Subset Synchronization of Transitive Automata

Vojtěch Vorel

Charles University
Prague, Czech Republic

AFL 2014

Outline

Outline

Finite Automata

- *DFA* is a triple $A = (Q, \Sigma, \delta)$
  - Q ... finite set of *states*
  - Σ ... finite set of *letters* (the *alphabet*)
  - δ ... total function $Q \times \Sigma \to Q$ (*transition function*)
- Extended transition function:

$$\delta : 2^Q \times \Sigma^\star \to 2^Q$$

Finite Automata

- *DFA* is a triple $A = (Q, \Sigma, \delta)$
  - Q ... finite set of *states*
  - Σ ... finite set of *letters* (the *alphabet*)
  - δ ... total function $Q \times \Sigma \to Q$ (*transition function*)
- Extended transition function:

$$\delta : 2^Q \times \Sigma^\star \to 2^Q$$

Outline

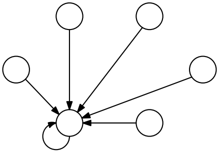
1. Synchronization of a DFA
   - DFA
   - Classical Synchronization
   - Subset Synchronization & The Result
2. Depth of Transformations
3. Proof Methods

Reset Words

- $w \in \Sigma^\star$ is a *reset word* of A if

$$|\delta(Q, w)| = 1,$$

i.e. if w acts like



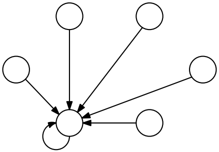
- If A has some reset word, we call it *synchronizing*.

Reset Words

- $w \in \Sigma^\star$ is a *reset word* of A if

$$|\delta(Q, w)| = 1,$$

  i.e. if w acts like



- If A has some reset word, we call it *synchronizing*.

Shortest Reset Words

- **Černý conjecture:**
  - If A is synchronizing, it has a reset word of length at most $(|Q|-1)^2$
- Known upper bounds:
  - $\frac{1}{3}|Q|^3 - n^2 + \frac{5}{3}n - 1$ (Kohavi, 1970)
  - $\frac{1}{6}|Q|^3 - \frac{1}{6}n$ (Pin, 1983)

Shortest Reset Words

- **Černý conjecture:**
  - If A is synchronizing, it has a reset word of length at most $(|Q|-1)^2$
- Known upper bounds:
  - $\frac{1}{3}|Q|^3 - n^2 + \frac{5}{3}n - 1$ (Kohavi, 1970)
  - $\frac{1}{6}|Q|^3 - \frac{1}{6}n$ (Pin, 1983)

Outline

1 Synchronization of a DFA
- DFA
- Classical Synchronization
- Subset Synchronization & The Result

2 Depth of Transformations

3 Proof Methods

Subset Reset Words

- $w \in \Sigma^\star$ is a *reset word of* $S \subseteq Q$ if

$$|\delta(S, w)| = 1,$$

  i.e. if w maps states from S to a unique state.

- If S has some reset word, we call it *synchronized.*

Subset Reset Words

- $w \in \Sigma^{\star}$ is a *reset word of* $S \subseteq Q$ if

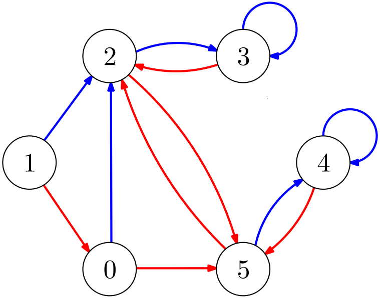
$$|\delta(S, w)| = 1,$$

i.e. if w maps states from S to a unique state.

- If S has some reset word, we call it *synchronized.*

Subset Reset Words: an Example

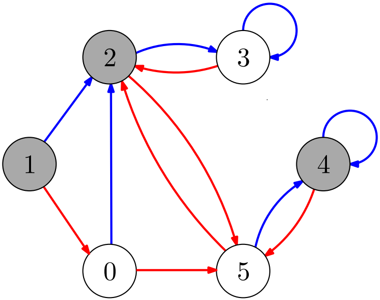
$Q = \{0, 1, 2, 3, 4, 5\}$
$\Sigma = \{a, b\}$



Subset Reset Words: an Example

$Q = \{0, 1, 2, 3, 4, 5\}$
$\Sigma = \{a, b\}$
$S = \{1, 2, 4\}$

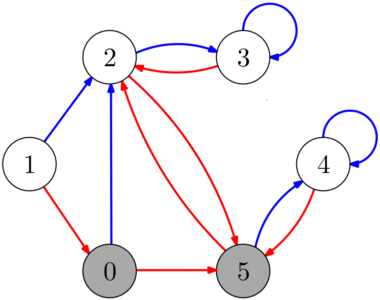
$w =$



Subset Reset Words: an Example

$Q = \{0, 1, 2, 3, 4, 5\}$
$\Sigma = \{a, b\}$
$S = \{1, 2, 4\}$

$w = a$

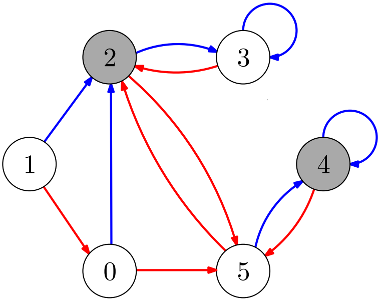


$$\left| \boxed{\delta(S, w)} \right| = 2$$

Subset Reset Words: an Example

$Q = \{0, 1, 2, 3, 4, 5\}$
$\Sigma = \{a, b\}$
$S = \{1, 2, 4\}$

$w = ab$

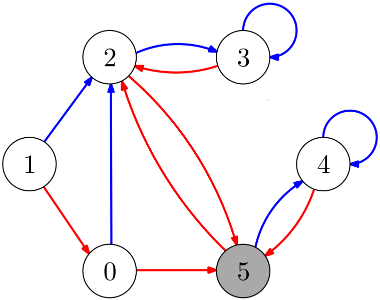


$$\left| \boxed{\delta(S, w)} \right| = 2$$

Subset Reset Words: an Example

$Q = \{0, 1, 2, 3, 4, 5\}$
$\Sigma = \{a, b\}$
$S = \{1, 2, 4\}$

$w = aba$
is a reset word of S



$$\left| \boxed{\delta(S, w)} \right| = 1$$

Bounds for Shortest Reset Words

	Classical Synchronization
Upper Bounds	$\mathcal{O}\left(\lvert Q\rvert^3\right)$
Lower Bounds	$\mathcal{O}\left(\lvert Q\rvert^2\right)$

Bounds for Shortest Reset Words

	Classical Synchronization	Subset Synchronization
Upper Bounds	$\mathcal{O}\left(\lvert Q\rvert^3\right)$	$2^{\mathcal{O}(\lvert Q\rvert)}$
Lower Bounds	$\mathcal{O}\left(\lvert Q\rvert^2\right)$	$2^{\Omega(\lvert Q\rvert)}$

Bounds for Shortest Reset Words

Over constant-size alphabets:

	Classical Synchronization	Subset Synchronization
Upper Bounds	$\mathcal{O}\left(\lvert Q\rvert^3\right)$	$2^{\mathcal{O}(\lvert Q\rvert)}$
Lower Bounds	$\mathcal{O}\left(\lvert Q\rvert^2\right)$	

Bounds for Shortest Reset Words

Over constant-size alphabets:

	Classical Synchronization	Subset Synchronization
Upper Bounds	$\mathcal{O}\left(\lvert Q\rvert^3\right)$	$2^{\mathcal{O}(\lvert Q\rvert)}$
Lower Bounds	$\mathcal{O}\left(\lvert Q\rvert^2\right)$	Former: $2^{\Omega\left(\frac{\lvert Q\rvert}{\log\lvert Q\rvert}\right)}$ New: $2^{\Omega(\lvert Q\rvert)}$

Lower Bound Construction

Infinite series of DFA satisfying:

- $|Q|$ grows, $|\Sigma| = 2$
- There is always a subset $S \subseteq Q$ with a shortest reset word of length $2^{\Omega(|Q|)}$.
- Transitivity

Lower Bound Construction

Infinite series of DFA satisfying:

- $|Q|$ grows, $|\Sigma| = 2$
- There is always a subset $S \subseteq Q$ with a shortest reset word of length $2^{\Omega(|Q|)}$.
- Transitivity

Outline

Depth of Transformations

- Full Transformation Monoid $\mathcal{T}_n$
- $\mathbf{G} \subseteq \mathcal{T}_n$
- $\langle \mathbf{G} \rangle \subseteq \mathcal{T}_n$
- *Depth* of $f \in \langle \mathbf{G} \rangle$

Depth of Transformations

- Full Transformation Monoid $\mathcal{T}_n$
- $\mathbf{G} \subseteq \mathcal{T}_n$
- $\langle \mathbf{G} \rangle \subseteq \mathcal{T}_n$
- *Depth* of $f \in \langle \mathbf{G} \rangle$

Depth of Transformations

- Full Transformation Monoid $\mathcal{T}_n$
- $\mathbf{G} \subseteq \mathcal{T}_n$
- $\langle \mathbf{G} \rangle \subseteq \mathcal{T}_n$
- *Depth* of $f \in \langle \mathbf{G} \rangle$

Depth of Transformations

- Full Transformation Monoid $\mathcal{T}_n$
- $\mathbf{G} \subseteq \mathcal{T}_n$
- $\langle \mathbf{G} \rangle \subseteq \mathcal{T}_n$
- *Depth* of $f \in \langle \mathbf{G} \rangle$

Worst-Case Depth of $f \in \langle \mathbf{G} \rangle$

Upper Bounds	Trivial: n^n
Lower Bounds	

Worst-Case Depth of $f \in \langle \mathbf{G} \rangle$

Upper Bounds	Trivial: n^n
Lower Bounds	$2^{\Omega(n)}$

Worst-Case Depth of $f \in \langle \mathbf{G} \rangle$

With constant-size G:

Upper Bounds	Trivial: n^n
Lower Bounds	

Worst-Case Depth of $f \in \langle \mathbf{G} \rangle$

With constant-size G:

Upper Bounds	Trivial: n^n
Lower Bounds	Former: $2^{\Omega\left(\frac{n}{\log n}\right)}$ New: $2^{\Omega(n)}$

Lower Bound Construction

Infinite series of sets $\mathbf{G} \subseteq \mathcal{T}_n$ satisfying:

- n is growing
- There is always a function $f \in \langle \mathbf{G} \rangle$ in depth $2^{\Omega(n)}$.

Using bad cases of subset synchronization:

$$\text{DFA } A = ([n], \Sigma, \delta) \quad \longrightarrow \quad \mathbf{G} \subseteq \mathcal{T}_n$$

$$\text{Synchronized subset } S \subseteq [n] \quad \longrightarrow \quad f \in \langle \mathbf{G} \rangle \text{ constant on } S$$

Lower Bound Construction

Infinite series of sets $\mathbf{G} \subseteq \mathcal{T}_n$ satisfying:

- n is growing
- There is always a function $f \in \langle \mathbf{G} \rangle$ in depth $2^{\Omega(n)}$.

Using bad cases of subset synchronization:

$$\text{DFA } A = ([n], \Sigma, \delta) \quad \longrightarrow \quad \mathbf{G} \subseteq \mathcal{T}_n$$

$$\text{Synchronized subset } S \subseteq [n] \quad \longrightarrow \quad f \in \langle \mathbf{G} \rangle \text{ constant on } S$$

Outline

Instability of Subsets

A subset $S \subseteq Q$ is ***unstable*** if:

- S is synchronized
- $(\exists w \in \Sigma^\star)$
- $\delta(S, w)$ is not synchronized

Instability of Subsets

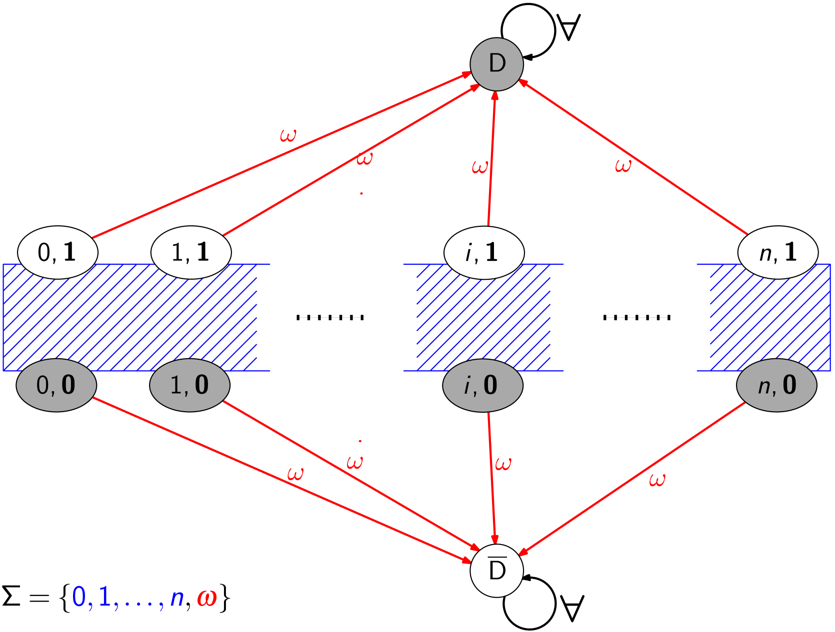
A subset $S \subseteq Q$ is ***unstable*** if:

- S is synchronized
- $(\exists w \in \Sigma^\star)$
- $\delta(S, w)$ is not synchronized

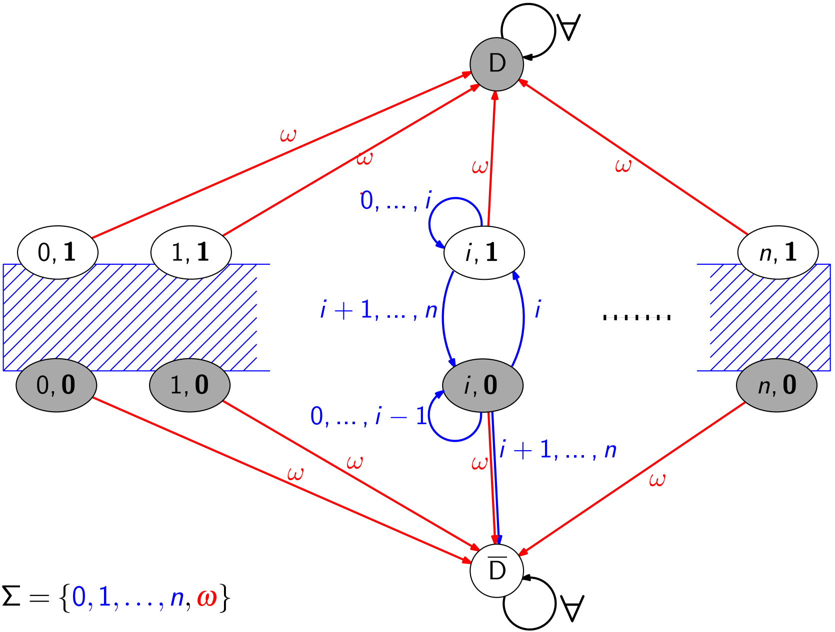
Instability of Subsets

A subset $S \subseteq Q$ is ***unstable*** if:

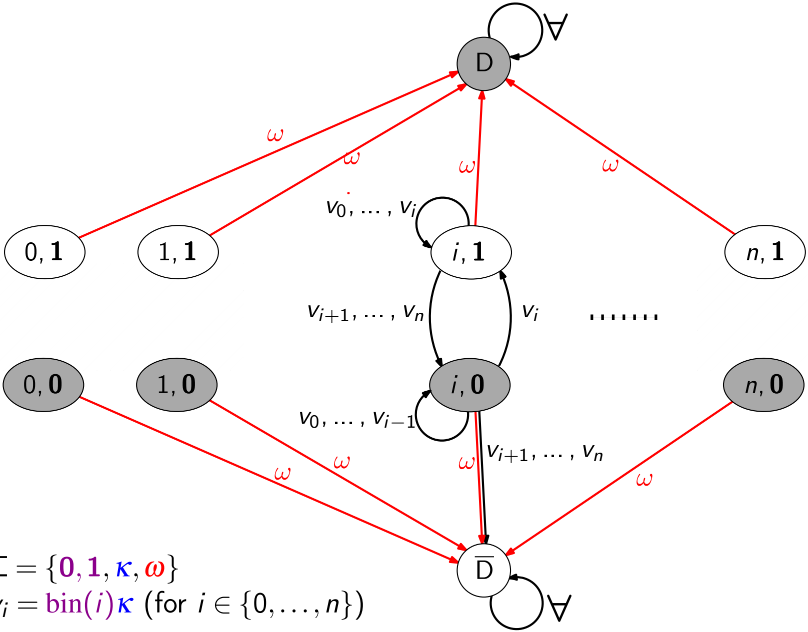
- S is synchronized
- $(\exists w \in \Sigma^{\star})$
- $\delta(S, w)$ is not synchronized



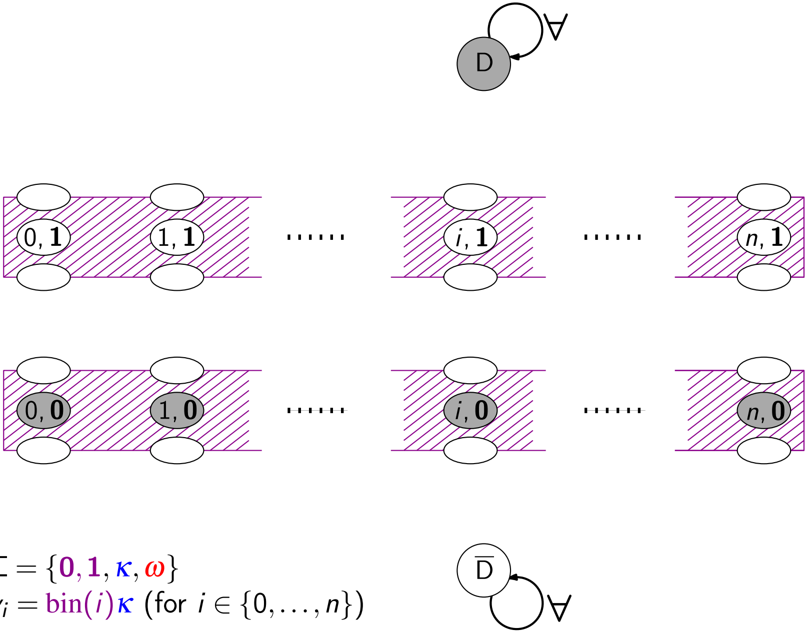
$\Sigma = \{0, 1, \ldots, n, \omega\}$



$$\Sigma = \{0, 1, \ldots, n, \omega\}$$

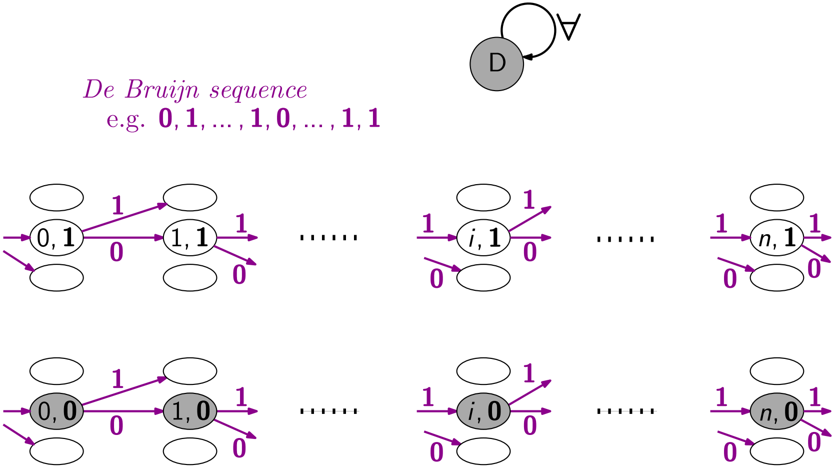


$$\Sigma = \{\mathbf{0}, \mathbf{1}, \kappa, \omega\}$$
$$v_i = \mathrm{bin}(i)\kappa \text{ (for } i \in \{0, \ldots, n\})$$

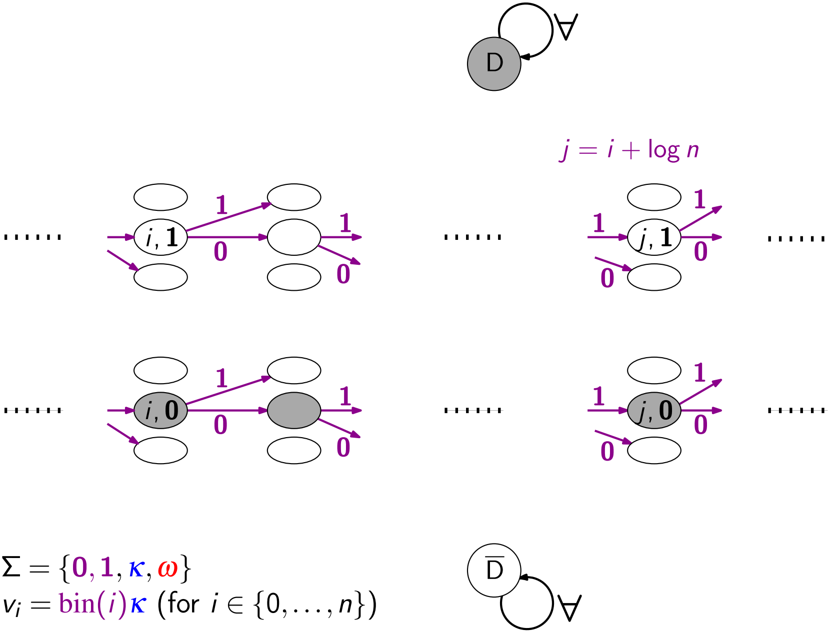


$\Sigma = \{\mathbf{0}, \mathbf{1}, \kappa, \omega\}$

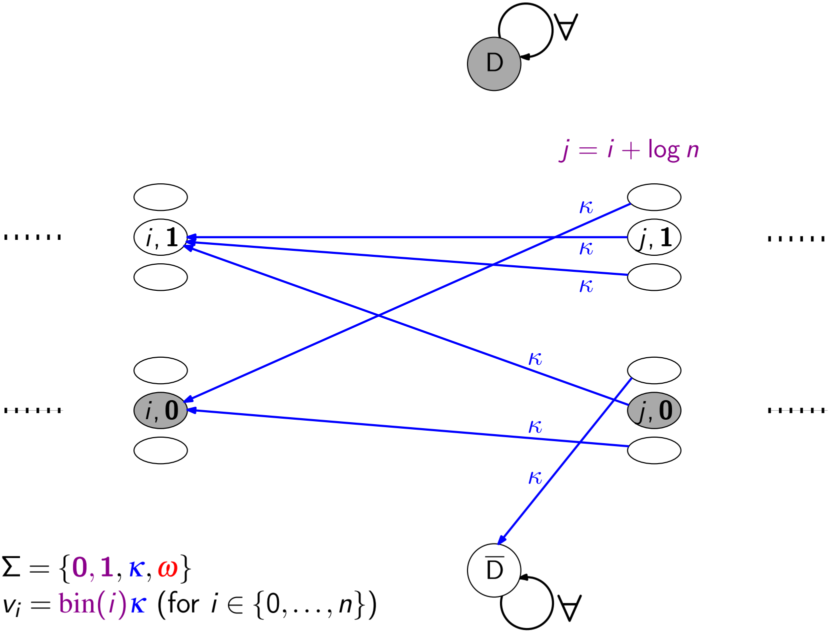
$v_i = \mathrm{bin}(i)\kappa$ (for $i \in \{0, \ldots, n\}$)



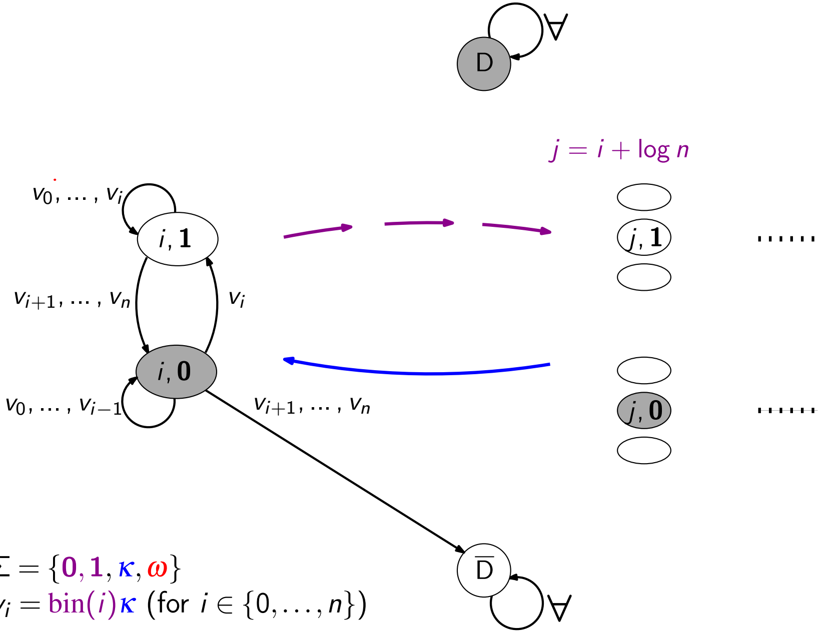
$\Sigma = \{\mathbf{0}, \mathbf{1}, \kappa, \omega\}$
$v_i = \mathrm{bin}(i)\kappa$ (for $i \in \{0, \ldots, n\}$)



$\Sigma = \{\mathbf{0}, \mathbf{1}, \kappa, \omega\}$
$v_i = \mathrm{bin}(i)\kappa$ (for $i \in \{0, \ldots, n\}$)



$\Sigma = \{\mathbf{0}, \mathbf{1}, \kappa, \omega\}$
$v_i = \mathrm{bin}(i)\kappa$ (for $i \in \{0, \ldots, n\}$)



$\Sigma = \{\mathbf{0}, \mathbf{1}, \kappa, \omega\}$

$v_i = \mathrm{bin}(i)\kappa$ (for $i \in \{0, \ldots, n\}$)

The Entire Construction

- DFA with 4-letter alphabets and subsets with exponential shortest r. w.
- A suitable method for making a DFA transitive.
- A suitable method for decreasing the alphabet size to 2.

The Entire Construction

- DFA with 4-letter alphabets and subsets with exponential shortest r. w.
- A suitable method for making a DFA transitive.
- A suitable method for decreasing the alphabet size to 2.

The Entire Construction

- DFA with 4-letter alphabets and subsets with exponential shortest r. w.
- A suitable method for making a DFA transitive.
- A suitable method for decreasing the alphabet size to 2.

Conclusion

- Some subsets require strongly exponential reset words even in transitive DFA with two-letter alphabets.
- Some transformations have strongly exponential depth even with respect to two generators.