1988) 31–36).

Random Automata

A (partial) explanation of these experimental observations: if Q is an n-set (with n large enough), then, on average, any product of $2n$ randomly chosen transformations of Q is a constant map (Peter Higgins, The range order of a product of i transformations from a finite full transformation semigroup, Semigroup Forum, 37 (1988) 31–36). In automata-theoretic terms, this fact means that a randomly chosen DFA with n states and a sufficiently large input alphabet tends to be synchronizing and is reset by any word of length $\leq 2n$.

Random Automata

A (partial) explanation of these experimental observations: if Q is an n-set (with n large enough), then, on average, any product of $2n$ randomly chosen transformations of Q is a constant map (Peter Higgins, The range order of a product of i transformations from a finite full transformation semigroup, Semigroup Forum, 37 (1988) 31–36). In automata-theoretic terms, this fact means that a randomly chosen DFA with n states and a sufficiently large input alphabet tends to be synchronizing and is reset by any word of length $\leq 2n$.

Thus, "slowly" synchronizing automata cannot be discovered via a random sampling.

Sporadic Examples

A synchronizing automaton $\mathscr{A} = \langle Q, \Sigma, \delta \rangle$ is *proper* if none of the automata obtained from $\mathscr{A}$ by erasing any letter in Σ are synchronizing.

Sporadic Examples

A synchronizing automaton $\mathscr{A} = \langle Q, \Sigma, \delta \rangle$ is *proper* if none of the automata obtained from $\mathscr{A}$ by erasing any letter in Σ are synchronizing. E.g., the Černý automata $\mathscr{C}_n$ with $n > 2$ are proper while $\mathscr{C}_2$ is not.

Sporadic Examples

A synchronizing automaton $\mathscr{A} = \langle Q, \Sigma, \delta \rangle$ is *proper* if none of the automata obtained from $\mathscr{A}$ by erasing any letter in Σ are synchronizing. E.g., the Černý automata $\mathscr{C}_n$ with $n > 2$ are proper while $\mathscr{C}_2$ is not.

A synchronizing automaton with n states *reaches the Černý bound* if the minimum length of its reset words is $(n-1)^2$.

Sporadic Examples

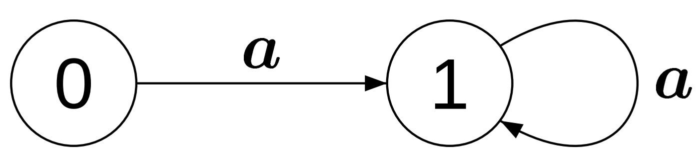
A synchronizing automaton $\mathscr{A} = \langle Q, \Sigma, \delta \rangle$ is *proper* if none of the automata obtained from $\mathscr{A}$ by erasing any letter in Σ are synchronizing. E.g., the Černý automata $\mathscr{C}_n$ with $n > 2$ are proper while $\mathscr{C}_2$ is not.

A synchronizing automaton with n states *reaches the Černý bound* if the minimum length of its reset words is $(n-1)^2$. We present here all known proper synchronizing automata beyond the Černý series $\mathscr{C}_n$, $n = 3, 4, \dots$, that reach the Černý bound.

Sporadic Examples

A synchronizing automaton $\mathscr{A} = \langle Q, \Sigma, \delta \rangle$ is *proper* if none of the automata obtained from $\mathscr{A}$ by erasing any letter in Σ are synchronizing. E.g., the Černý automata $\mathscr{C}_n$ with $n > 2$ are proper while $\mathscr{C}_2$ is not.
A synchronizing automaton with n states *reaches the Černý bound* if the minimum length of its reset words is $(n-1)^2$. We present here all known proper synchronizing automata beyond the Černý series $\mathscr{C}_n$, $n = 3, 4, \dots$, that reach the Černý bound.

For the sake of completeness, we start with $n = 2$:

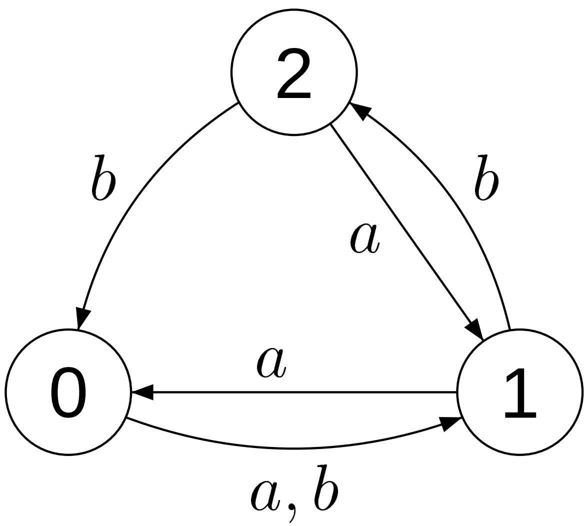


Sporadic Examples

For $n = 3$ we have three sporadic automata:

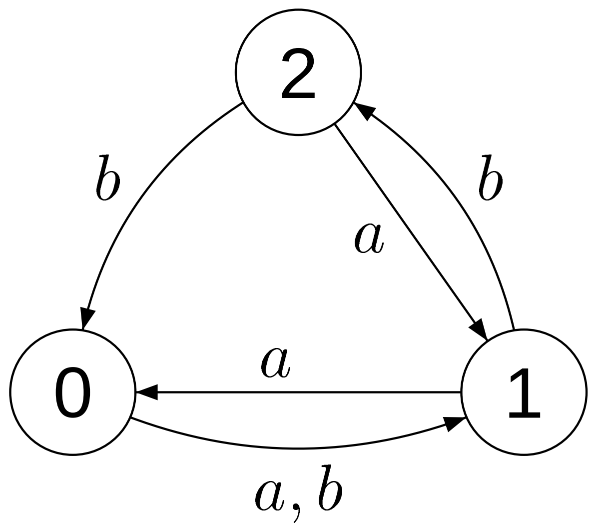
Sporadic Examples

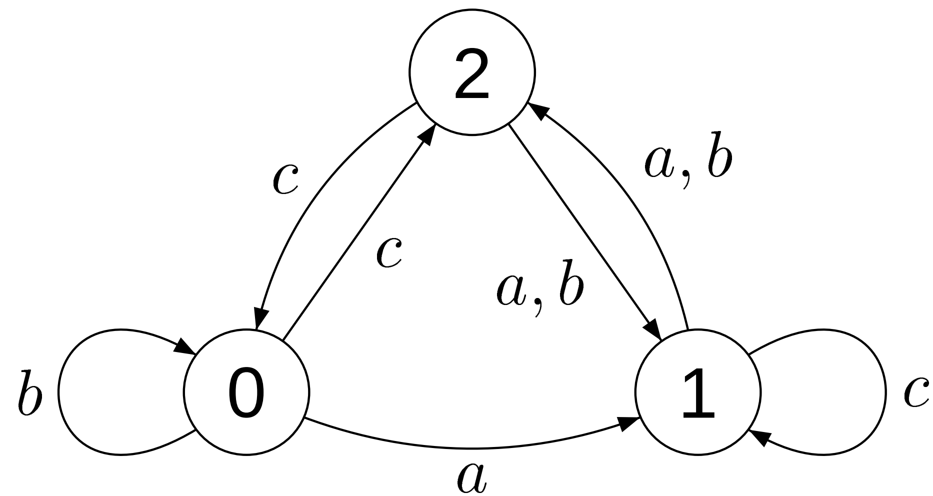
For $n = 3$ we have three sporadic automata:



Sporadic Examples

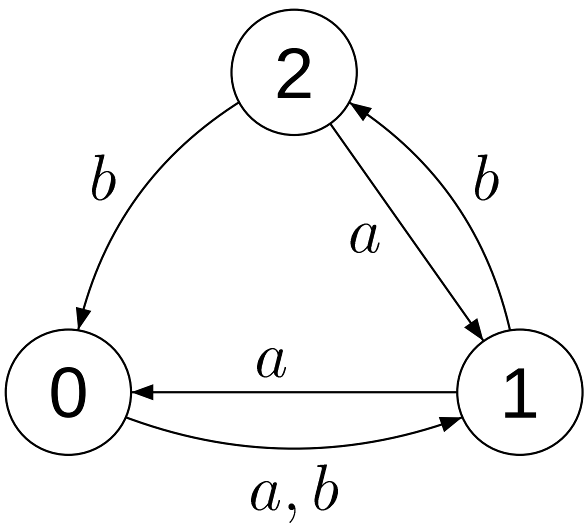
For $n = 3$ we have three sporadic automata:

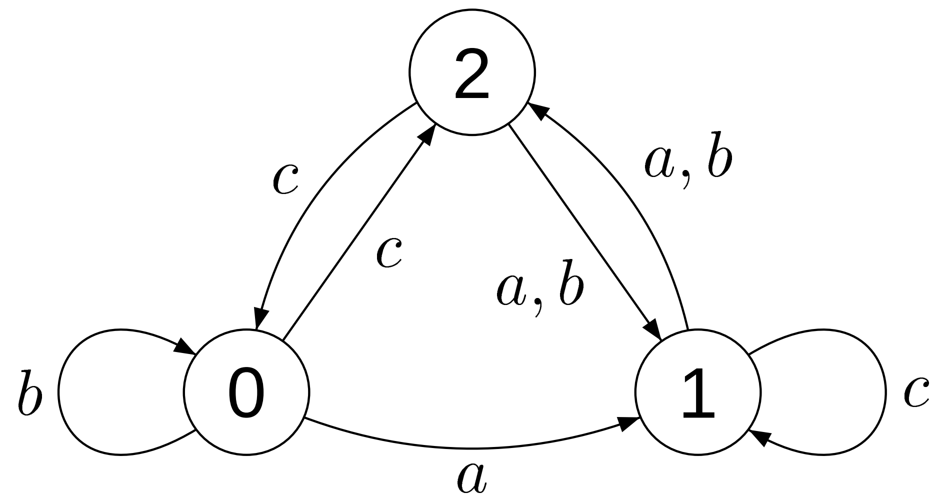


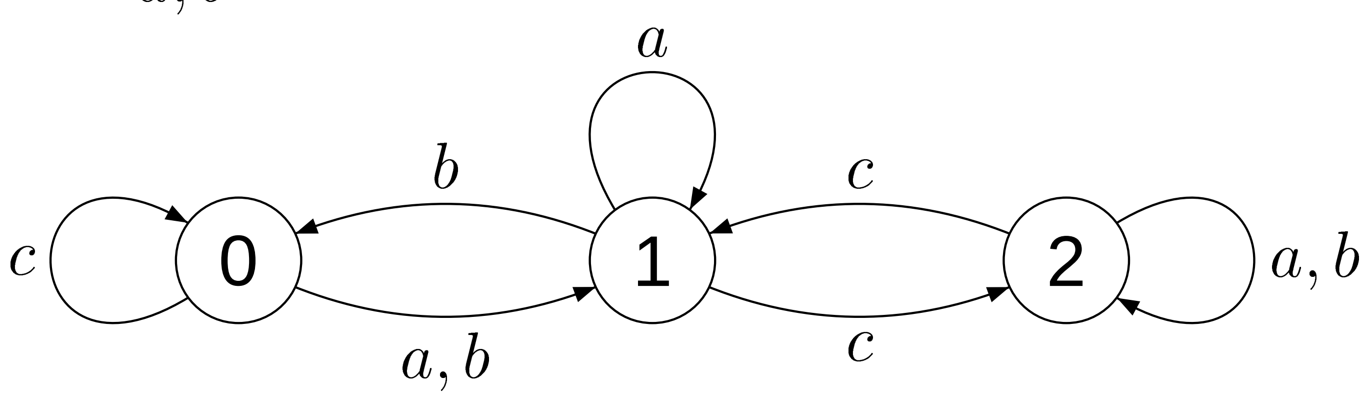


Sporadic Examples

For $n = 3$ we have three sporadic automata:





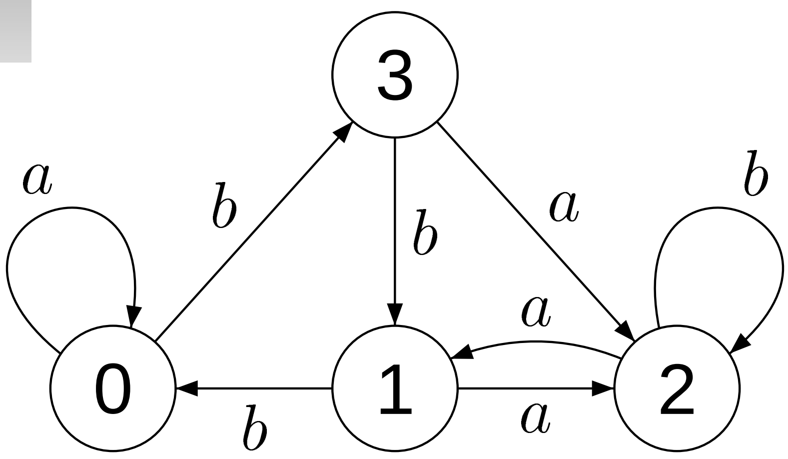


Sporadic Examples

Also for $n = 4$ three sporadic automata are known:

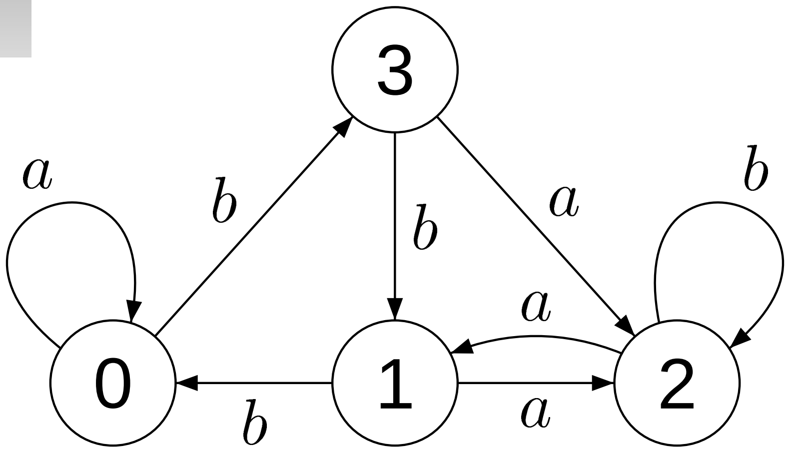
Sporadic Examples

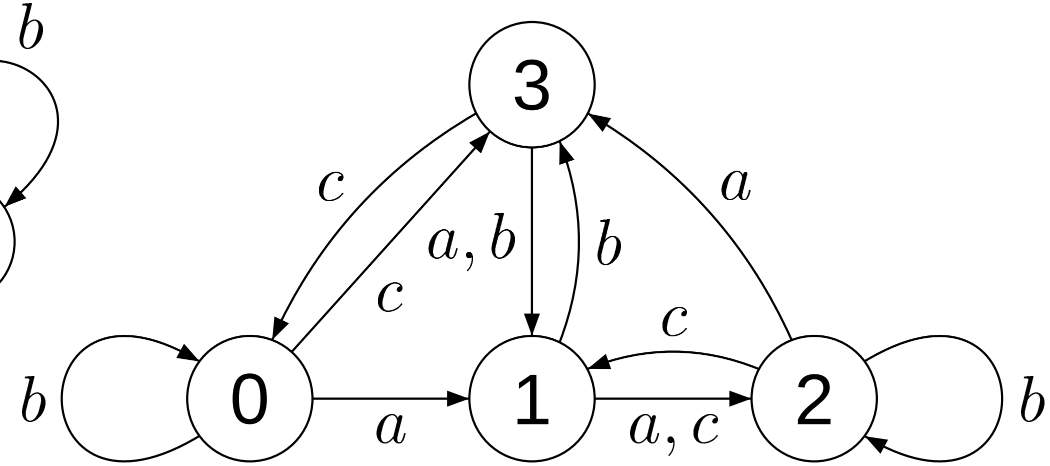
Also for $n = 4$ three sporadic automata are known:



Sporadic Examples

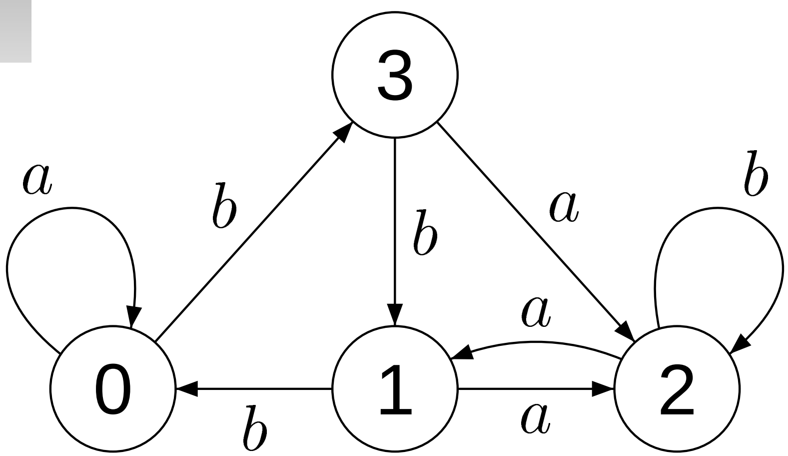
Also for $n = 4$ three sporadic automata are known:

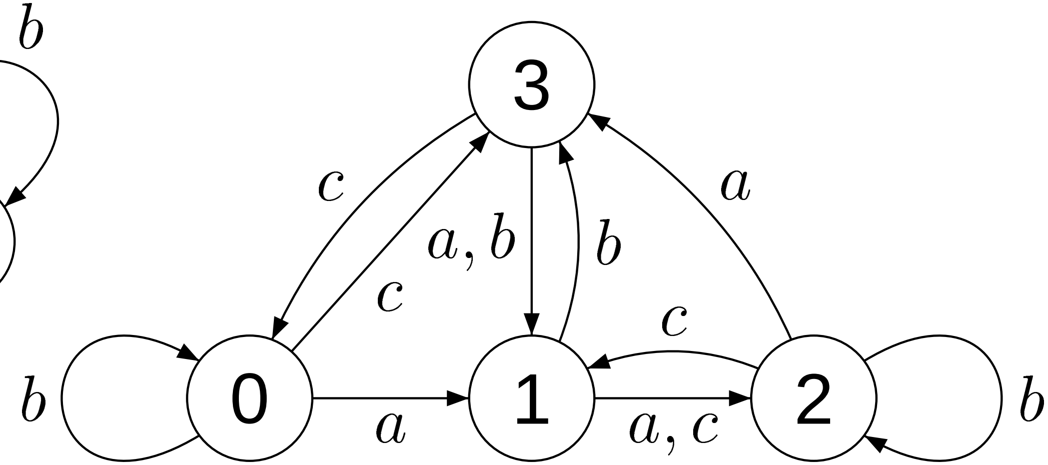


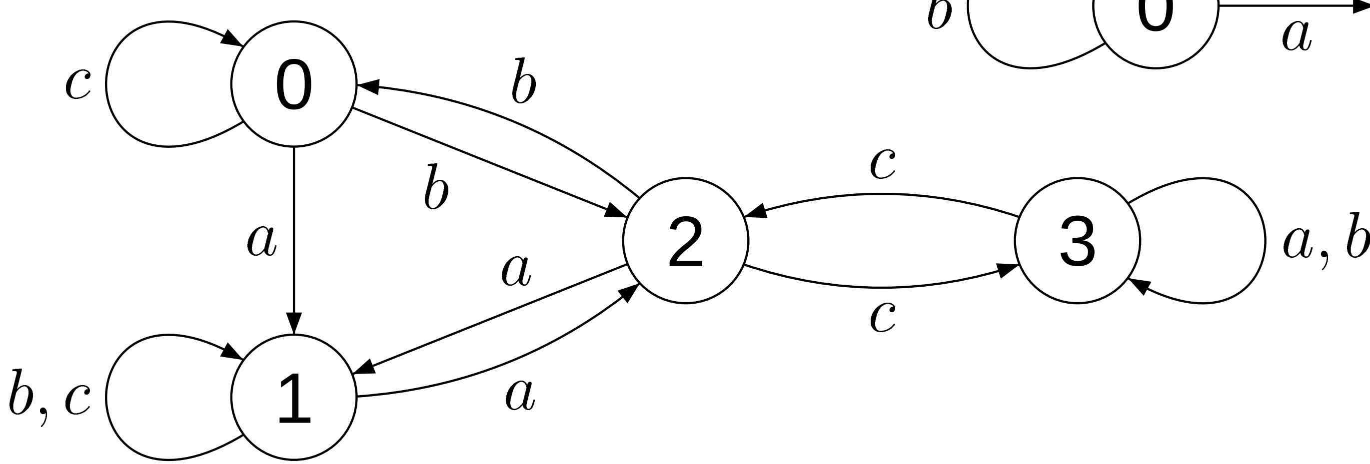


Sporadic Examples

Also for $n = 4$ three sporadic automata are known:





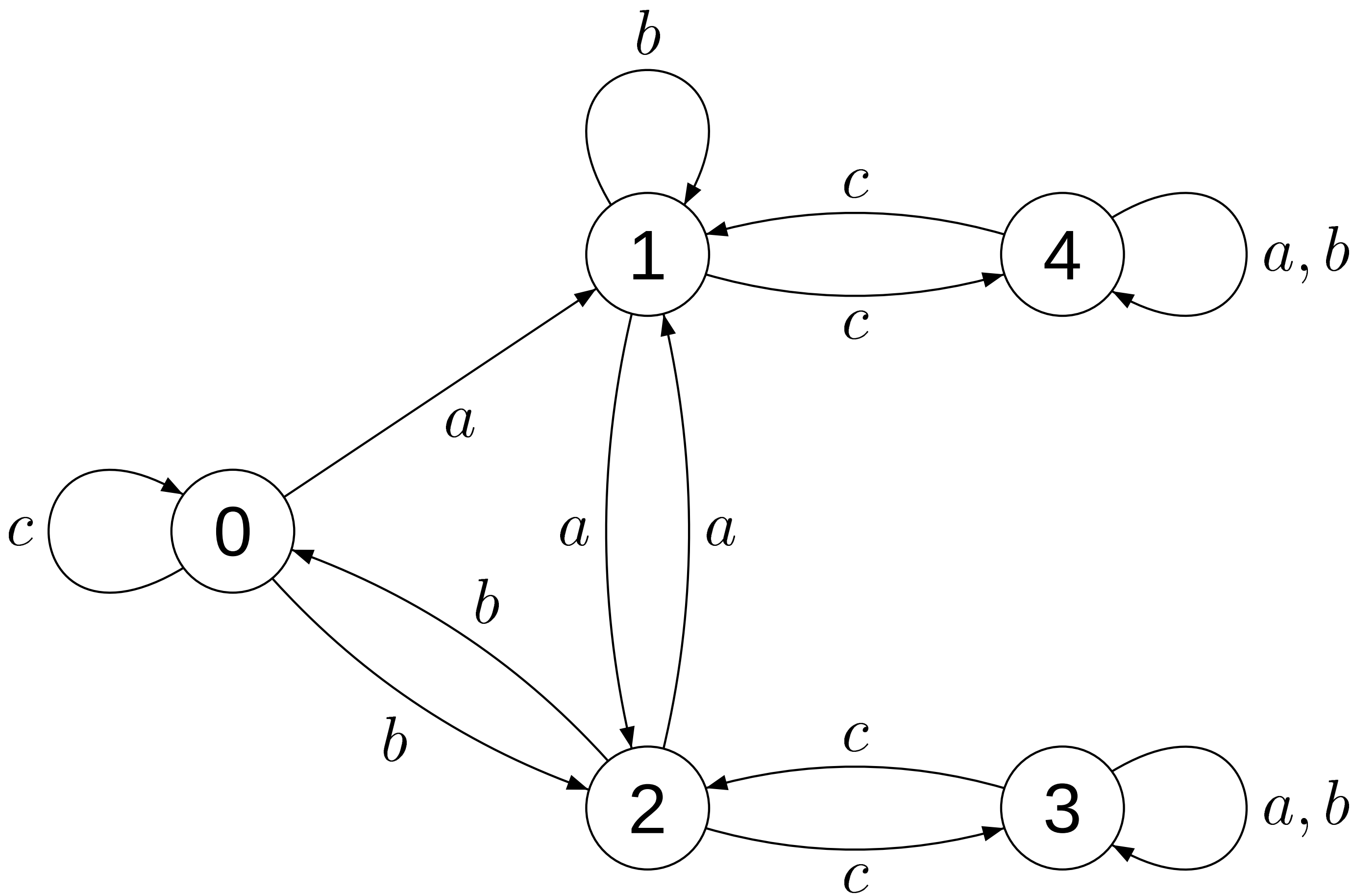


Sporadic Examples

A proper 5-state automaton reaching the Černý bound has been recently discovered by Adam Roman.

Sporadic Examples

A proper 5-state automaton reaching the Černý bound has been recently discovered by Adam Roman.

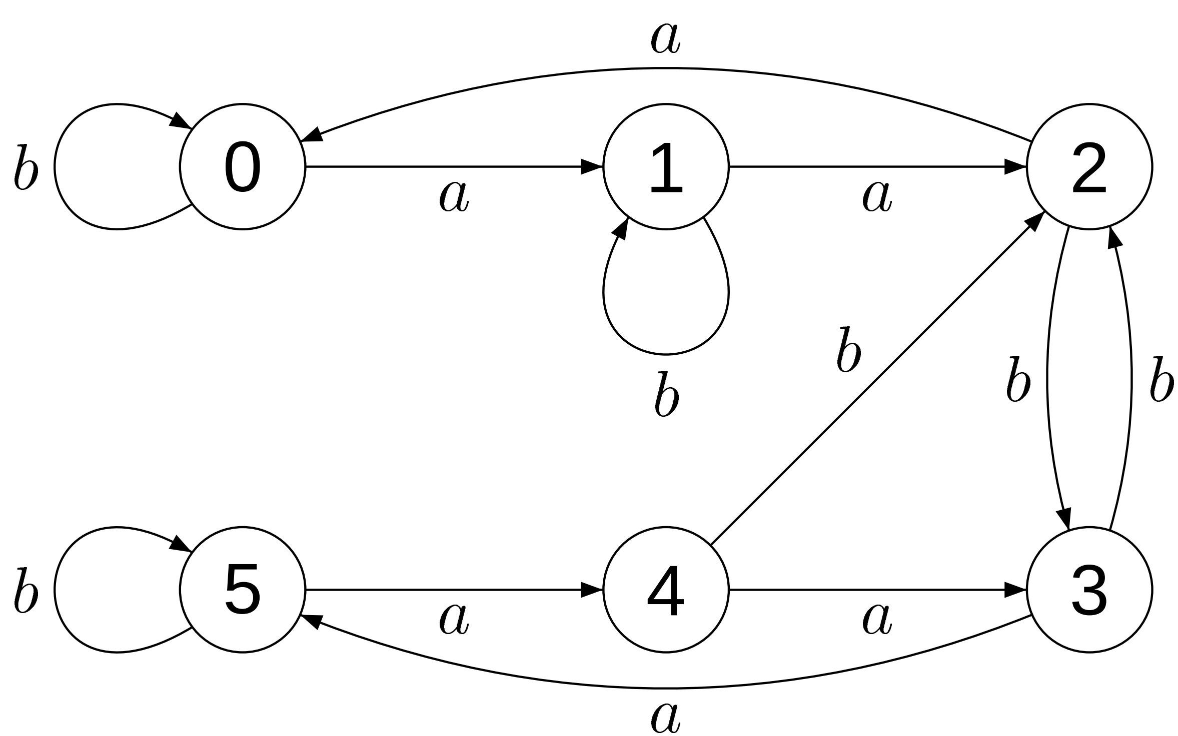


Kari’s Example

The last in our list and the most remarkable example was published in 2001 by Jarkko Kari (A counter example to a conjecture concerning synchronizing words in finite automata, EATCS Bull., 73, 146).

Kari's Example

The last in our list and the most remarkable example was published in 2001 by Jarkko Kari (A counter example to a conjecture concerning synchronizing words in finite automata, EATCS Bull., 73, 146).



Kari's Example

Kari's automaton $\mathscr{K}_{\mathbf{6}}$ has refuted several conjectures.

Kari's Example

Kari's automaton $\mathscr{K}_6$ has refuted several conjectures.

The most well known of them was suggested by Jean-Eric Pin in 1978. Pin conjectured that if a DFA $\mathscr{A} = \langle Q, \Sigma, \delta \rangle$ with n states admits a word $w \in \Sigma^*$ such that $|Q \,.\, w| = k$, $1 \leq k \leq n$, then $\mathscr{A}$ possesses a word of length at most $(n-k)^2$ with the same property.

Kari's Example

Kari's automaton $\mathscr{K}_6$ has refuted several conjectures.

The most well known of them was suggested by Jean-Eric Pin in 1978. Pin conjectured that if a DFA $\mathscr{A} = \langle Q, \Sigma, \delta \rangle$ with n states admits a word $w \in \Sigma^*$ such that $|Q \,.\, w| = k$, $1 \leq k \leq n$, then $\mathscr{A}$ possesses a word of length at most $(n-k)^2$ with the same property. (The Černý conjecture corresponds to the case $k = 1$.)

Kari's Example

Kari's automaton $\mathscr{K}_6$ has refuted several conjectures.

The most well known of them was suggested by Jean-Eric Pin in 1978. Pin conjectured that if a DFA $\mathscr{A} = \langle Q, \Sigma, \delta \rangle$ with n states admits a word $w \in \Sigma^*$ such that $|Q \,.\, w| = k$, $1 \leq k \leq n$, then $\mathscr{A}$ possesses a word of length at most $(n-k)^2$ with the same property. (The Černý conjecture corresponds to the case $k = 1$.)

However, in $\mathscr{K}_6$ there is no word w of length $16 = (6-2)^2$ such that $|Q \,.\, w| = 2$.

Kari's Example

The *rank* of a DFA $\mathscr{A} = \langle \boldsymbol{Q}, \boldsymbol{\Sigma}, \boldsymbol{\delta} \rangle$ is the minimum cardinality of the sets $\boldsymbol{Q} \,.\, \boldsymbol{w}$ where $\boldsymbol{w}$ runs over $\boldsymbol{\Sigma}^*$.

Kari's Example

The *rank* of a DFA $\mathscr{A} = \langle \boldsymbol{Q}, \boldsymbol{\Sigma}, \boldsymbol{\delta} \rangle$ is the minimum cardinality of the sets $\boldsymbol{Q} \,.\, \boldsymbol{w}$ where $\boldsymbol{w}$ runs over $\boldsymbol{\Sigma}^*$. This is the minimum score that can be achieved in the solitaire game on the automaton $\mathscr{A}$.

Kari's Example

The *rank* of a DFA $\mathscr{A} = \langle Q, \Sigma, \delta \rangle$ is the minimum cardinality of the sets $Q \,.\, w$ where w runs over Σ^*. This is the minimum score that can be achieved in the solitaire game on the automaton $\mathscr{A}$. Synchronizing automata are precisely those of rank 1.

Kari's Example

The *rank* of a DFA $\mathscr{A} = \langle \boldsymbol{Q}, \boldsymbol{\Sigma}, \boldsymbol{\delta} \rangle$ is the minimum cardinality of the sets $\boldsymbol{Q} \,.\, \boldsymbol{w}$ where $\boldsymbol{w}$ runs over Σ^*. This is the minimum score that can be achieved in the solitaire game on the automaton $\mathscr{A}$. Synchronizing automata are precisely those of rank 1.

A corrected (and perhaps correct) version of Pin's conjecture is the following rank conjecture:

Kari's Example

The *rank* of a DFA $\mathscr{A} = \langle Q, \Sigma, \delta \rangle$ is the minimum cardinality of the sets $Q \,.\, w$ where w runs over Σ^*. This is the minimum score that can be achieved in the solitaire game on the automaton $\mathscr{A}$. Synchronizing automata are precisely those of rank 1.

A corrected (and perhaps correct) version of Pin's conjecture is the following rank conjecture: if a DFA $\mathscr{A} = \langle Q, \Sigma, \delta \rangle$ with n states has rank k, then there exists a word $w \in \Sigma^*$ of length at most $(n-k)^2$ such that $|Q \,.\, w| = k$.

Kari's Example

The *rank* of a DFA $\mathscr{A} = \langle Q, \Sigma, \delta \rangle$ is the minimum cardinality of the sets $Q \,.\, w$ where w runs over Σ^*. This is the minimum score that can be achieved in the solitaire game on the automaton $\mathscr{A}$. Synchronizing automata are precisely those of rank 1.

A corrected (and perhaps correct) version of Pin's conjecture is the following rank conjecture: if a DFA $\mathscr{A} = \langle Q, \Sigma, \delta \rangle$ with n states has rank k, then there exists a word $w \in \Sigma^*$ of length at most $(n-k)^2$ such that $|Q \,.\, w| = k$.

Again, the Černý conjecture corresponds to the case $k = 1$.

Kari's Example

Kari's automaton does not refute the rank conjecture!

Kari's Example

Kari's automaton does not refute the rank conjecture! In the solitaire game on $\mathscr{K}_{\mathbf{6}}$, no sequence of 16 moves removes 4 coins.

Kari's Example

Kari's automaton does not refute the rank conjecture! In the solitaire game on $\mathscr{K}_{\mathbf{6}}$, no sequence of 16 moves removes 4 coins. However, 4 is not the maximum number of tokens that can be removed!

Kari's Example

Kari's automaton does not refute the rank conjecture! In the solitaire game on $\mathscr{K}_{\mathbf{6}}$, no sequence of 16 moves removes 4 coins. However, 4 is not the maximum number of tokens that can be removed! One can show that 5 states can be freed by a sequence of 25 moves — in full accordance with the rank conjecture.

Kari's Example

Kari's automaton does not refute the rank conjecture! In the solitaire game on $\mathscr{K}_{\mathbf{6}}$, no sequence of 16 moves removes 4 coins. However, 4 is not the maximum number of tokens that can be removed! One can show that 5 states can be freed by a sequence of 25 moves — in full accordance with the rank conjecture.

Yet another hope killed by Kari's example is the extensibility conjecture.

Kari's Example

Kari's automaton does not refute the rank conjecture! In the solitaire game on $\mathscr{K}_{\mathbf{6}}$, no sequence of 16 moves removes 4 coins. However, 4 is not the maximum number of tokens that can be removed! One can show that 5 states can be freed by a sequence of 25 moves — in full accordance with the rank conjecture.

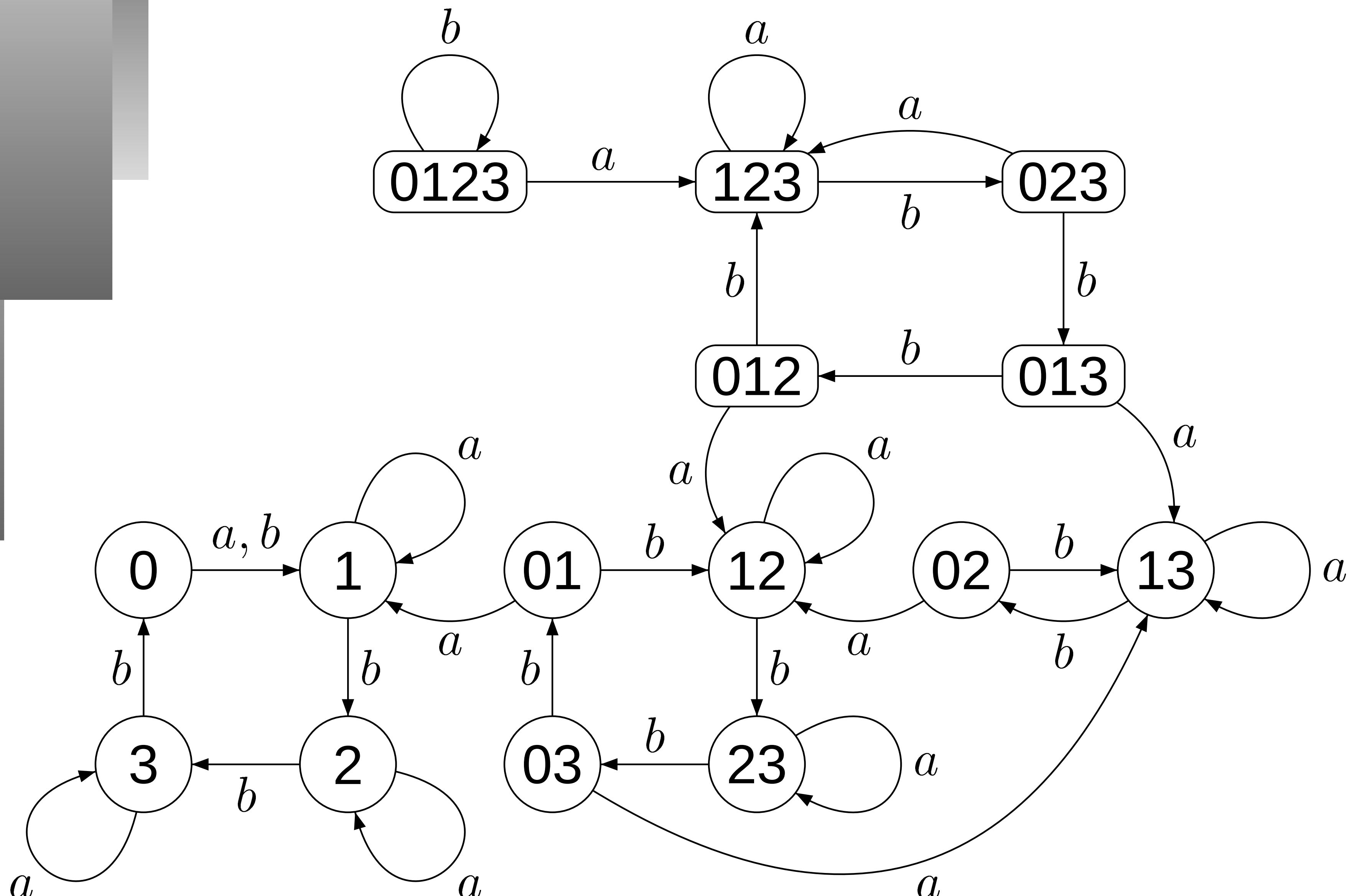
Yet another hope killed by Kari's example is the extensibility conjecture. In a DFA $\mathscr{A} = \langle \boldsymbol{Q}, \boldsymbol{\Sigma}, \boldsymbol{\delta} \rangle$, a subset $\boldsymbol{P} \subset \boldsymbol{Q}$ is *extensible* if $\boldsymbol{P} = \boldsymbol{R} \,.\, \boldsymbol{w}$ for some $\boldsymbol{w} \in \boldsymbol{\Sigma}^*$ of length at most $\boldsymbol{n} = |\boldsymbol{Q}|$ and some $\boldsymbol{R} \subseteq \boldsymbol{Q}$ with $|\boldsymbol{R}| > |\boldsymbol{P}|$.

Kari's Example

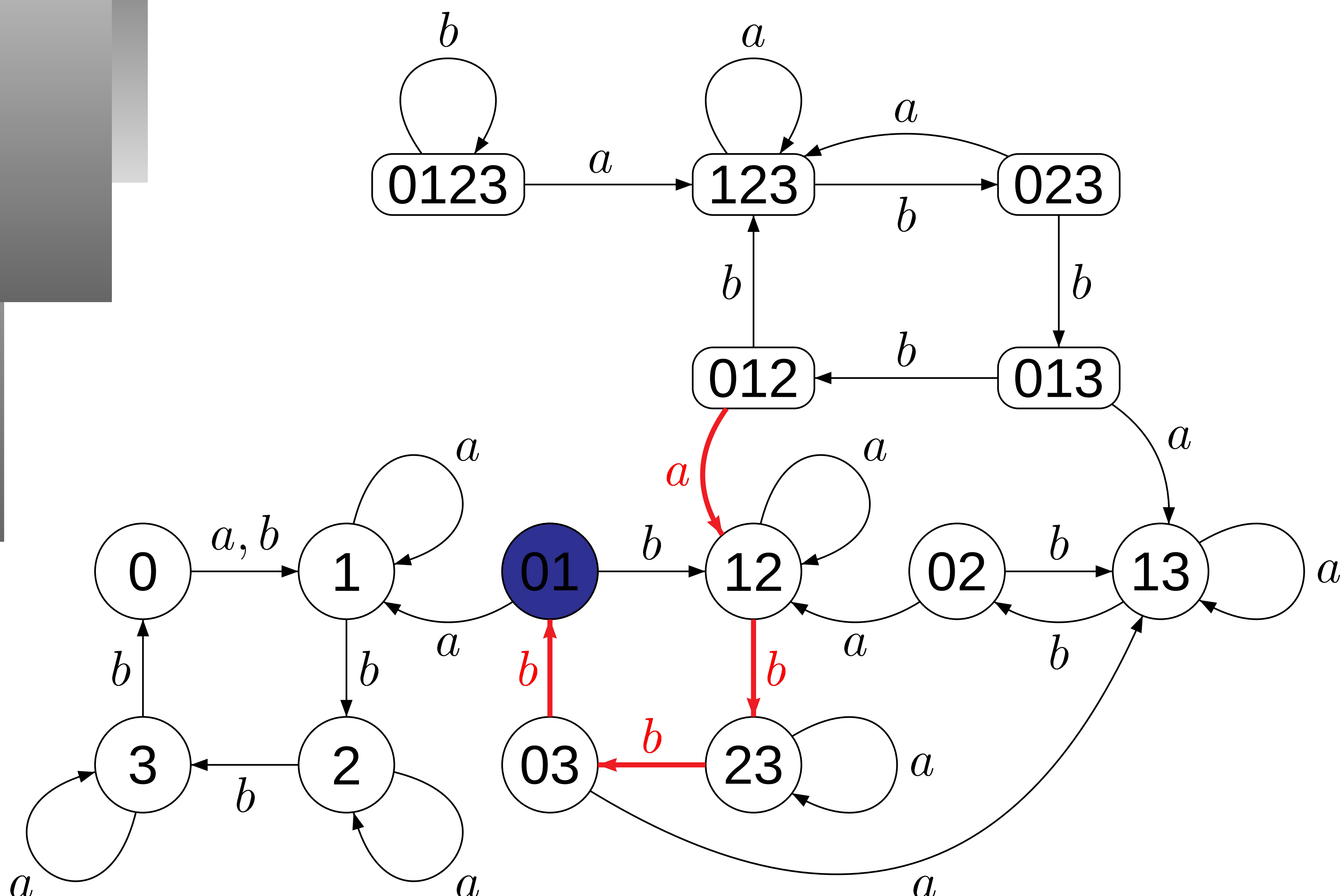
Kari's automaton does not refute the rank conjecture! In the solitaire game on $\mathscr{K}_6$, no sequence of 16 moves removes 4 coins. However, 4 is not the maximum number of tokens that can be removed! One can show that 5 states can be freed by a sequence of 25 moves — in full accordance with the rank conjecture.

Yet another hope killed by Kari's example is the extensibility conjecture. In a DFA $\mathscr{A} = \langle Q, \Sigma, \delta \rangle$, a subset $P \subset Q$ is *extensible* if $P = R \,.\, w$ for some $w \in \Sigma^*$ of length at most $n = |Q|$ and some $R \subseteq Q$ with $|R| > |P|$. It was conjectured that in synchronizing automata every proper non-singleton subset is extensible.

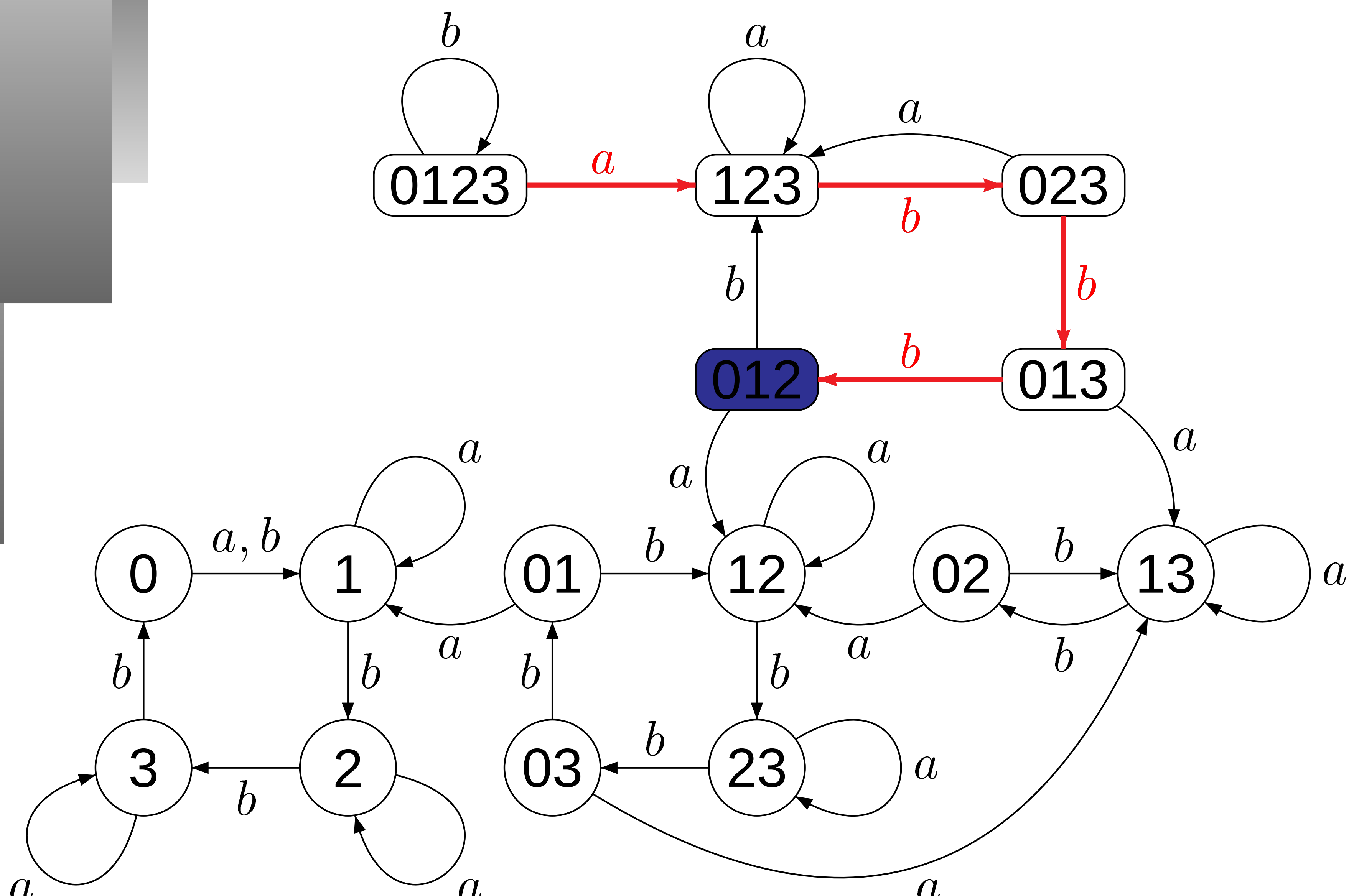
Extensibility



Extensibility



Extensibility



Extensibility

Observe that the extensibility conjecture implies the Černý conjecture.

Extensibility

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

Extensibility

Observe that the extensibility conjecture implies the Černý conjecture.

Indeed, if $\mathscr{A} = \langle Q, \Sigma, \delta \rangle$ is synchronizing, then some letter $a \in \Sigma$ should sent 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 $P_{i-1} = P_i \cdot w_i$ for some word w_i of length $\leq n$.

Extensibility

Observe that the extensibility conjecture implies the Černý conjecture.
Indeed, if $\mathscr{A} = \langle Q, \Sigma, \delta \rangle$ is synchronizing, then some letter $a \in \Sigma$ should sent 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 $P_{i-1} = P_i \,.\, w_i$ 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

$$Q \,.\, w_{n-2} w_{n-1} \cdots w_1 a = \{p\},$$

that is, $w_{n-2} w_{n-1} \cdots w_1 a$ is a reset word.

Extensibility

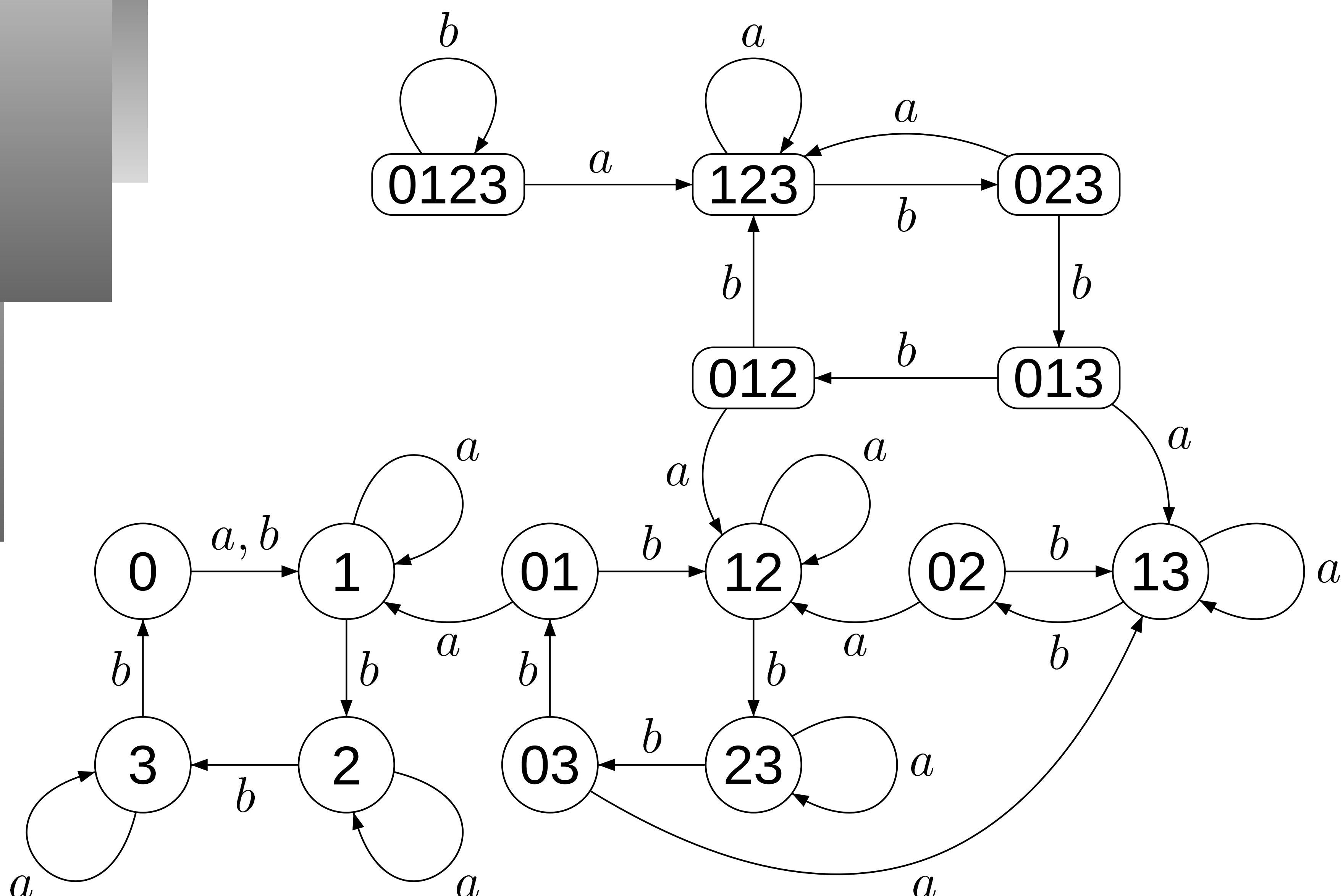
Observe that the extensibility conjecture implies the Černý conjecture.

Indeed, if $\mathscr{A} = \langle Q, \Sigma, \delta \rangle$ is synchronizing, then some letter $a \in \Sigma$ should sent 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 $P_{i-1} = P_i \,.\, w_i$ 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

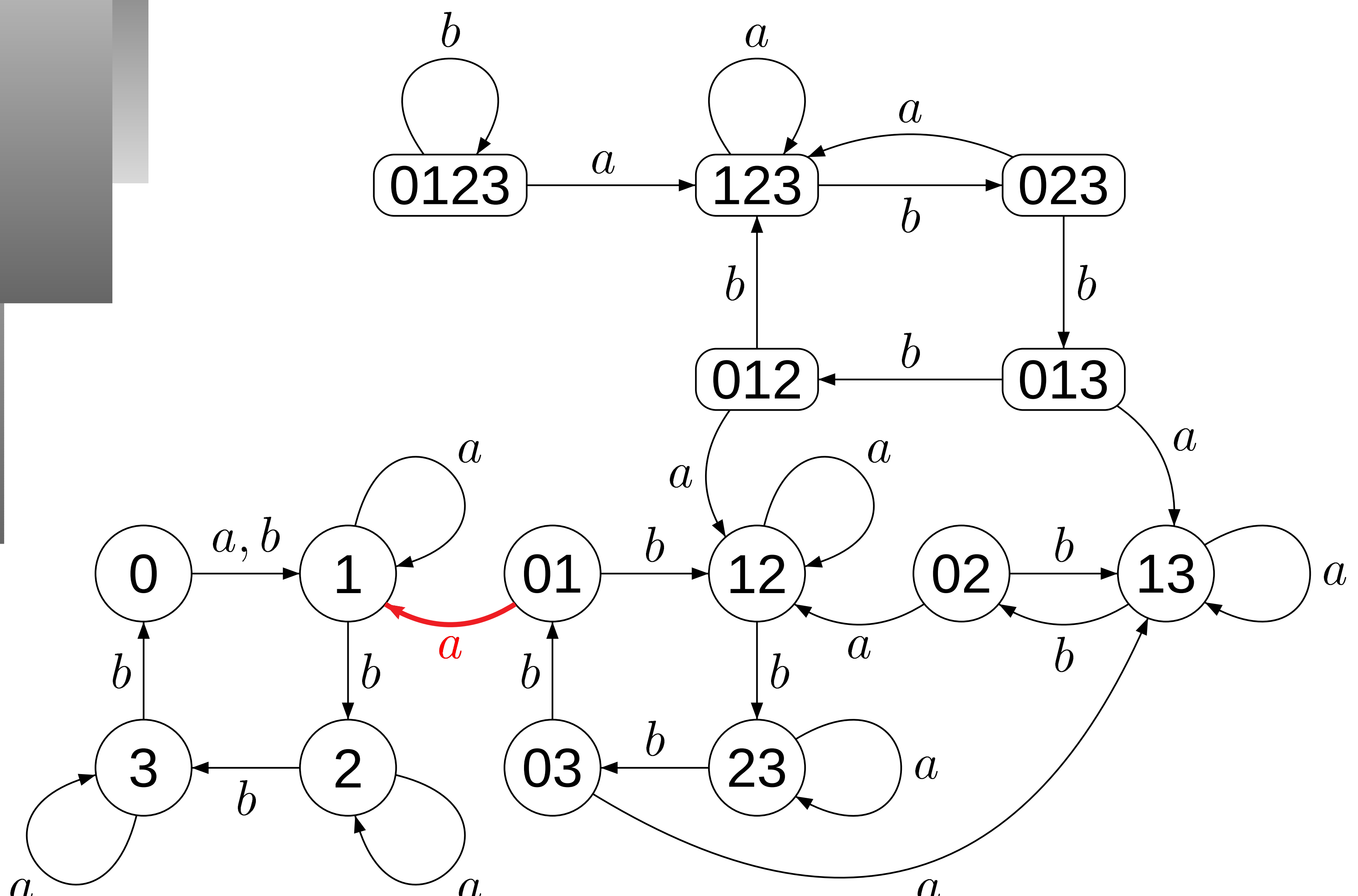
$$Q \,.\, w_{n-2} w_{n-1} \cdots w_1 a = \{p\},$$

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

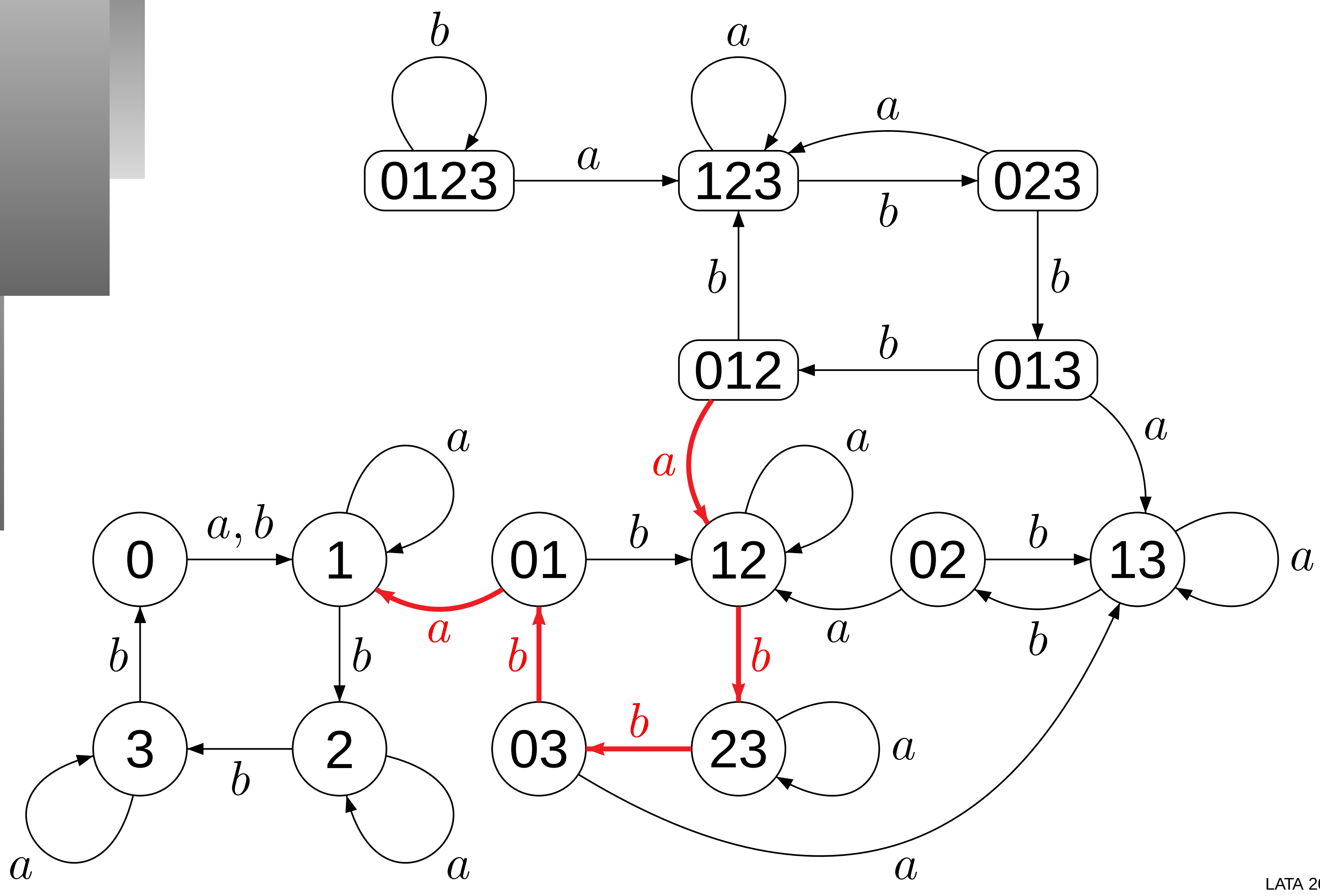
Extensibility



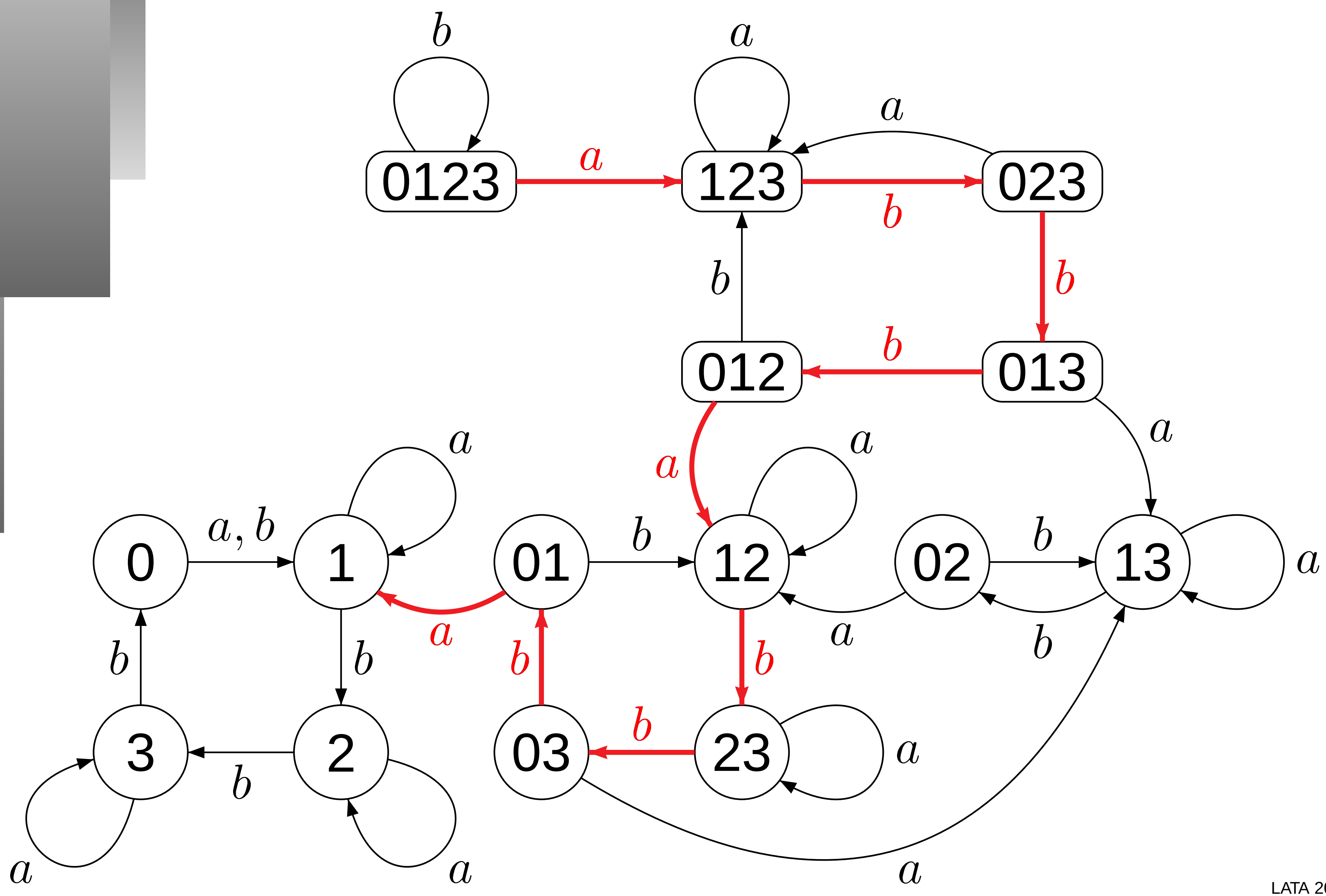
Extensibility



Extensibility



Extensibility



Extensibility

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, in particular:

Extensibility

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, in particular:

- 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 (1998) 21–34 [in French]).

Extensibility

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, in particular:

• 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 (1998) 21–34 [in French]).
• Jarkko Kari's result for automata with Eulerian digraphs (Synchronizing finite automata on Eulerian digraphs, Theoret. Comput. Sci., 295 (2003) 223–232.)

Extensibility vs Kari's Example

However, in $\mathscr{K}_{\mathbf{6}}$ 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).

Extensibility vs Kari's Example

However, in $\mathscr{K}_{\mathbf{6}}$ 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.