Fast Synchronization of Random Automata

JCB 2020

Cyril Nicaud

LIGM – Univ Gustave Eiffel & CNRS

February 2020

Topic of the talk

Does the Černý conjecture hold with high probability?

Topic of the talk

Does the Černý conjecture hold with high probability?

The Černý conjecture (1964)

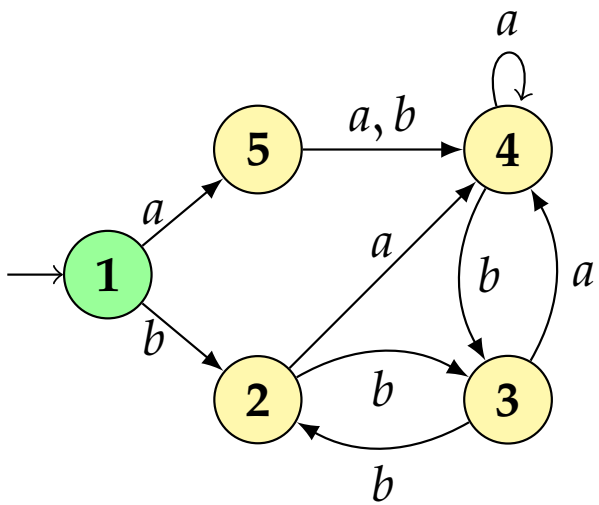
A synchronizing automaton with n states admits a synchronizing word of length at most $(n-1)^2$.

1. Automata & Synchronization

Deterministic and complete automata

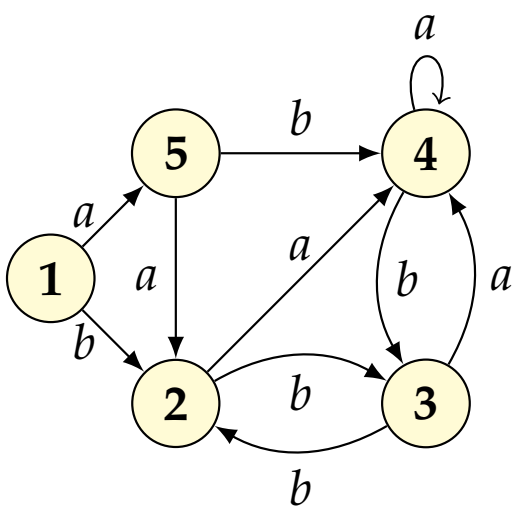
A (complete and deterministic) automaton is a directed graph s.t.:

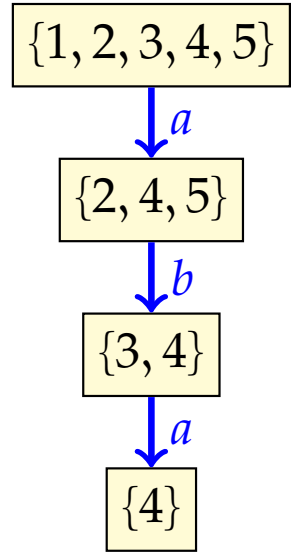
- vertices are called "states", and edges are called "transitions"
- For each state and for each letter a of a fixed alphabet A, there is exactly one outgoing transition labeled by a



Synchronizing automata

- An automaton is **synchronizing** when there exists a word that brings every state to one and the same state
- Such a word is a **synchronizing word**

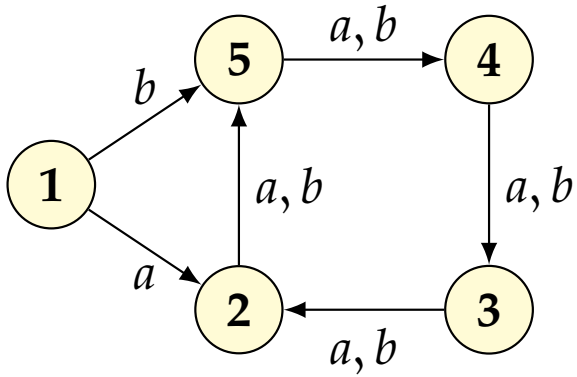




- *aaaa* is a synchronizing word
- *aba* is a smaller synchronizing word

Synchronizing automata

- An automaton is **synchronizing** when there exists a word that brings every state to one and the same state
- Such a word is a **synchronizing word**



- This automaton is not synchronizing.

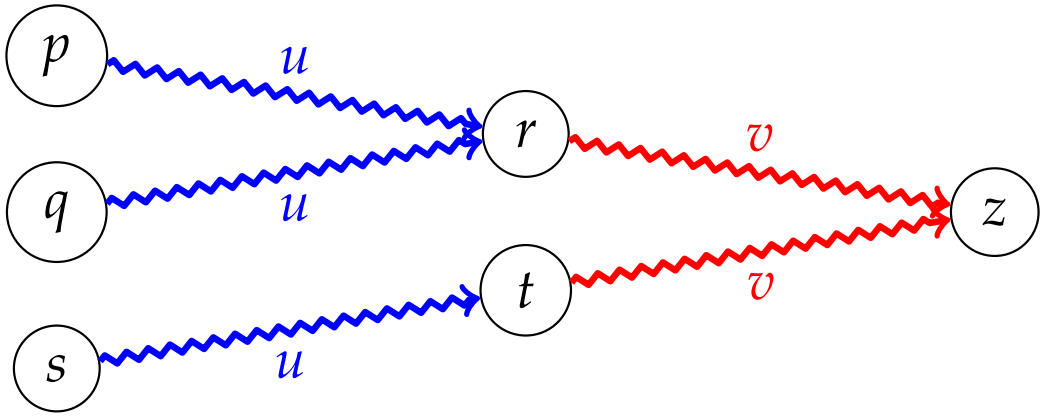
Pairwise Synchronization

- A pair of states (p,q) is synchronized when there exists a word u such that $p \cdot u = q \cdot u$.

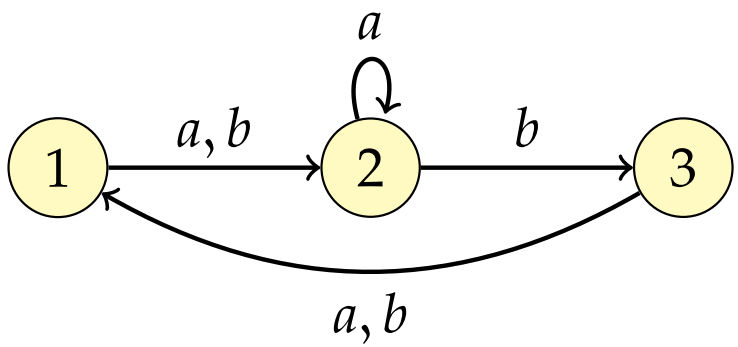
Lemma

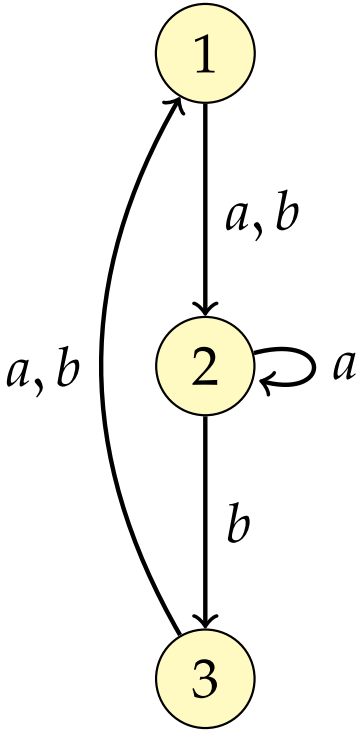
If every pair of states is synchronized, then the automaton is synchronizing.

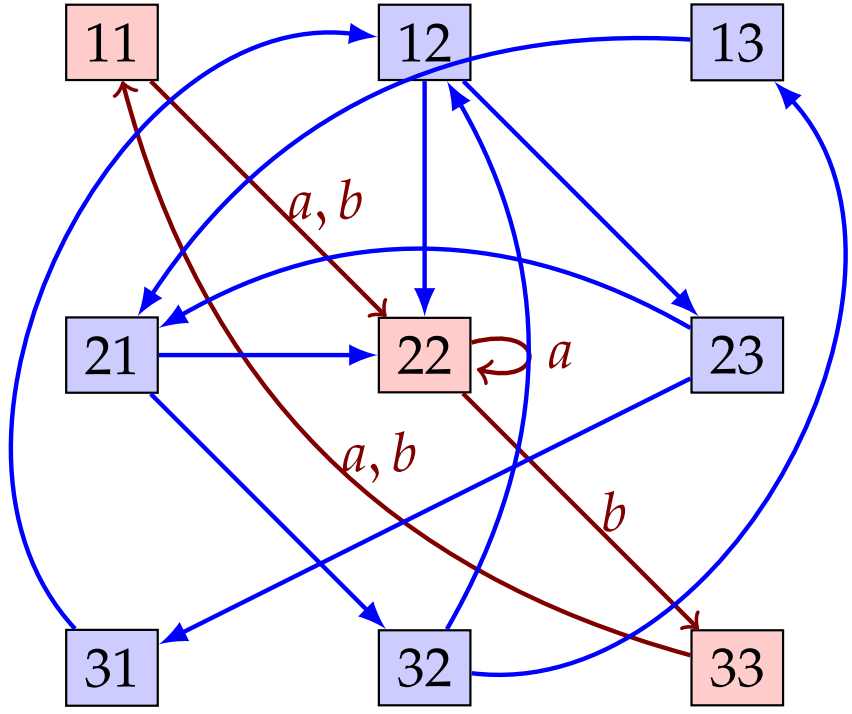
More precisely, is every pair is synchronized by a word of length at most ℓ, then the automaton is synchronized by a word of length at most $n(\ell - 1)$.



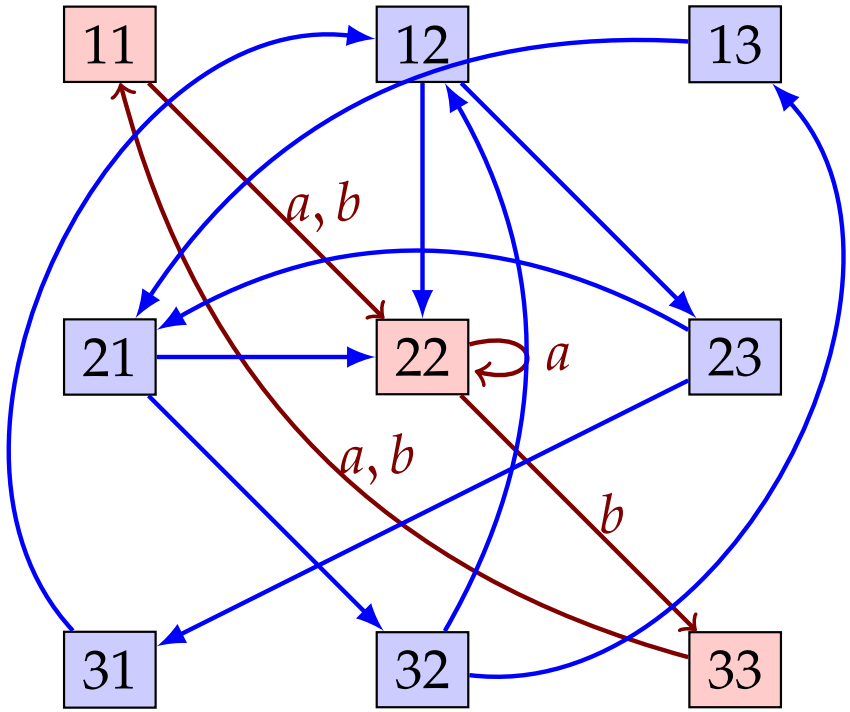
Checking Synchronization: Square of an Automaton







Checking Synchronization: Square of an Automaton



- Synchronizing iff there is a path from every (p, q) to a state (x, x)
- Checked in $\mathcal{O}(n^2)$
- Using the lemma: synchronizing word of length at most n^3

The Černý conjecture

Conjecture [Černý 64]

A synchronizing automaton with n states admits a synchronizing word of length at most $(n-1)^2$.

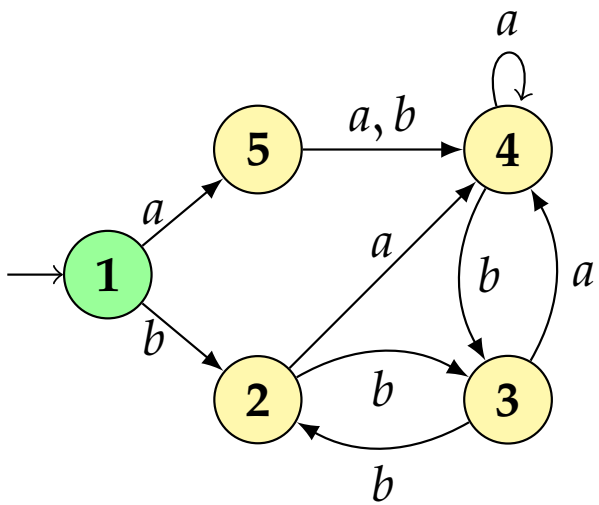
- $(n-1)^2$ is best possible
- n^3 is trivial
- First (general) known bound [Frankl] [Pin 83]: $\frac{1}{6}(n^3 - n)$.
- the conjecture holds for many families of automata
- [Szykuła 18] improve the coefficient of n^3 to $\frac{114}{685} = \frac{1}{6} - \frac{1}{4110}$

2. Settings

Deterministic and complete automata

A (complete and deterministic) automaton is a directed graph s.t.:

- vertices are called "states", and edges are called "transitions"
- For each state and for each letter a of a fixed alphabet A, there is exactly one outgoing transition labeled by a



Random deterministic automata: some models

There are three main probabilistic models:

- **Uniform deterministic and complete automata:** the target of each transition is chosen uniformly at random, independently
- Uniform **accessible** deterministic and complete automata
- Uniform **minimal** automata

For these models, we can instead consider that each state is final with some fixed probability $p \in (0, 1)$, independently.

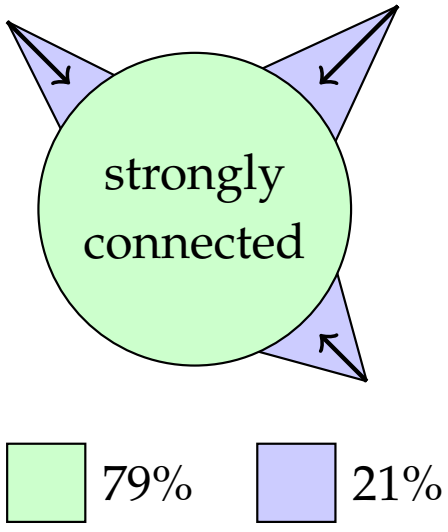
In this talk : our model is the first one, the simplest.

Random automata vs random digraphs

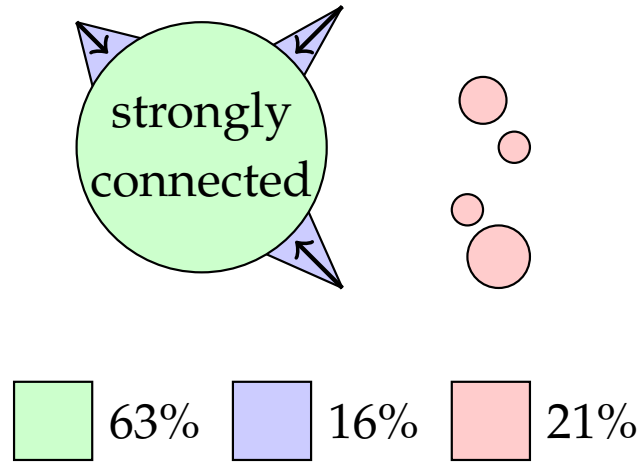
For $A = \{a, b\}$.

- **Random automata:** each state has 2 outgoing transitions
- **Random digraph (Erdős-Rényi):** each edge has probability $\frac{2}{n}$
- Let θ be the unique positive real solution of $1 - x = e^{-2x}$ ($\theta \approx 0.79$)

Random automaton



Random digraph [Karp 90]



Probabilistic Černý conjecture

Question 1

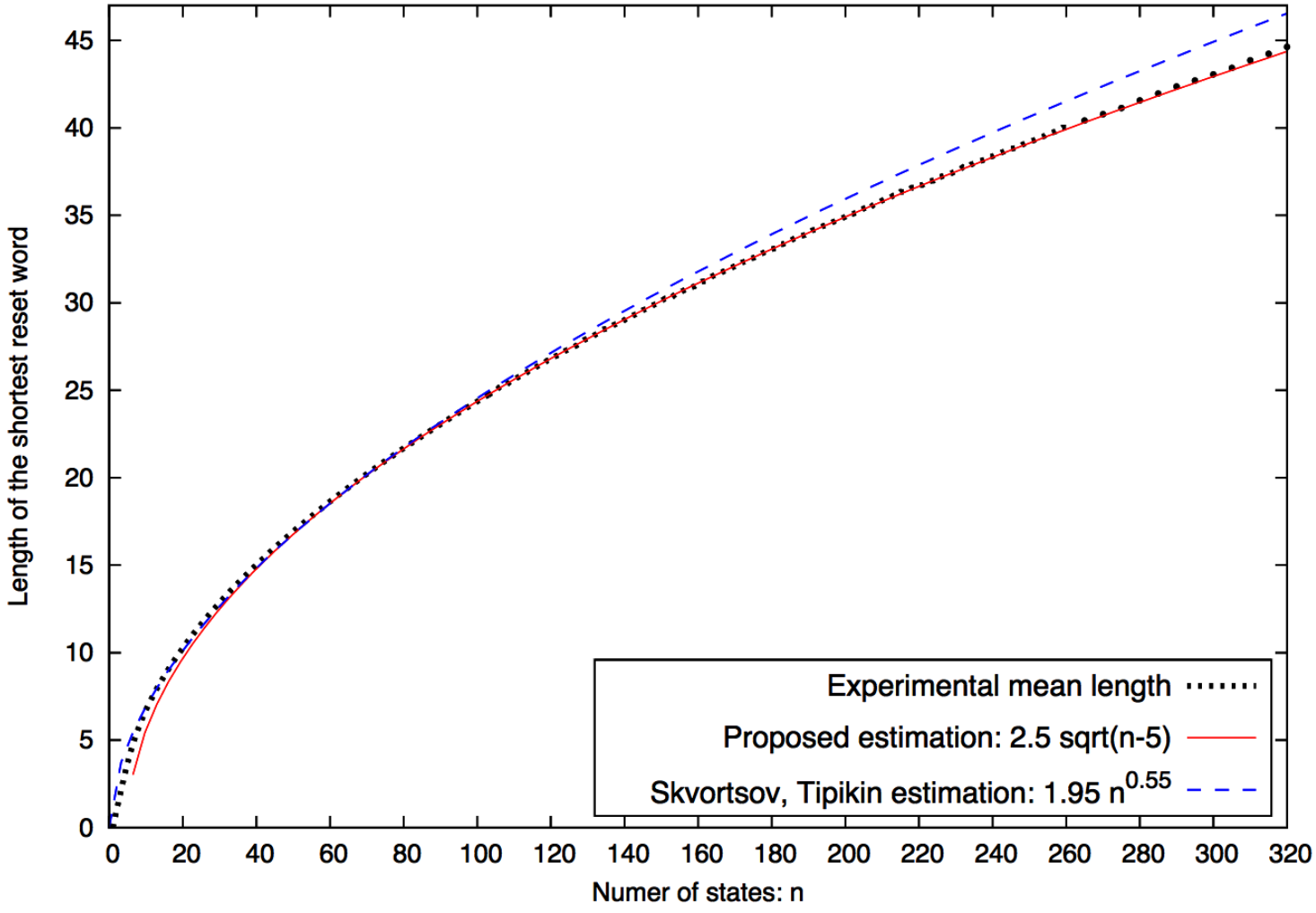
What is the probability that an automaton is synchronizing?

Question 2

Does the Černý conjecture hold with high probability?

Experiments [Kisielewicz, Kowalski and Szykuła 13]

:



The graphic comes from [Kisielewicz, Kowalski and Szykuła 13]

Answer to Q1: Berlinkov's theorem

Theorem [Berlinkov'16]

For alphabets with at least two letters, deterministic automata are synchronizing with high probability.

More precisely, a random automaton is not synchronizing with probability $\mathcal{O}(\frac{1}{n^{k/2}})$.

- For $k = 2$, the bound is tight: $\Theta(\frac{1}{n})$.

An answer to Q2: this talk

Theorem [N. RANDOM'16]

For alphabets with at least two letters, a random automaton admits a synchronizing word of length at most $\mathcal{O}(n \log^3 n)$ with high probability.

- The proof is independent of Berlinkov's proof
- It is more elementary
- The error term is not tight
- It provides information on the reset threshold

Corollary

For alphabets with at least two letters, the Černý conjecture holds with high probability.

An algebraic version

- in an automaton, the action of each letter a on the set of states is a mapping δ_a
- we are interested in the monoid generated by the δ_a's

An algebraic version

- in an automaton, the action of each letter a on the set of states is a mapping δ_a
- we are interested in the monoid generated by the δ_a's

Theorem (Dixon 69)

Let σ and τ be two uniform random **permutations** of size n. With high probability, the group generated by σ and τ is either the symmetric group or the alternating group.

An algebraic version

- in an automaton, the action of each letter a on the set of states is a mapping δ_a
- we are interested in the monoid generated by the δ_a's

Theorem (Dixon 69)

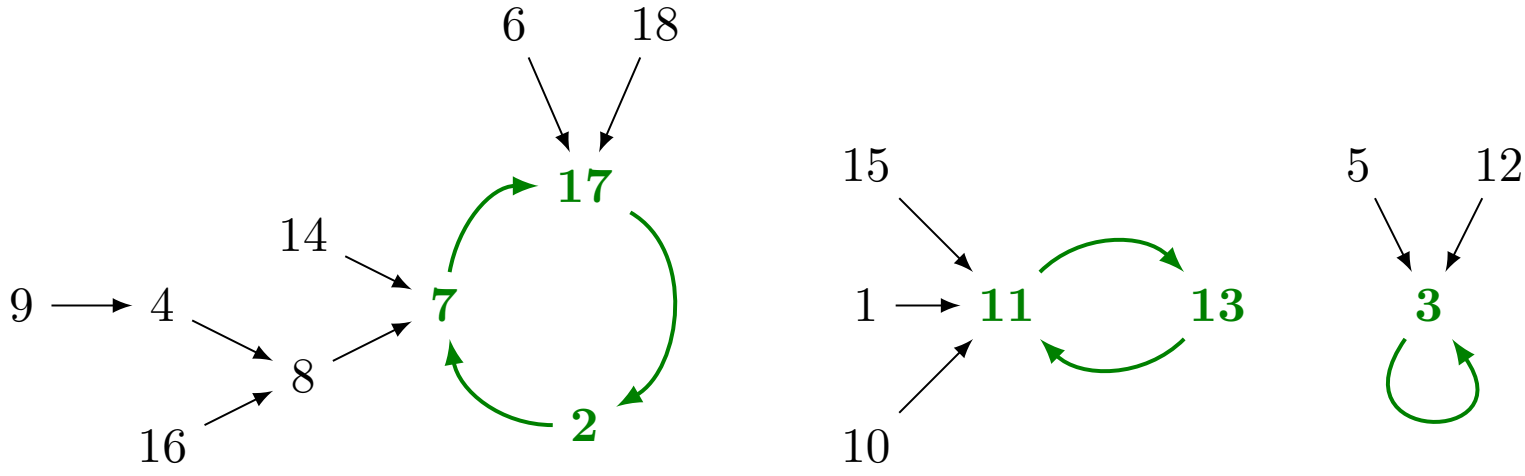
Let σ and τ be two uniform random **permutations** of size n. With high probability, the group generated by σ and τ is either the symmetric group or the alternating group.

- An automaton is **synchronized** $\Leftrightarrow$ the monoid **contains a constant map**

3. Proof sketch

Tuples of random mappings

- We consider **uniform random mapping** from $[n]$ to itself
- Its functional graph is a set of cycles of trees
- The mapping below has height 3, and it has 6 cyclic points



- A tuple of uniform random mappings defines a uniform random automaton (one mapping for the action of each letter)

A property of random p-mappings

Lemma

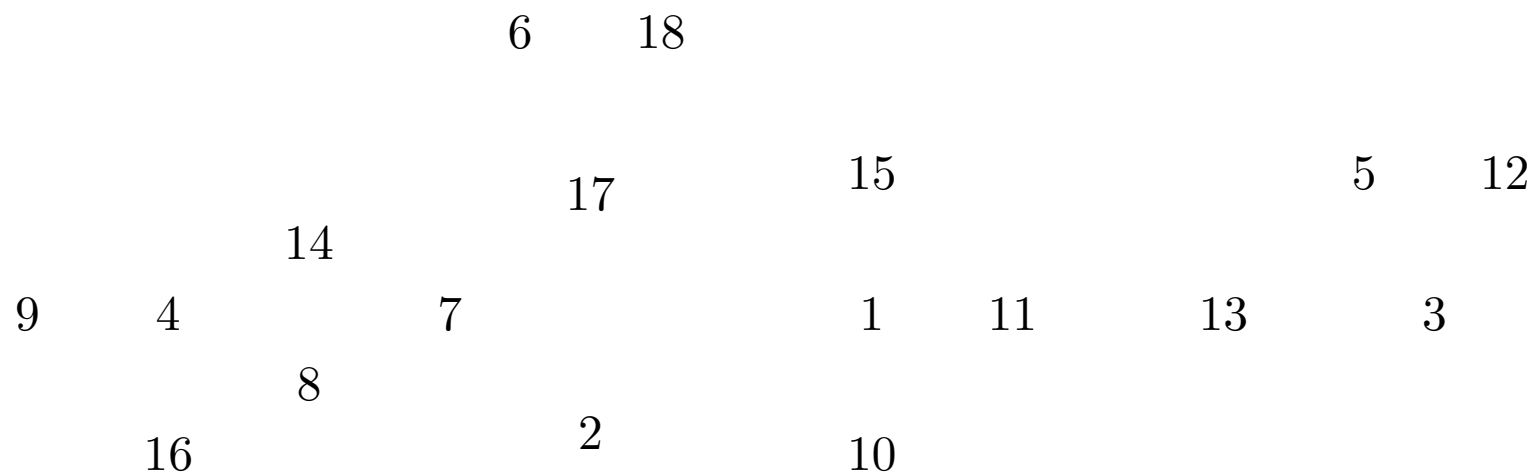
With high probability, a uniform random mapping has **height** at most $2\sqrt{n \log n}$ and has at most $2\sqrt{n \log n}$ **cyclic points**. It still holds for p-random mappings.

- **Proof:** Birthday paradox.

- random p-mapping: the image of each element is taken independently in $[n]$, following the probability distribution p.

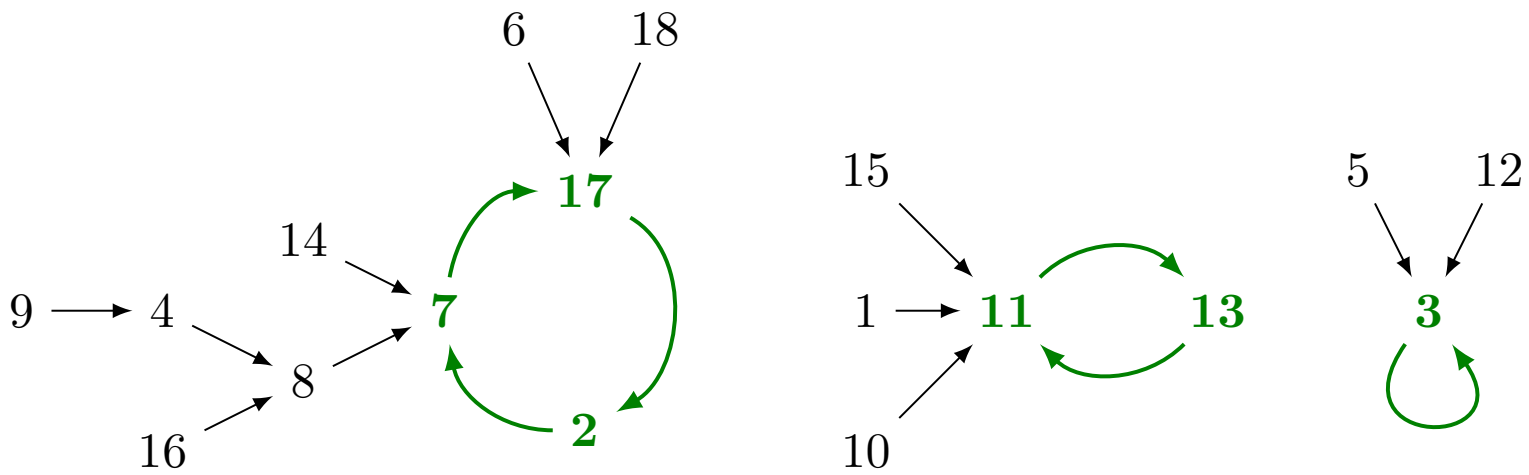
First step: a-transitions

- **Main idea:**
  - Start from an automaton with no transitions
  - Add random transitions as needed
- First, we add all the a-transitions

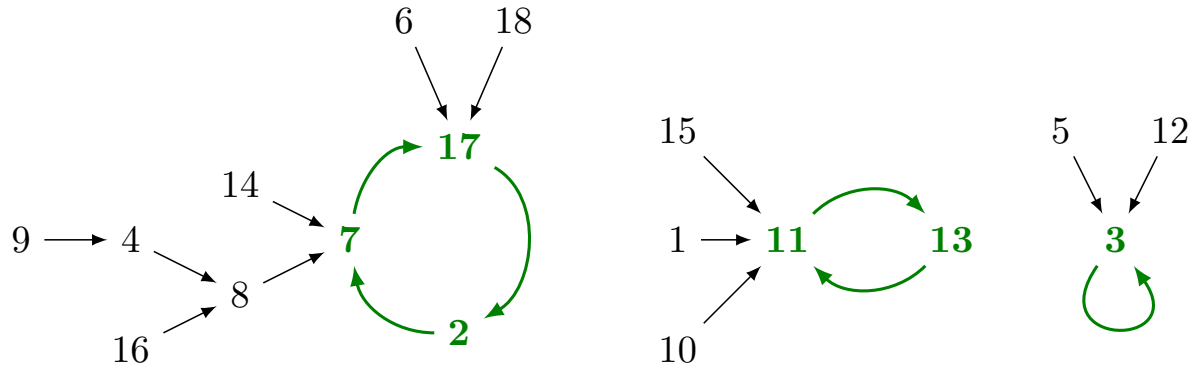


First step: *a*-transitions

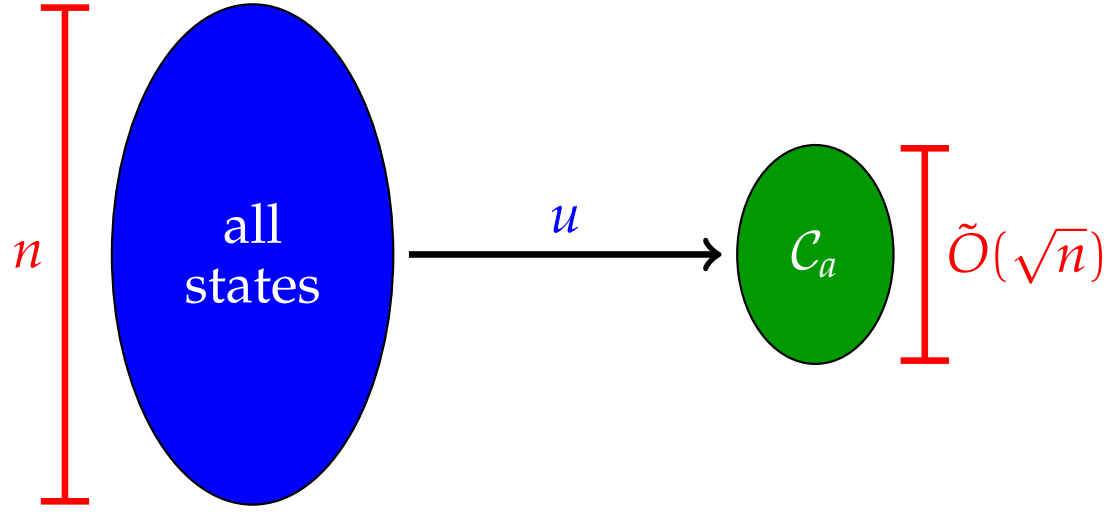
- **Main idea:**
  - Start from an automaton with no transitions
  - Add random transitions as needed
- First, we add all the *a*-transitions



Shrinking to a-cyclic points

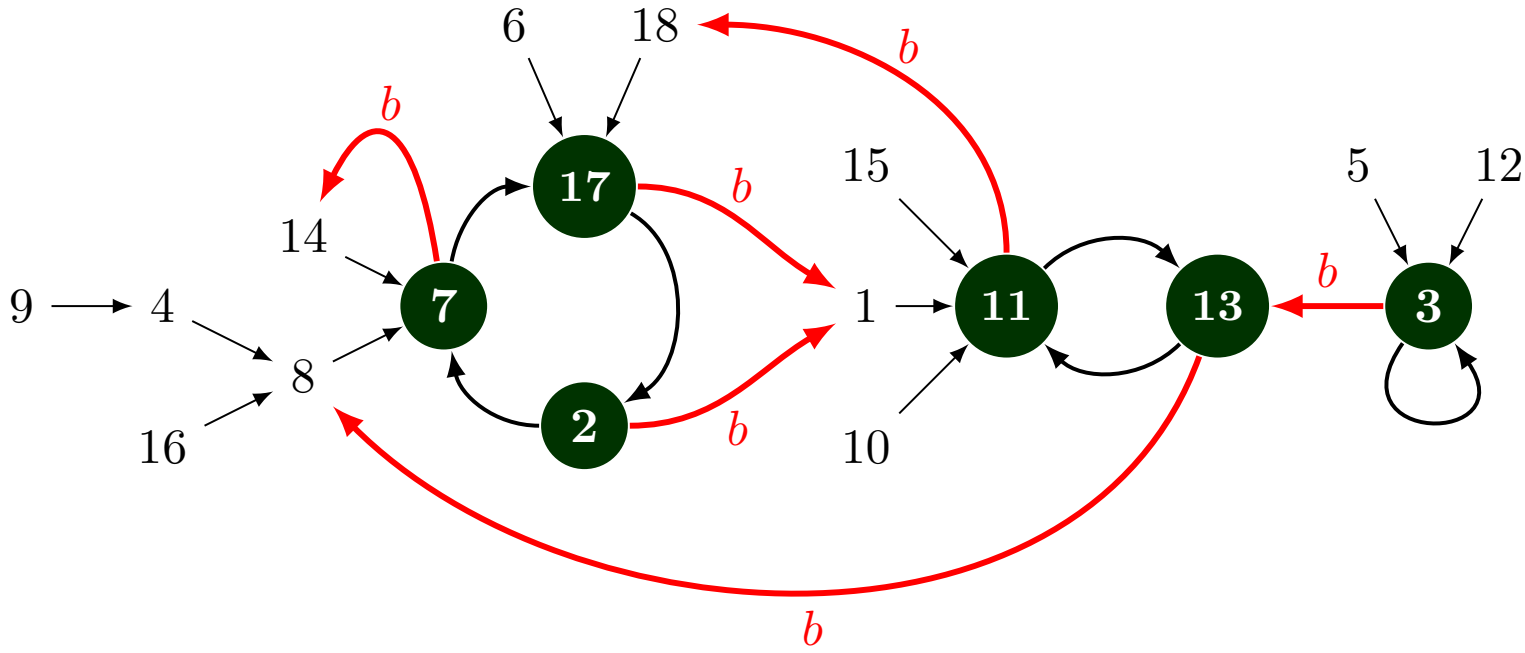


- $\mathcal{C}_a$ is the set of a-cyclic points
- W.h.p., $|\mathcal{C}_a| \leq 2\sqrt{n \log n}$ and $u = a^{2\sqrt{n \log n}}$ maps $[n]$ to $\mathcal{C}_a$



Shrinking $\mathcal{C}_a$

- We fix the a-transitions
- We now generate b-transitions starting from the states of $\mathcal{C}_a$

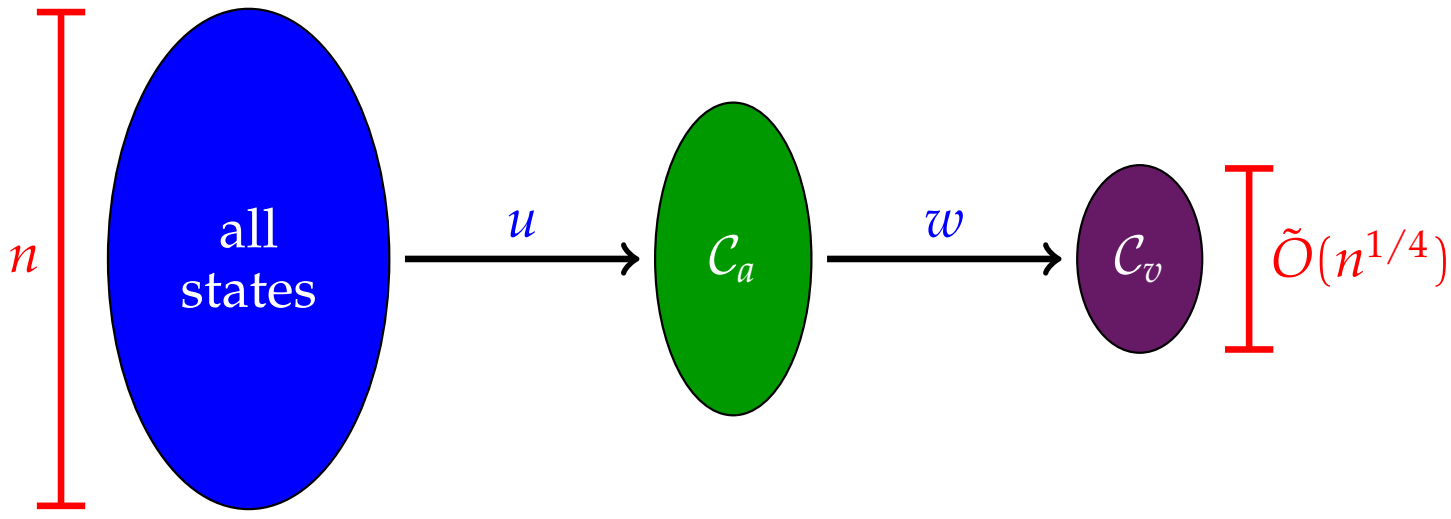


- We consider the map $\delta_v : \mathcal{C}_a \to \mathcal{C}_a$ defined with $v = bu$

$$\mathbb{P}\left(f(p) = q\right) = \frac{\text{number of preimages of } q \text{ by } u}{n}$$

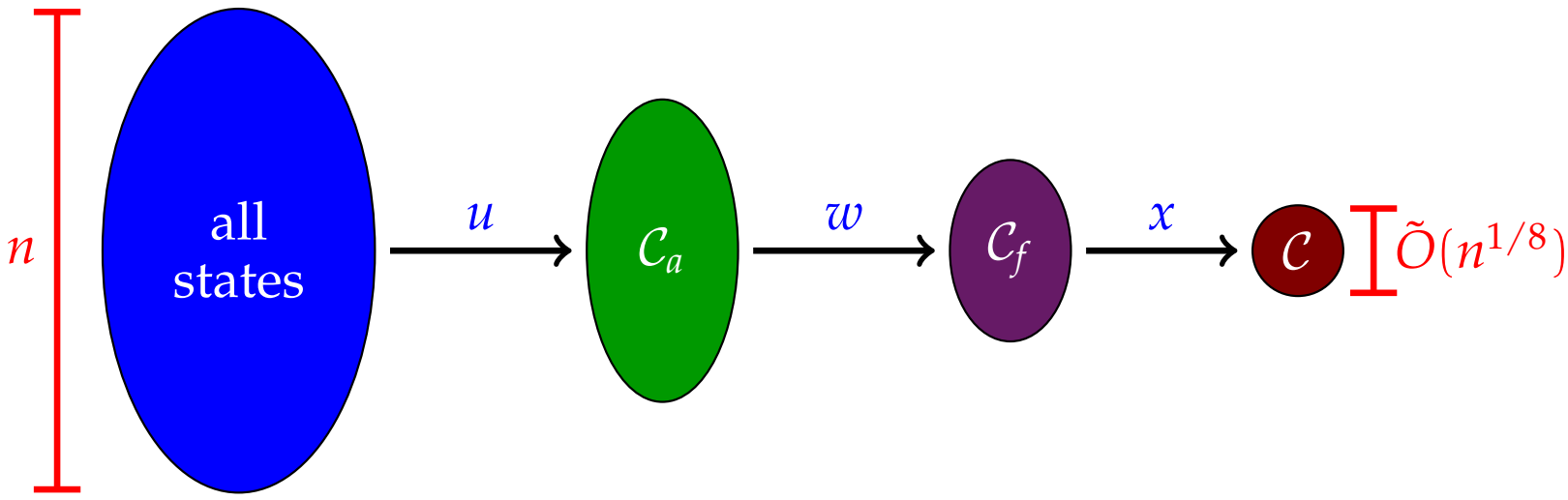
Shrinking $\mathcal{C}_a$

- δ_v is a **random p-mapping** on $\mathcal{C}_a$
- Let $w = v^{\beta_n}$, with $\beta_n = 3n^{1/4}(\log n)^{3/4}$
- W.h.p $|\mathcal{C}_w| \leq \beta_n$ and δ_w maps $\mathcal{C}_a$ to $\mathcal{C}_w$



Shrinking once more

- Using a third letter c, we can do the same trick once again
- If $A = \{a, b\}$, with some care, we can use $c = bb$

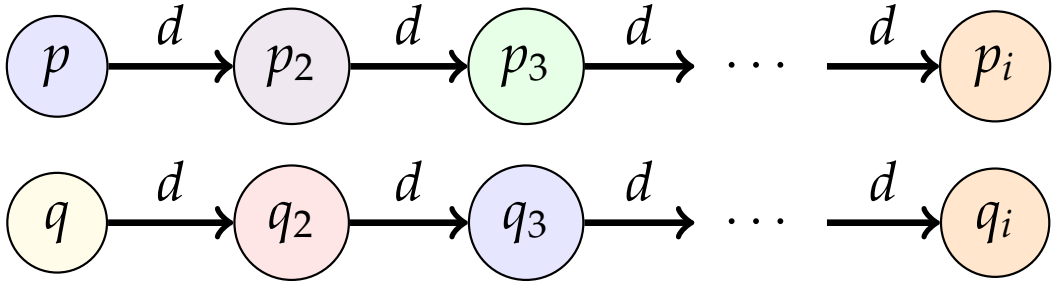


- W.h.p. the word $s = uwx$ has length at most $n^{7/8} \log^3 n$ and maps the set of states to a set C of size $\tilde{O}(n^{1/8})$.

Synchronizing $\mathcal{C}$

- We synchronize every pair (p, q) of states of $\mathcal{C}$

Repeatedly draw d-transitions starting from p and q:



- if $\delta_s(p_i) = \delta_s(q_i)$ the synchronization is a **success**
- if p_i or q_i already have a d-transition or if the sequence is too long, it is a **failure**
- **Proposition:** w.h.p. this synchronization process is a **success** for every pair of states of $\mathcal{C}$.

Proof sketch

- Shrink the set of states three times to a set $\mathcal{C}$ of size $\approx n^{1/8}$
- Synchronize pairs of states of $\mathcal{C}$ using words of the form $d^i \cdot s$
- **(technical)** adapt the proof to alphabets with two letters

Theorem (N. 16)

For alphabets with at least two letters, a random automaton admits a synchronizing word of length at most $\mathcal{O}(n \log^3 n)$ with high probability.

Further directions

- The expected reset threshold in $\Theta(\sqrt{n})$
- The error term in $\Theta(1/n)$

- Proof of the **Černý conjecture** ...

Thanks!