Parametrized Asynchronous Shared-Memory Systems

Patricia Bouyer, Nicolas Markey, Arnaud Sangnier, Mickael Randour and Daniel STAN

GDT 30/03/2016

1. The model
2. (Non-)Deterministic Model Checking
3. Probabilistic case

1 The model
- Definitions
- Example

2 (Non-)Deterministic Model Checking

3 Probabilistic case

Definition (Distributed protocol)

A distributed protocol is given by $\mathcal{P} = \langle Q, D, T \rangle$

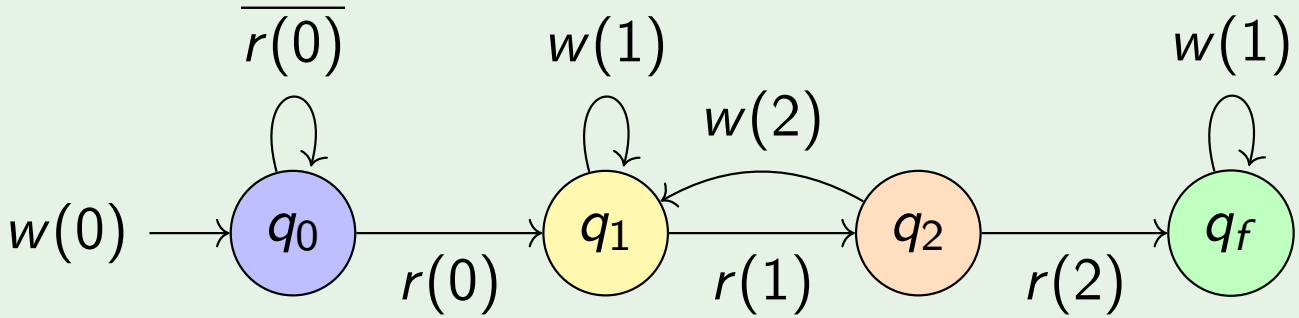
- Q: control states
- D: possible values of the register
- T: transitions of the form $p \xrightarrow{r(d)} q$ and $p \xrightarrow{w(d)} q$ for $p, q \in Q$, $d \in D$.

Definition (Distributed protocol)

A distributed protocol is given by $\mathcal{P} = \langle Q, D, T \rangle$

- Q: control states
- D: possible values of the register
- T: transitions of the form $p \xrightarrow{r(d)} q$ and $p \xrightarrow{w(d)} q$ for $p, q \in Q$, $d \in D$.

Example



Definition (Configuration of the protocol)

$$\gamma = \langle f, d \rangle$$

with $f : Q \to \mathbb{N}$ (multiset) and $d \in D$ the register value. We write $\gamma(q) = f(q)$ and $v(\gamma) = d$.

Definition (Configuration of the protocol)

$$\gamma = \langle f, d \rangle$$

with $f : Q \to \mathbb{N}$ (multiset) and $d \in D$ the register value. We write $\gamma(q) = f(q)$ and $v(\gamma) = d$.

Some notations:

- Γ is the set of configurations
- $|\gamma| = \sum_q \gamma(q)$ (size)
- $\overline{S}(\gamma) = (\{q \mid \gamma(q) > 0\}, v(\gamma))$
- $\mathrm{Pre}(X)$, $\mathrm{Post}(X)$
- $+$, $-$ operations on multisets are extended to configurations.

Definition (Configuration of the protocol)

$$\gamma = \langle f, d \rangle$$

with $f : Q \to \mathbb{N}$ (multiset) and $d \in D$ the register value. We write $\gamma(q) = f(q)$ and $v(\gamma) = d$.

Some notations:

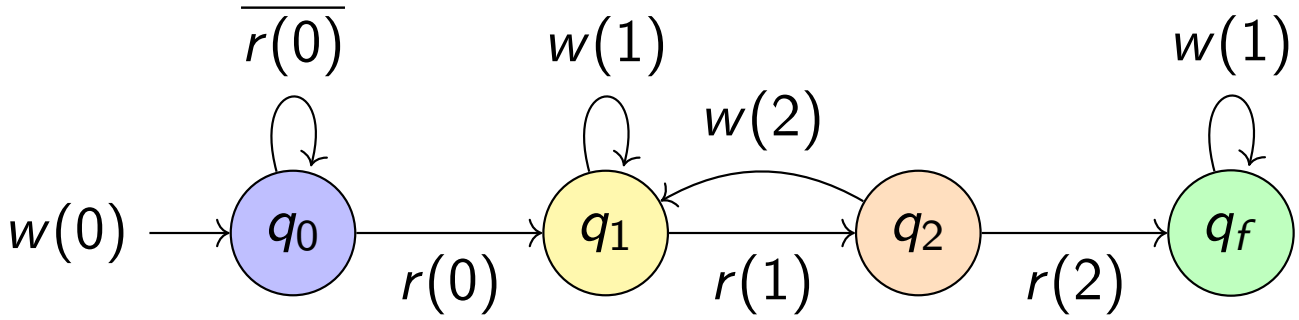
- Γ is the set of configurations
- $|\gamma| = \sum_q \gamma(q)$ (size)
- $\overline{S}(\gamma) = (\{q \mid \gamma(q) > 0\}, v(\gamma))$
- $\mathrm{Pre}(X)$, $\mathrm{Post}(X)$
- $+$, $-$ operations on multisets are extended to configurations.

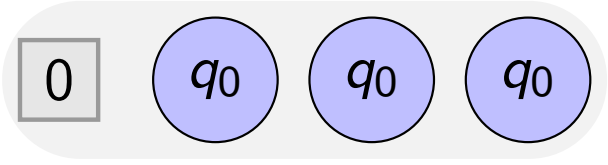
Definition (Semantics)

$\gamma \to \gamma'$ if $\gamma' = \gamma - q + q'$ with either

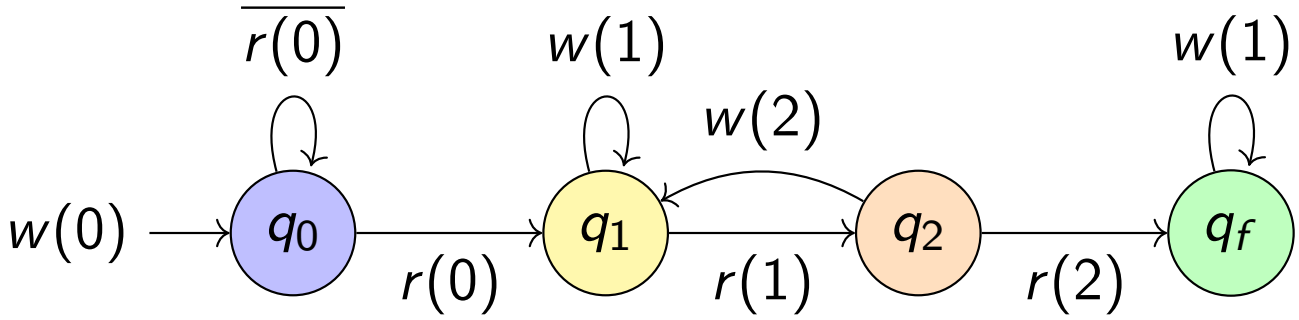
- $q \xrightarrow{w(v(\gamma))} q'$ (write operation)
- or $d = v(\gamma) = v(\gamma')$ and $q \xrightarrow{r(d)} q'$ (read operation)

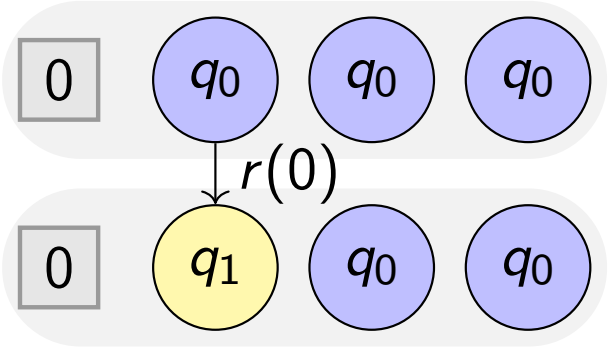
Semantics



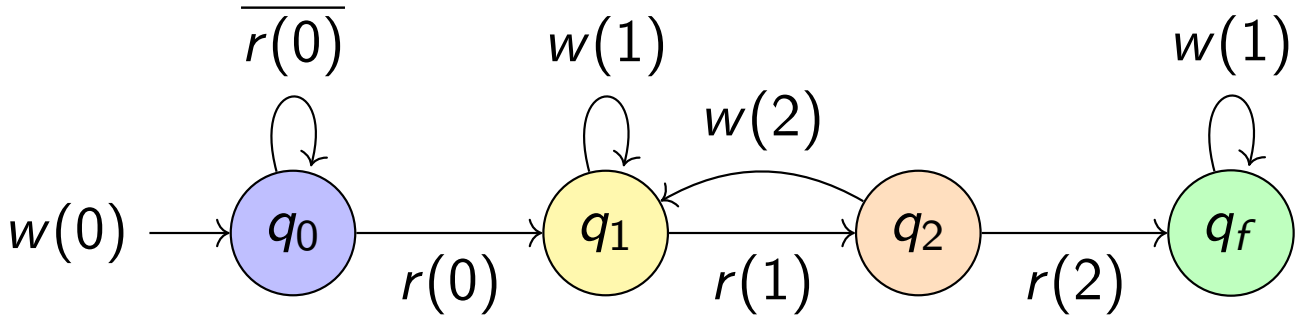


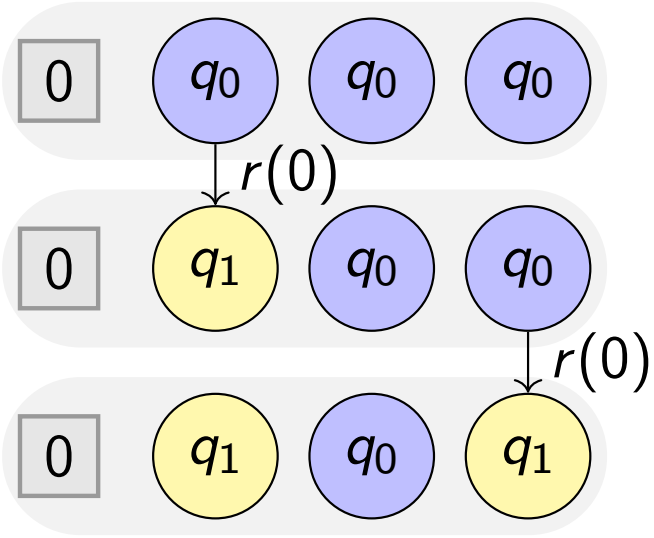
Semantics



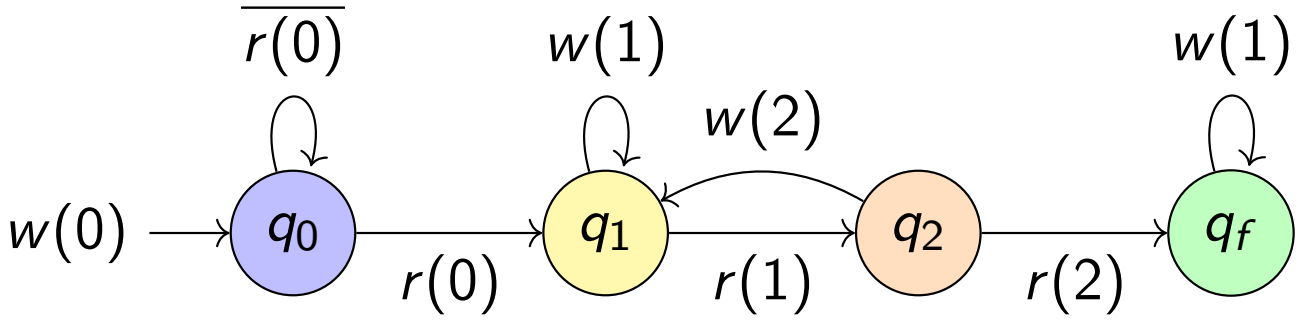


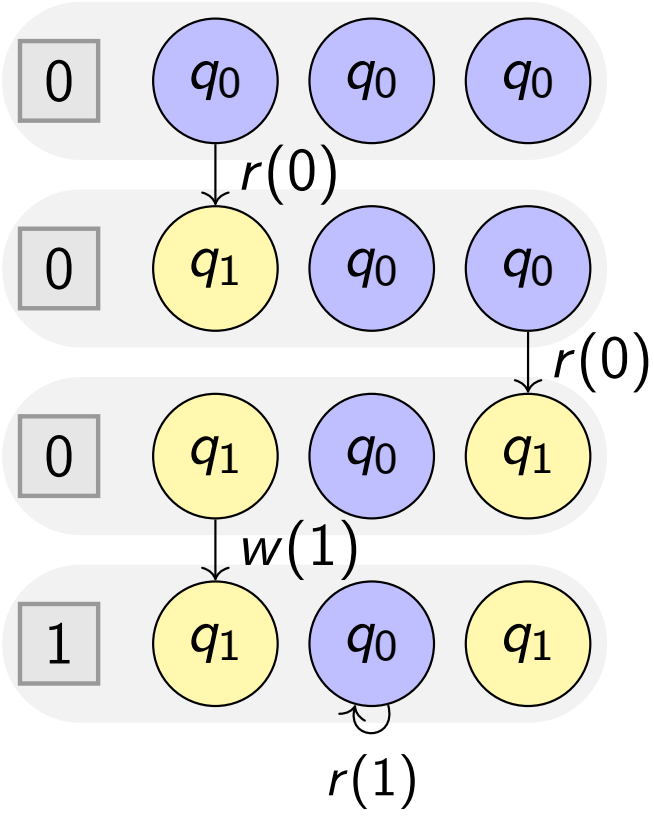
Semantics


$\overline{r(0)}$
$w(1)$
$w(1)$
$w(2)$
$w(0)$
q_0
q_1
q_2
q_f
$r(0)$
$r(1)$
$r(2)$

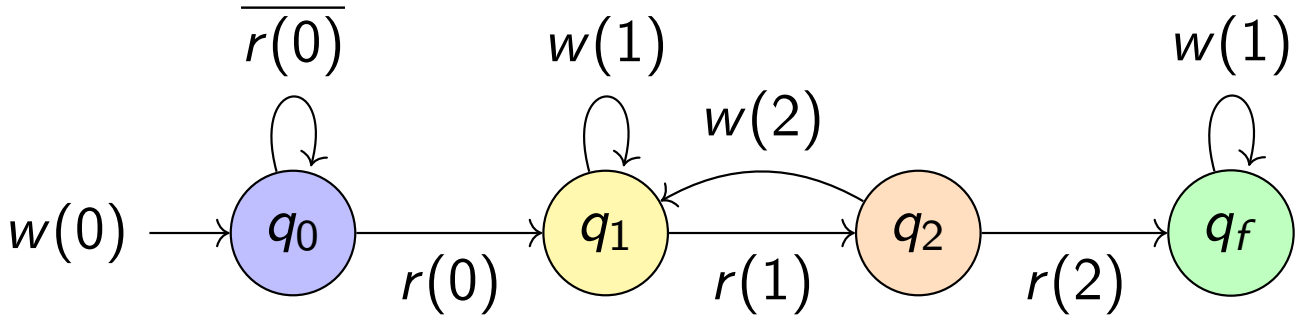

0
q_0
q_0
q_0
$r(0)$
0
q_1
q_0
q_0
$r(0)$
0
q_1
q_0
q_1

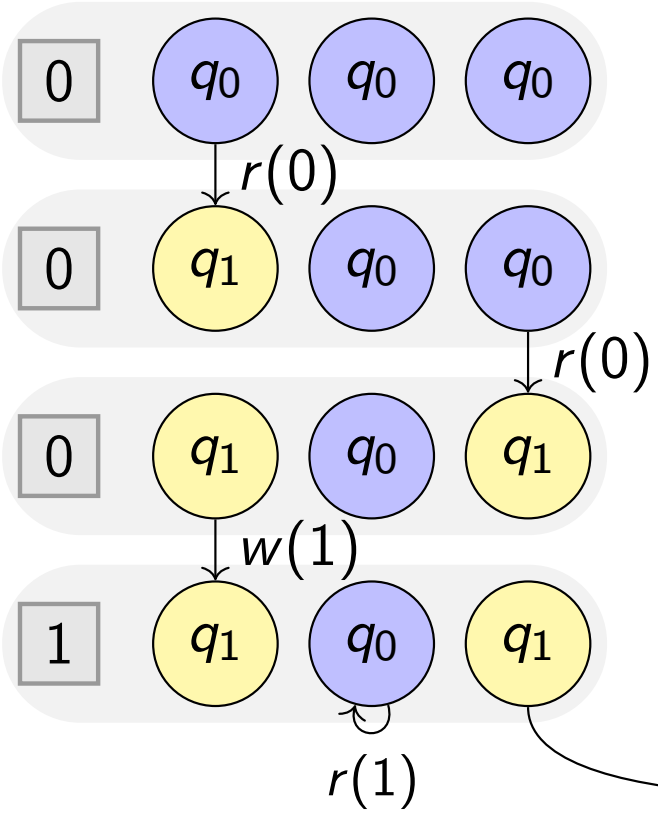
Semantics

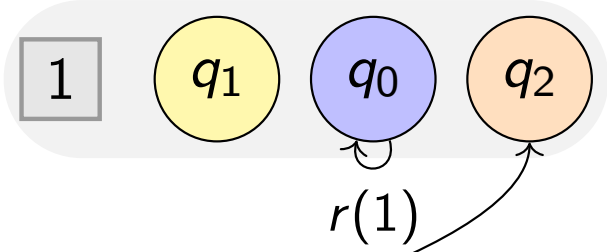

$\overline{r(0)}$
$w(1)$
$w(1)$
$w(2)$
$w(0)$
q_0
q_1
q_2
q_f
$r(0)$
$r(1)$
$r(2)$

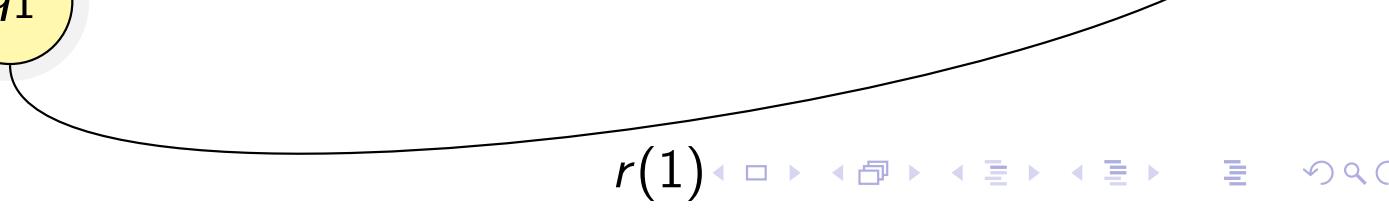

0
q_0 q_0 q_0
$r(0)$
0
q_1 q_0 q_0
$r(0)$
0
q_1 q_0 q_1
$w(1)$
1
q_1 q_0 q_1
$r(1)$

Semantics

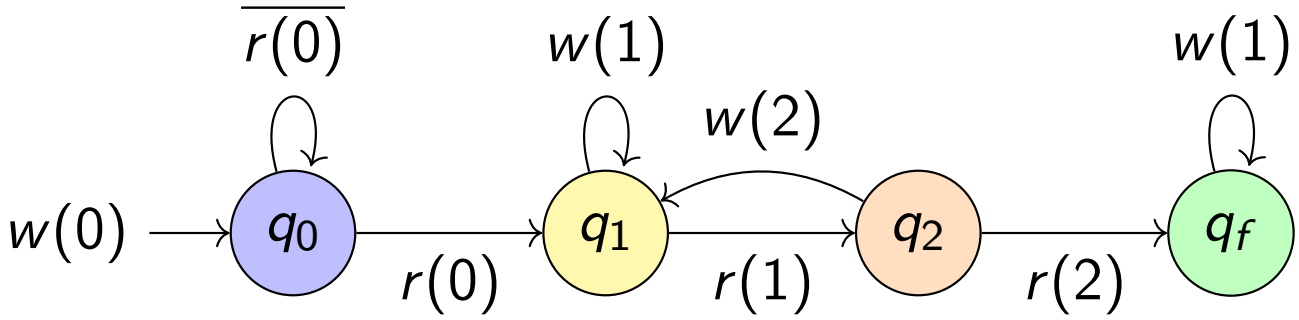

$\overline{r(0)}$
$w(1)$
$w(2)$
$w(1)$
$w(0)$
q_0
q_1
q_2
q_f
$r(0)$
$r(1)$
$r(2)$

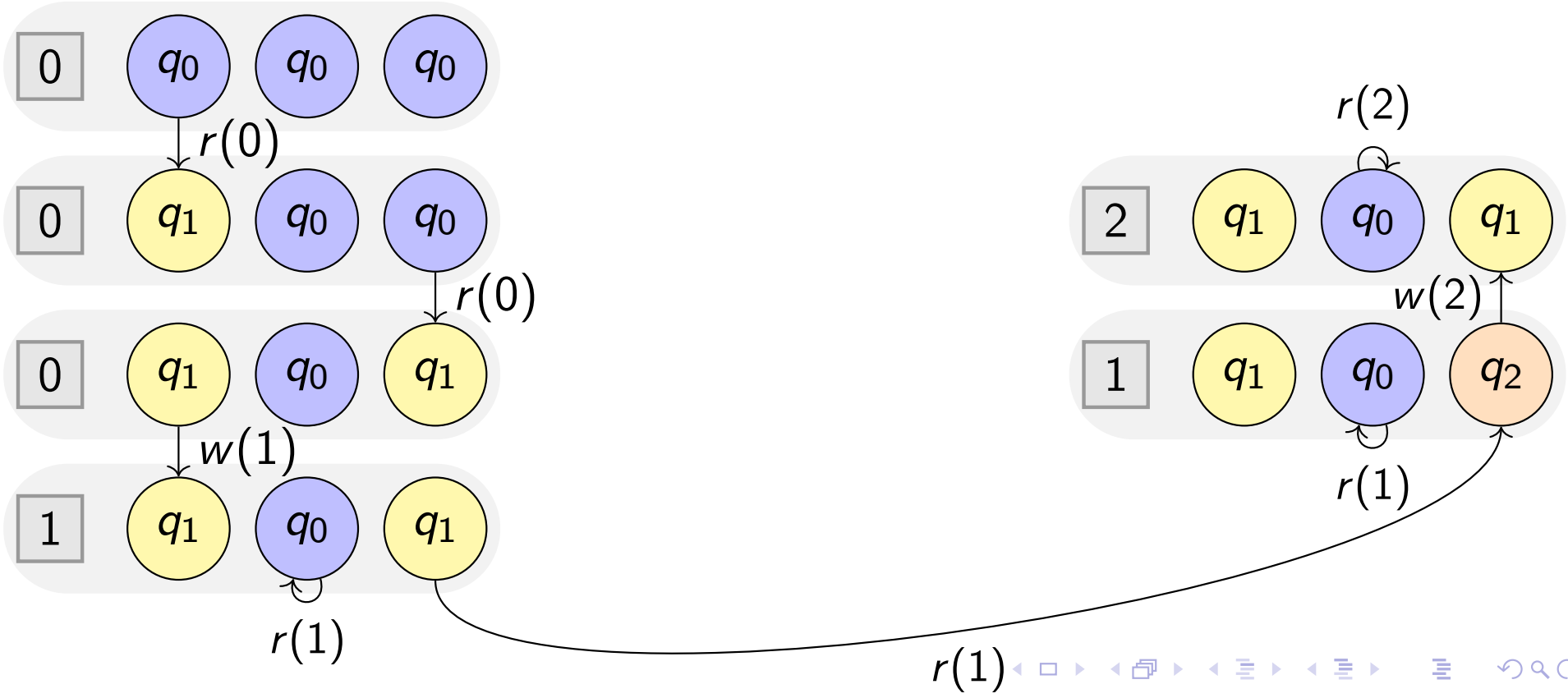

0
q_0 q_0 q_0
$r(0)$
0
q_1 q_0 q_0
$r(0)$
0
q_1 q_0 q_1
$w(1)$
1
q_1 q_0 q_1
$r(1)$


1
q_1 q_0 q_2
$r(1)$

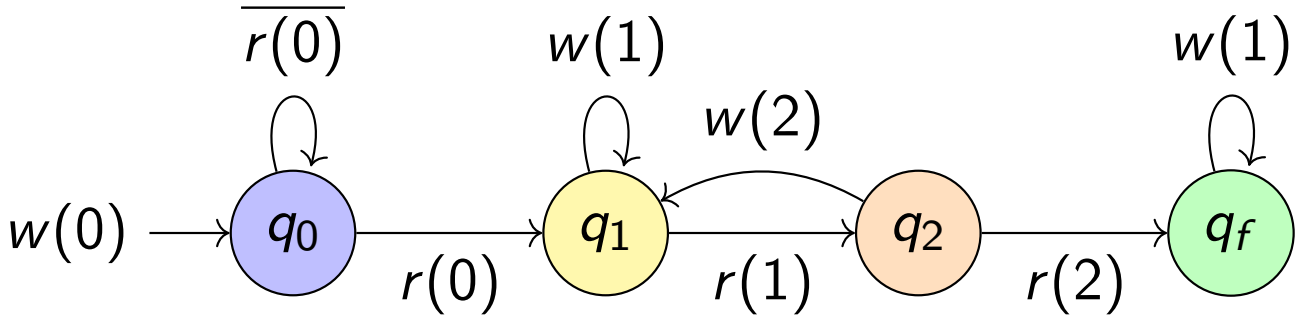

$r(1)$

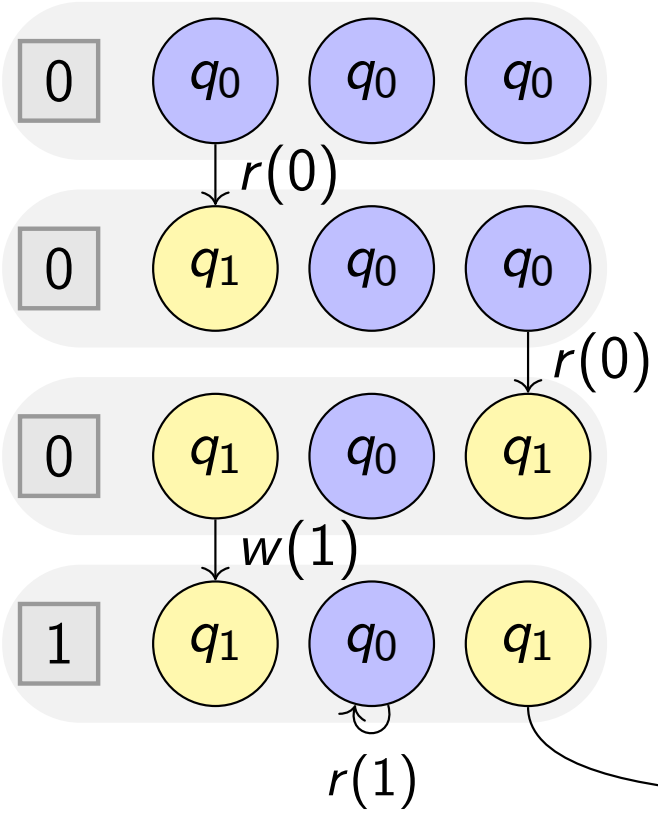
Semantics

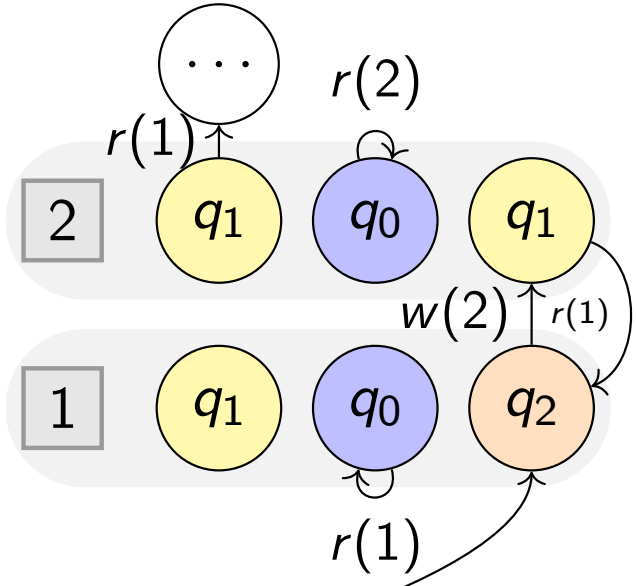

$\overline{r(0)}$
$w(1)$
$w(1)$
$w(2)$
$w(0)$
q_0
q_1
q_2
q_f
$r(0)$
$r(1)$
$r(2)$

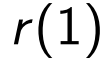

0
q_0 q_0 q_0
$r(0)$
0
q_1 q_0 q_0
$r(0)$
0
q_1 q_0 q_1
$w(1)$
1
q_1 q_0 q_1
$r(1)$
$r(1)$
$r(2)$
2
q_1 q_0 q_1
$w(2)$
1
q_1 q_0 q_2
$r(1)$

Semantics

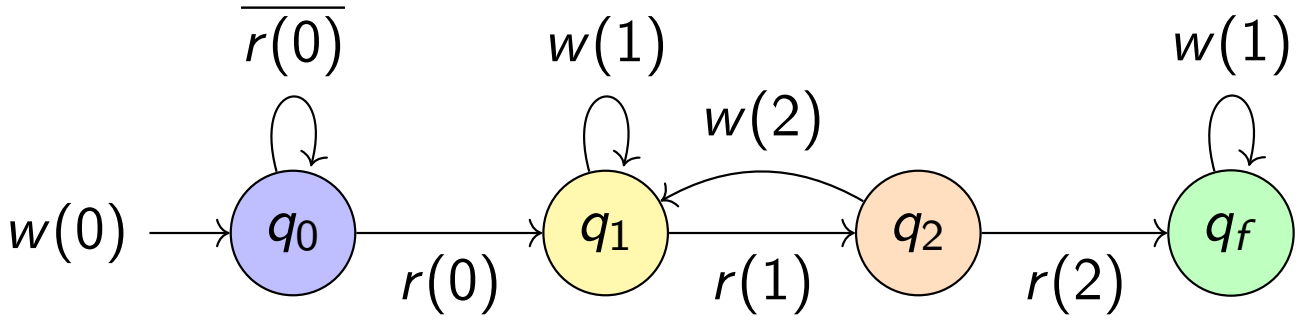

$\overline{r(0)}$
$w(1)$
$w(2)$
$w(1)$
$w(0)$
q_0
q_1
q_2
q_f
$r(0)$
$r(1)$
$r(2)$

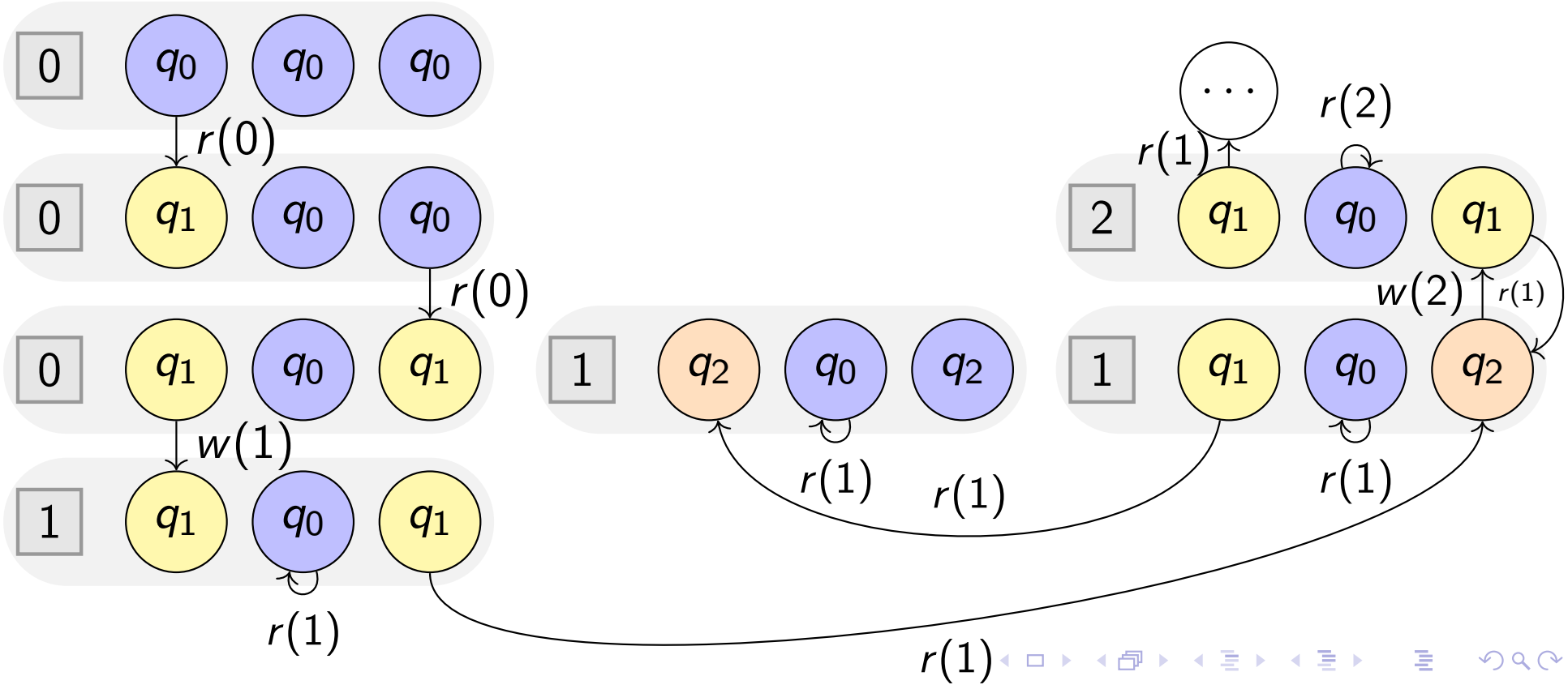

0
q_0 q_0 q_0
$r(0)$
0
q_1 q_0 q_0
$r(0)$
0
q_1 q_0 q_1
$w(1)$
1
q_1 q_0 q_1
$r(1)$


$\cdots$
$r(2)$
$r(1)$
2
q_1 q_0 q_1
$w(2)$
$r(1)$
1
q_1 q_0 q_2
$r(1)$

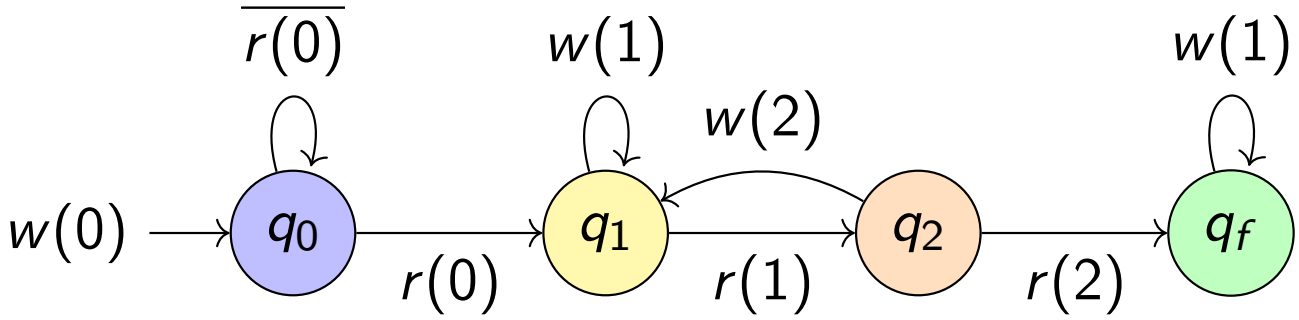

$r(1)$

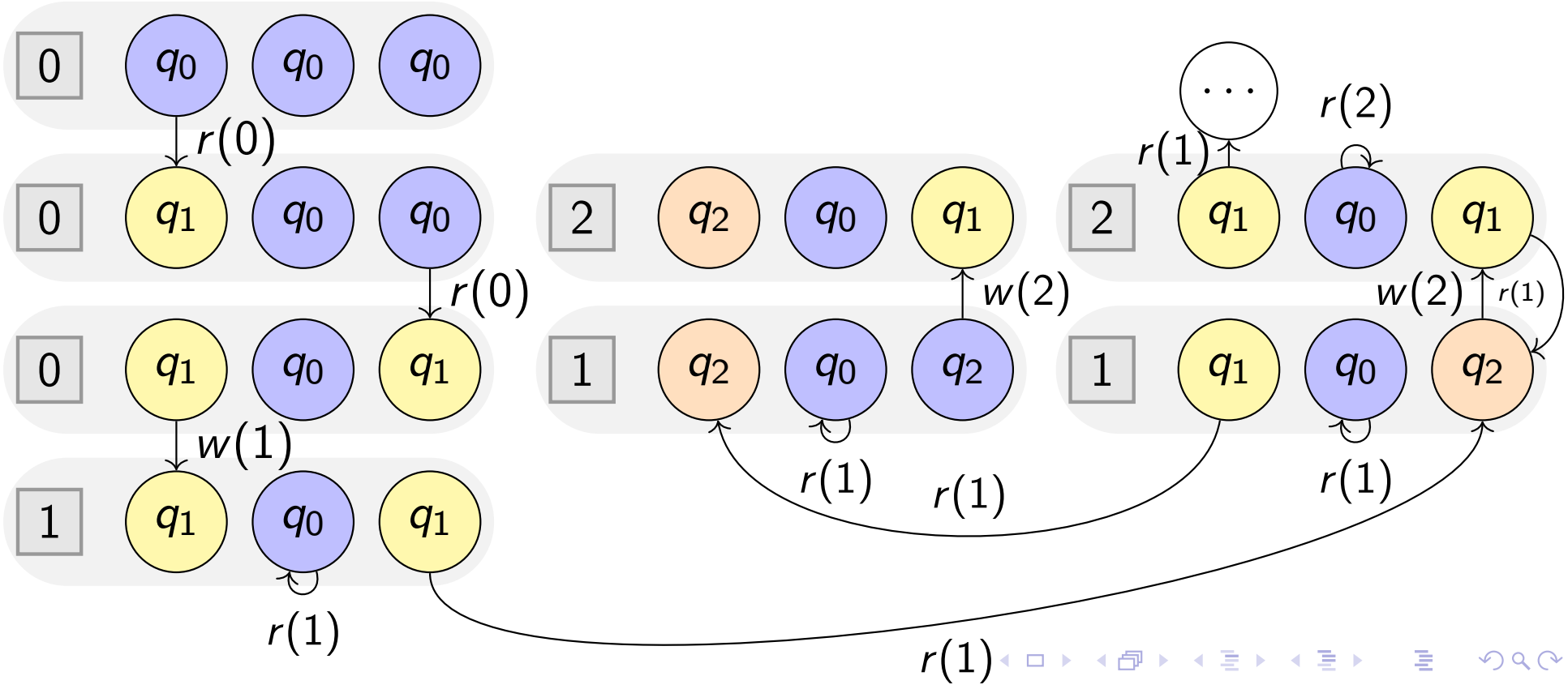
Semantics


$\overline{r(0)}$
$w(1)$
$w(2)$
$w(1)$
$w(0)$
q_0
q_1
q_2
q_f
$r(0)$
$r(1)$
$r(2)$

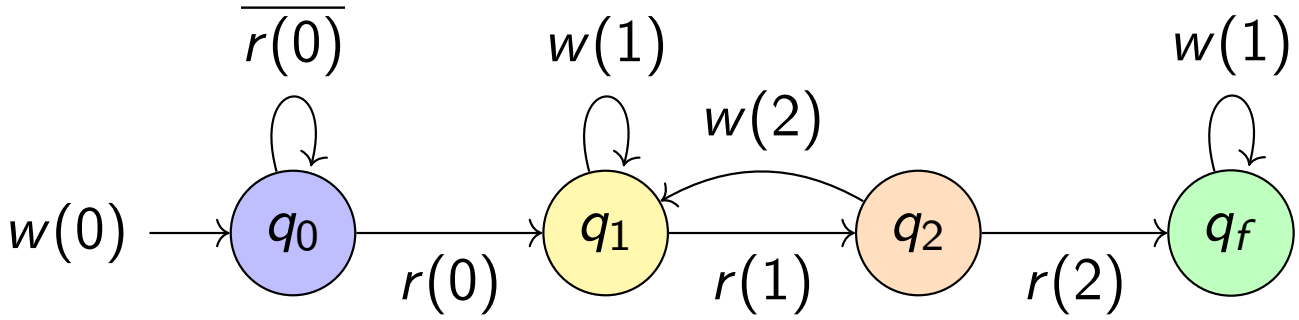

0
q_0 q_0 q_0
$r(0)$
0
q_1 q_0 q_0
$r(0)$
0
q_1 q_0 q_1
$w(1)$
1
q_1 q_0 q_1
$r(1)$
1
q_2 q_0 q_2
$r(1)$ $r(1)$
$r(1)$
2
q_1 q_0 q_1
$r(2)$
$w(2)$ $r(1)$
1
q_1 q_0 q_2
$r(1)$
$r(1)$

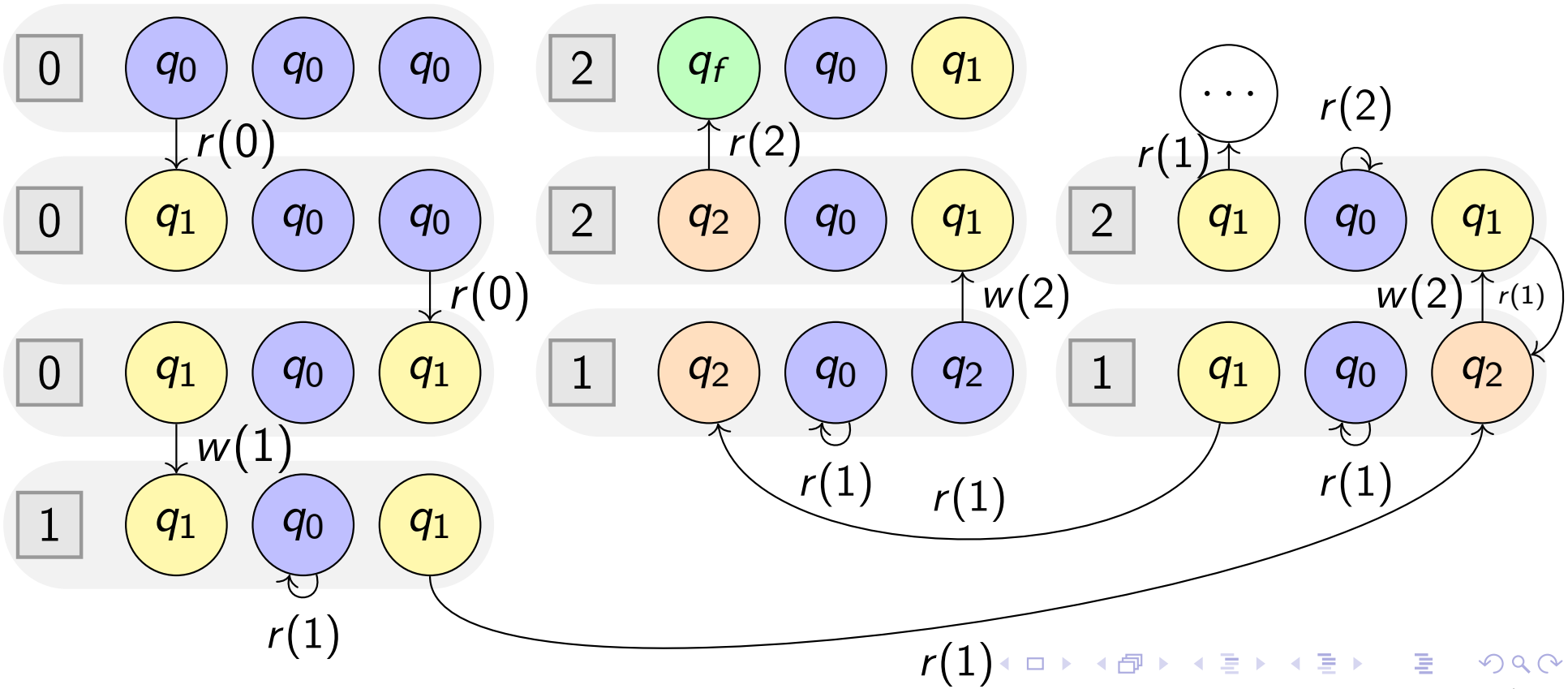
Semantics


$\overline{r(0)}$
$w(1)$
$w(2)$
$w(1)$
$w(0)$
q_0
q_1
q_2
q_f
$r(0)$
$r(1)$
$r(2)$


0
q_0 q_0 q_0
$r(0)$
0
q_1 q_0 q_0
$r(0)$
0
q_1 q_0 q_1
$w(1)$
1
q_1 q_0 q_1
$r(1)$
2
q_2 q_0 q_1
$w(2)$
1
q_2 q_0 q_2
$r(1)$ $r(1)$
$\cdots$
$r(1)$
$r(2)$
2
q_1 q_0 q_1
$w(2)$ $r(1)$
1
q_1 q_0 q_2
$r(1)$
$r(1)$

Semantics


$\overline{r(0)}$
$w(1)$
$w(2)$
$w(1)$
$w(0)$
q_0
q_1
q_2
q_f
$r(0)$
$r(1)$
$r(2)$


0
q_0 q_0 q_0
$r(0)$
0
q_1 q_0 q_0
$r(0)$
0
q_1 q_0 q_1
$w(1)$
1
q_1 q_0 q_1
$r(1)$
2
q_f q_0 q_1
$r(2)$
2
q_2 q_0 q_1
$w(2)$
1
q_2 q_0 q_2
$r(1)$ $r(1)$
$r(1)$
$\cdots$
$r(2)$
2
q_1 q_0 q_1
$w(2)$ $r(1)$
1
q_1 q_0 q_2
$r(1)$
$r(1)$

1 The model

2 (Non-)Deterministic Model Checking
- Symbolic graph
- Reconstructing the symbols
- Conclusion

3 Probabilistic case

Definition (Reachability problem)

Let $(q_0, d_0) \in Q \times D$ and some target $q_f \in Q$. Does there exist $\gamma \in \Gamma$ with $\gamma(q_f) > 0$ reachable from $(q_0^{|\gamma|}, d_0)$?

Definition (Reachability problem with leader)

Let $(q_0, d_0) \in Q \times D$, $q_l \in Q$ and some target $q_f \in Q$. Does there exist $\gamma \in \Gamma$ with $\gamma(q_f) > 0$ reachable from $(q_l + q_0^{|\gamma|}, d_0)$?

- Once γ is fixed, the number of processes in the run is fixed.
- Monotonicity : if q_f is reachable with n processes, still reachable with a bigger number of processes.
- Bound of the maximal parameter value to consider ?

Symbolic graph

In the following, we consider the leader-less case.

Definition (Symbolic graph)

$G_{\text{symb}} = (S, E)$ with

- $S = 2^Q \times D$
- E is defined by $(X_1, d_1) \to (X_2, d_2)$ if there exists $x_1 \in X_1$, $x_2 \in X_2$ such that

$$X_1 \backslash \{x_1, x_2\} = X_2 \backslash \{x_1, x_2\} \tag{1}$$

$$x_1 \xrightarrow{w(d_2)} x_2 \vee \left(x_1 \xrightarrow{r(d_2)} x_2 \wedge d_1 = d_2 \right) \tag{2}$$

Symbolic graph

In the following, we consider the leader-less case.

Definition (Symbolic graph)

$G_{\text{symb}} = (S, E)$ with

- $S = 2^Q \times D$
- E is defined by $(X_1, d_1) \to (X_2, d_2)$ if there exists $x_1 \in X_1$, $x_2 \in X_2$ such that

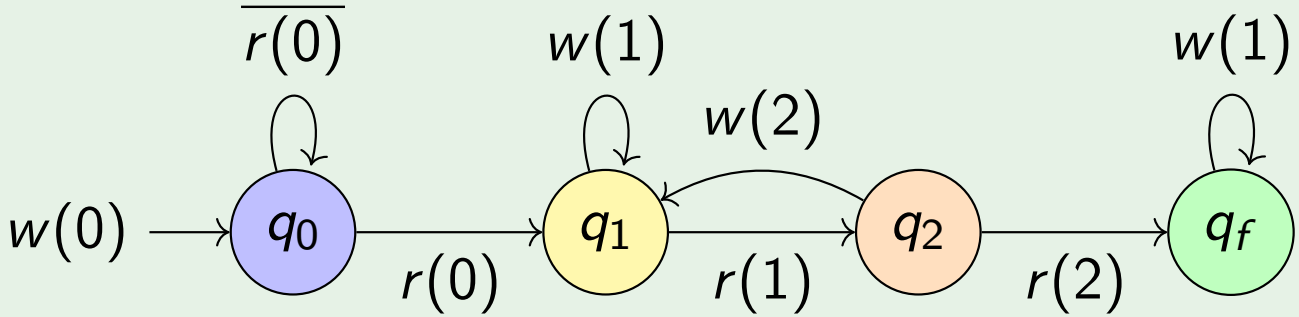
$$X_1 \backslash \{x_1, x_2\} = X_2 \backslash \{x_1, x_2\} \tag{1}$$

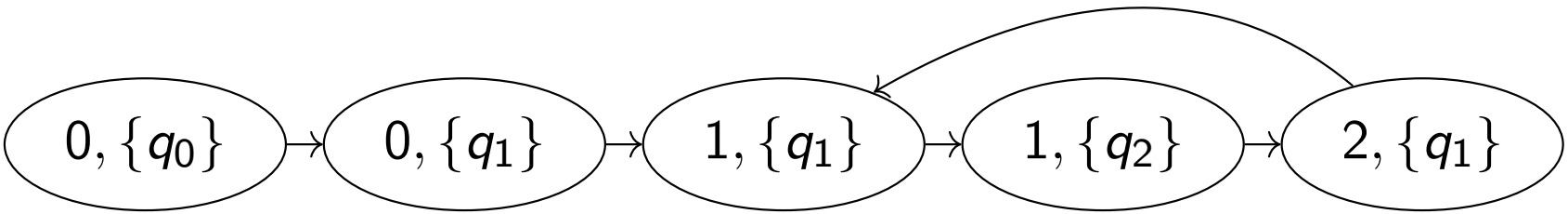
$$x_1 \xrightarrow{w(d_2)} x_2 \vee \left(x_1 \xrightarrow{r(d_2)} x_2 \wedge d_1 = d_2 \right) \tag{2}$$

Lemma

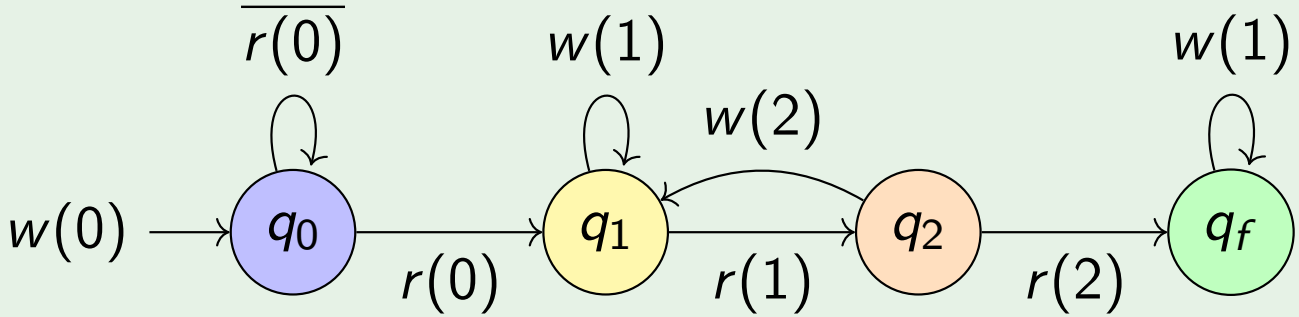
Every "concrete" run of $\mathcal{P}$ corresponds to a symbolic run. $\overline{S}(\cdot)$ can be seen as an abstraction.

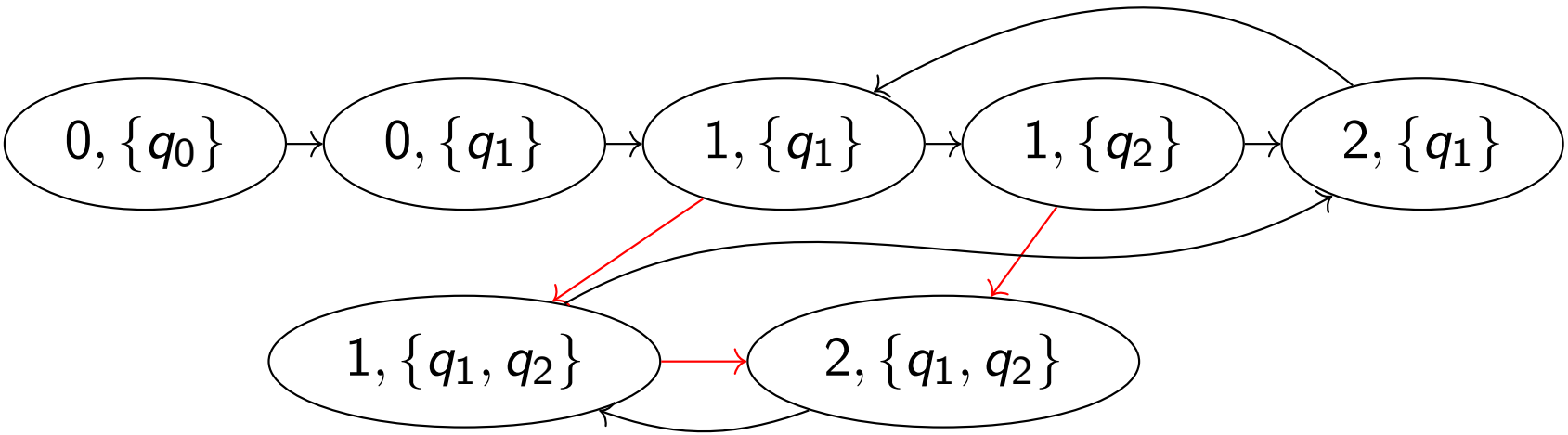
Example



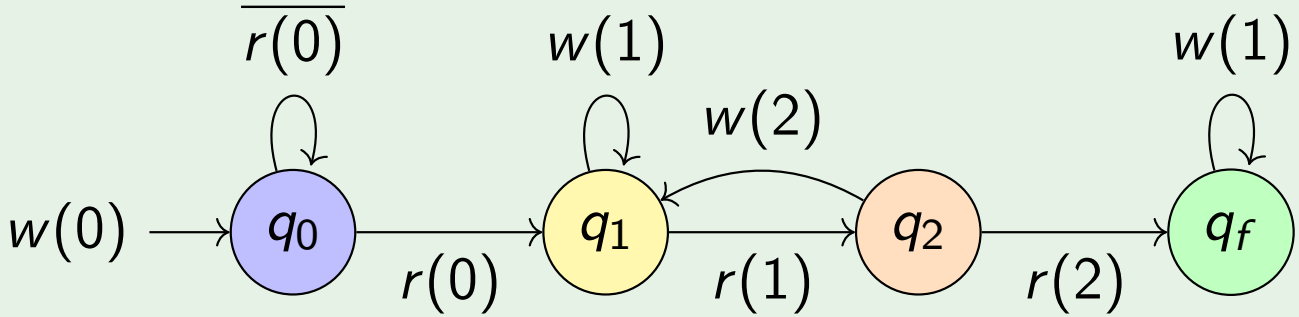


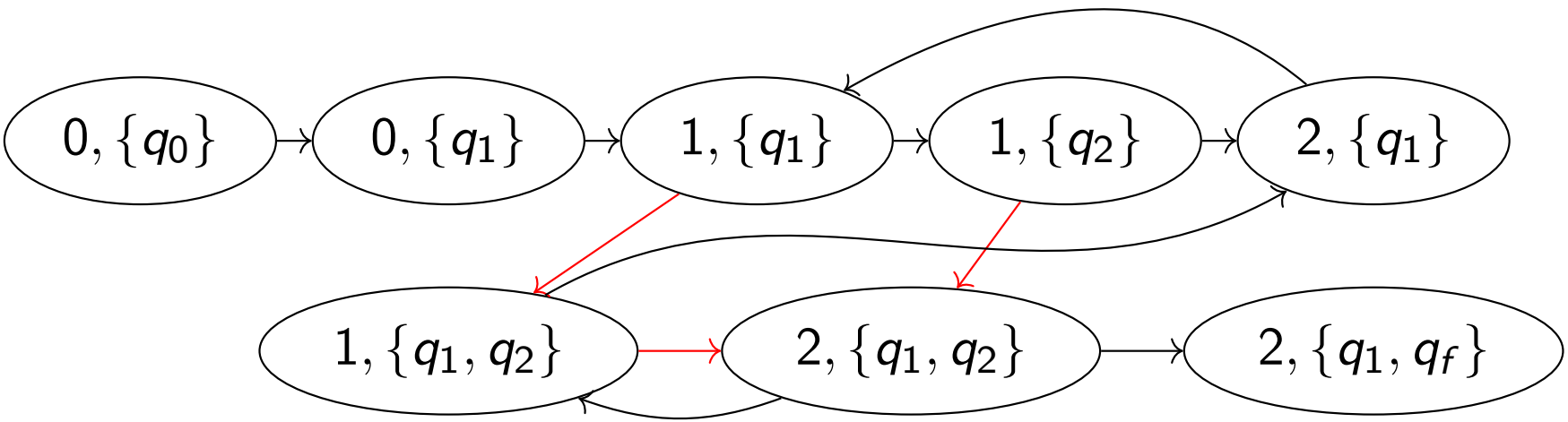
Example


$\overline{r(0)}$
$w(1)$
$w(2)$
$w(1)$
$w(0)$
q_0
q_1
q_2
q_f
$r(0)$
$r(1)$
$r(2)$

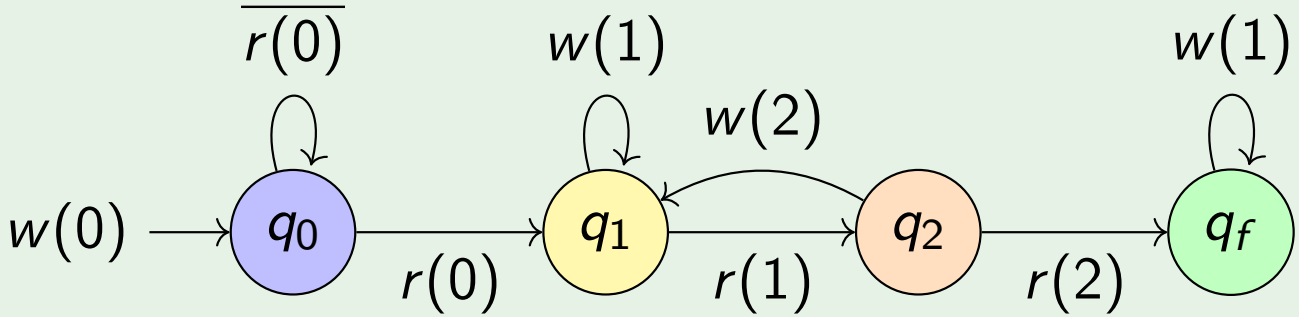

$0, \{q_0\}$
$0, \{q_1\}$
$1, \{q_1\}$
$1, \{q_2\}$
$2, \{q_1\}$
$1, \{q_1, q_2\}$
$2, \{q_1, q_2\}$

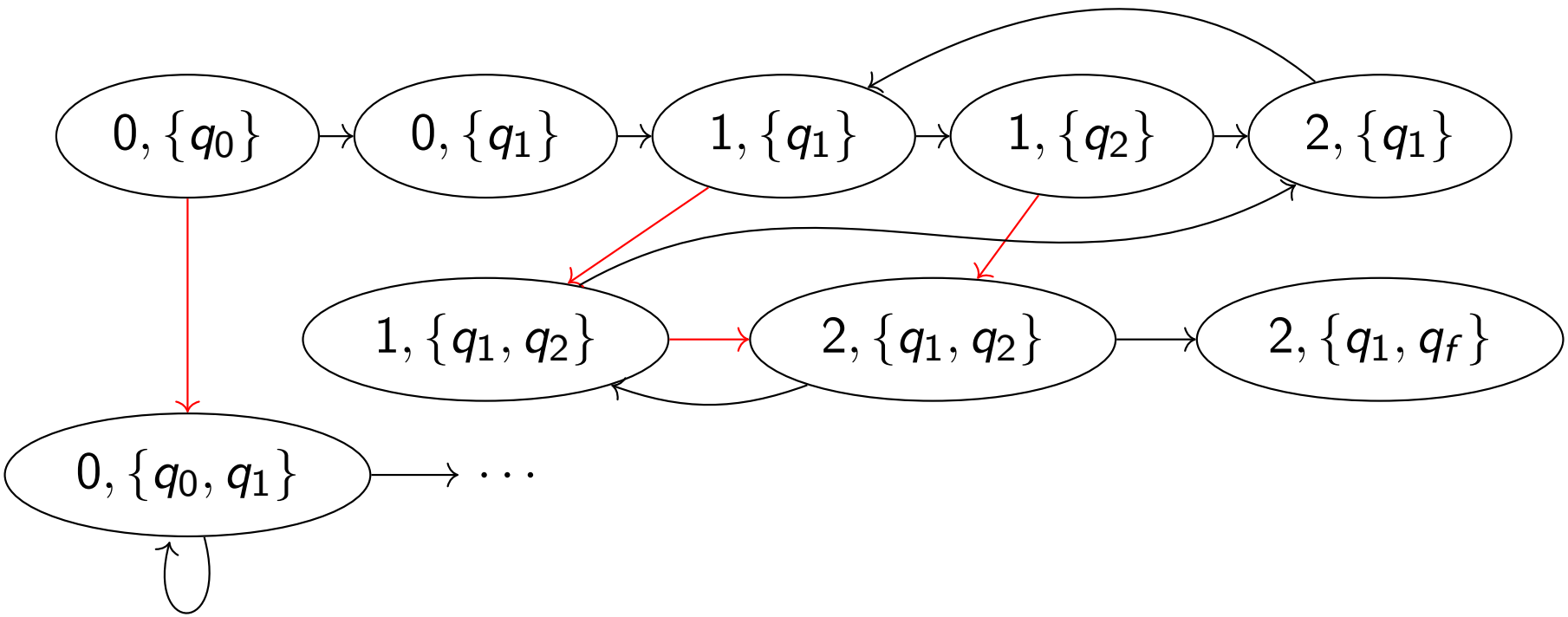
Example


$\overline{r(0)}$
$w(1)$
$w(2)$
$w(1)$
$w(0)$
q_0
q_1
q_2
q_f
$r(0)$
$r(1)$
$r(2)$

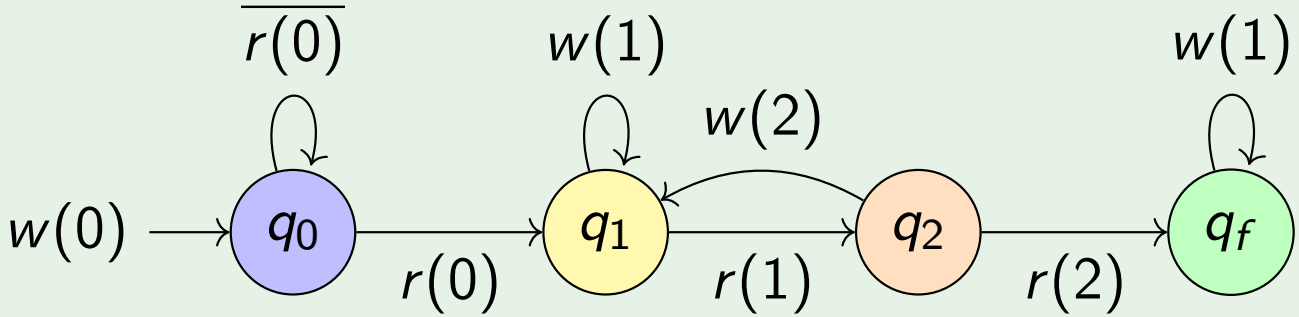

$0, \{q_0\}$
$0, \{q_1\}$
$1, \{q_1\}$
$1, \{q_2\}$
$2, \{q_1\}$
$1, \{q_1, q_2\}$
$2, \{q_1, q_2\}$
$2, \{q_1, q_f\}$

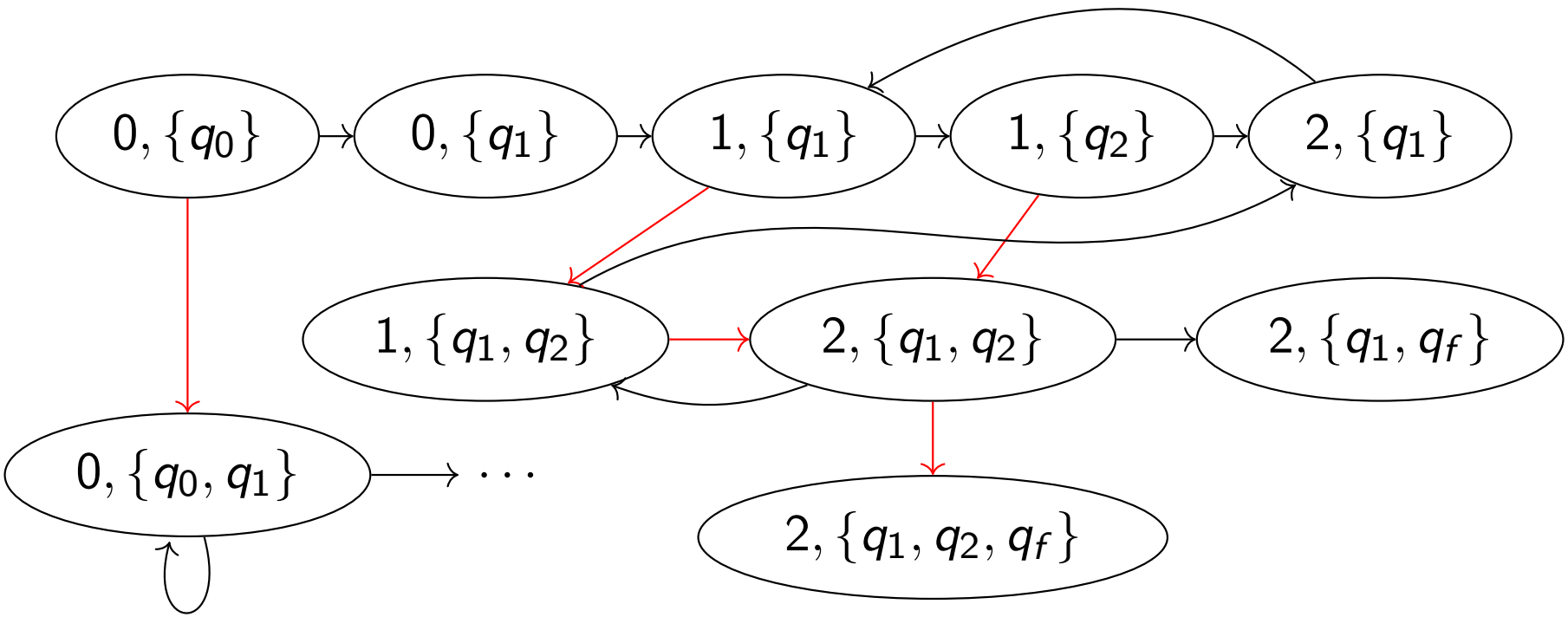
Example


$\overline{r(0)}$
$w(1)$
$w(2)$
$w(1)$
$w(0)$
q_0
q_1
q_2
q_f
$r(0)$
$r(1)$
$r(2)$


$0, \{q_0\}$
$0, \{q_1\}$
$1, \{q_1\}$
$1, \{q_2\}$
$2, \{q_1\}$
$1, \{q_1, q_2\}$
$2, \{q_1, q_2\}$
$2, \{q_1, q_f\}$
$0, \{q_0, q_1\}$
$\cdots$

Example


$\overline{r(0)}$
$w(1)$
$w(1)$
$w(2)$
$w(0)$
q_0
q_1
q_2
q_f
$r(0)$
$r(1)$
$r(2)$


$0, \{q_0\}$
$0, \{q_1\}$
$1, \{q_1\}$
$1, \{q_2\}$
$2, \{q_1\}$
$1, \{q_1, q_2\}$
$2, \{q_1, q_2\}$
$2, \{q_1, q_f\}$
$0, \{q_0, q_1\}$
$\cdots$
$2, \{q_1, q_2, q_f\}$

Reconstructing the run

Lemma

If $(X, d) \rightarrow^{L} (Y, e)$ *in* G_{symb}*, then there exists a concrete run* $\gamma \rightarrow^{*} \gamma'$ *with*

- $\overline{S}(\gamma) = X$
- $\overline{S}(\gamma') = Y$
- $|\gamma| = |\gamma'| \leq L$

Reconstructing the run

Lemma

If $(X, d) \rightarrow^{L} (Y, e)$ *in* G_{symb}*, then there exists a concrete run* $\gamma \rightarrow^{*} \gamma'$ *with*

- $\overline{S}(\gamma) = X$
- $\overline{S}(\gamma') = Y$
- $|\gamma| = |\gamma'| \leq L$

Sketch.

Every red transition in the symbolic graph implies a copy of the current involved state. □

Reducing a symbolic path

$$X_1, d_1 \longrightarrow X_k, d_k$$

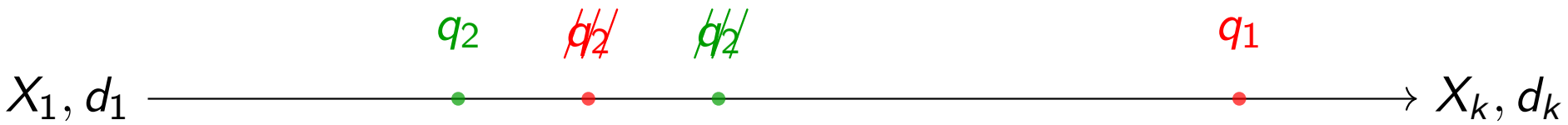
Reducing a symbolic path

Reducing a symbolic path

Reducing a symbolic path

Reducing a symbolic path

Reducing a symbolic path

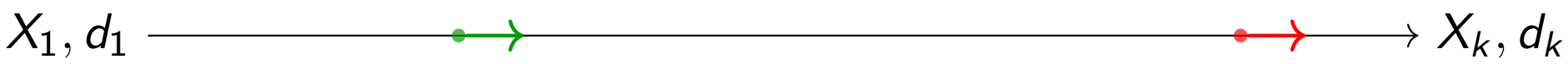


Reducing a symbolic path

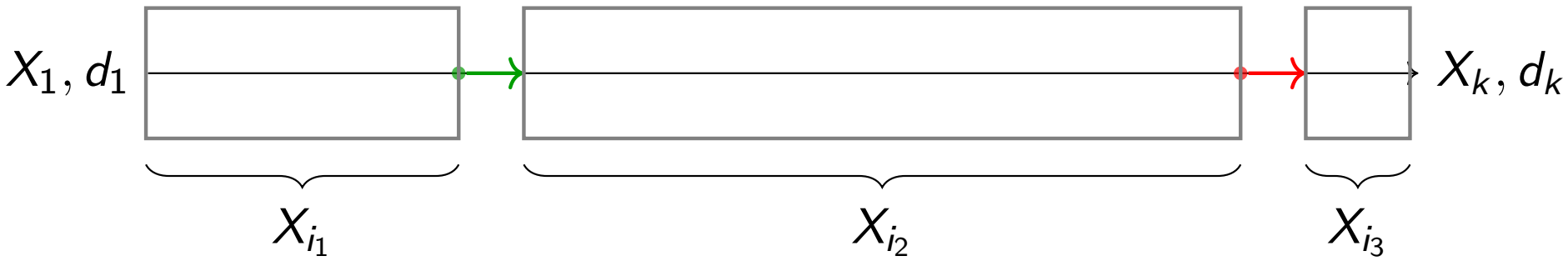
Without loss of generality

For each $q \in Q$, there is at most two transitions making q appearing or disappearing (one each).

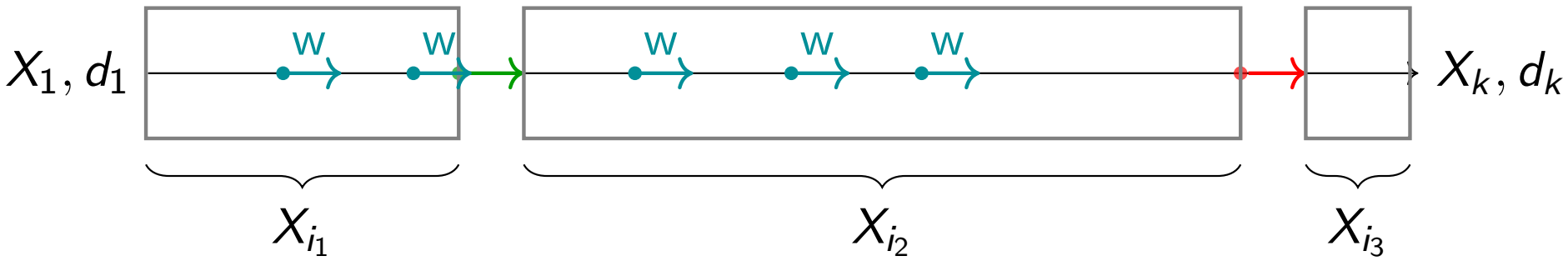
Fixed support behaviour



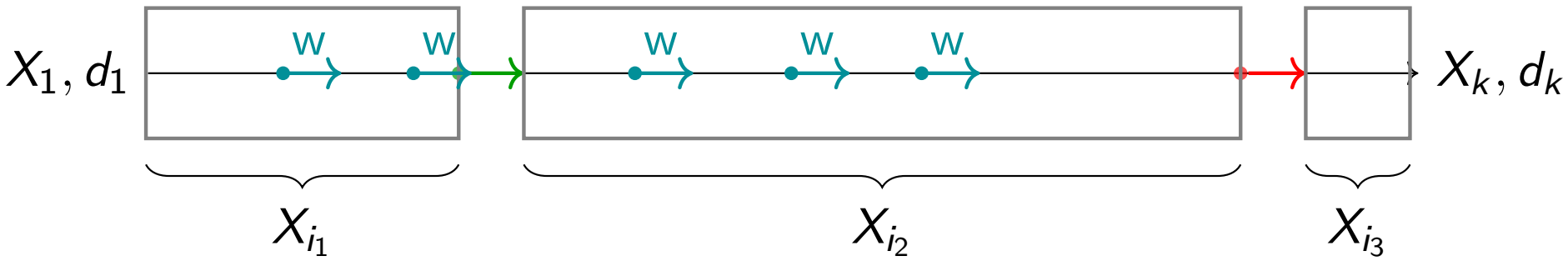
Fixed support behaviour



Fixed support behaviour



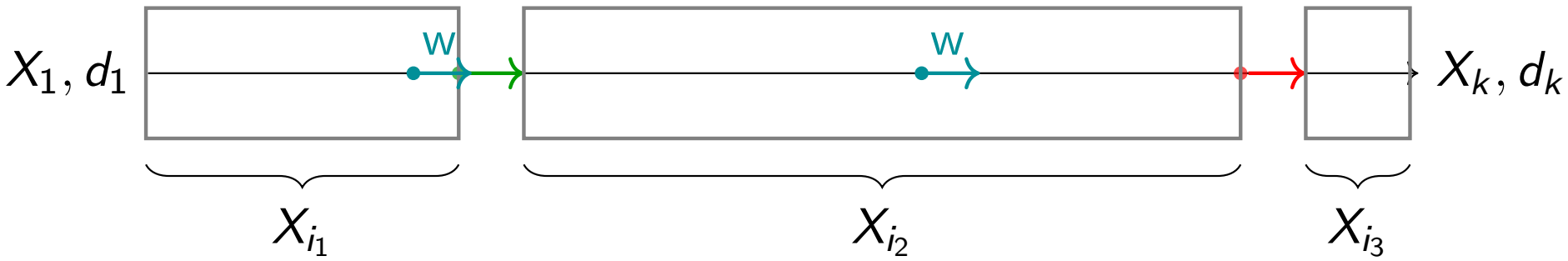
Fixed support behaviour



Key Idea

Only the last write transition is required.

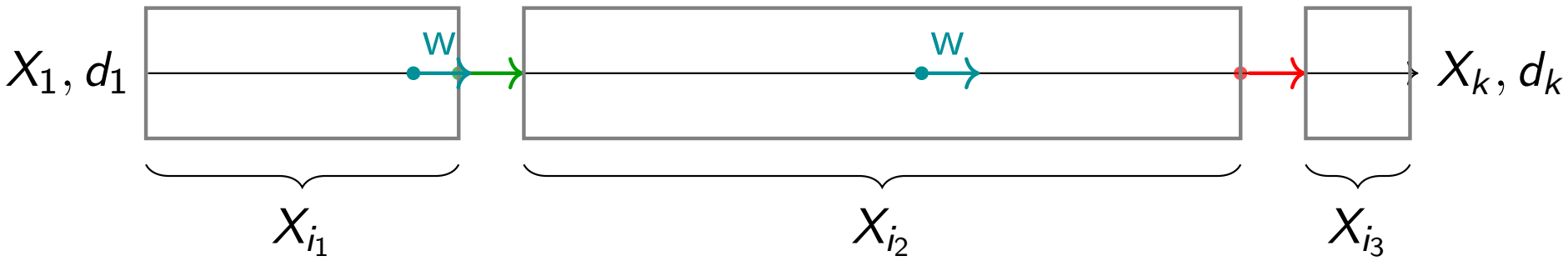
Fixed support behaviour



Key Idea

Only the last write transition is required.

Fixed support behaviour



Key Idea

Only the last write transition is required.

Theorem

Every path in G_{symb} *has less than* $4|Q| + 1$ *transitions.*

What the symbolic graph taught us

Theorem

If $\gamma \rightarrow^* \gamma'$ there exists $\eta \rightarrow^* \eta'$ with same set of states/register values such that $|\eta| \leq 4|Q| + 1$.

Leader case

In case of a leader, we have to keep track of the exact control state of the leader process.

- Symbolic states : (X, q'_l, d)
- Still $2|Q| + 1$ fixed support blocks
- Each block can be reduced to last write and at most $|Q|$ transitions of the leader
- Final bound of the form $2|Q| + (2|Q| + 1)|Q|$.

Leader case

In case of a leader, we have to keep track of the exact control state of the leader process.

- Symbolic states : (X, q'_l, d)
- Still $2|Q| + 1$ fixed support blocks
- Each block can be reduced to last write and at most $|Q|$ transitions of the leader
- Final bound of the form $2|Q| + (2|Q| + 1)|Q|$.

Theorem

The reachability problem is NP-complete.

Sketch.

- Guess the polynomial path.
- Reduction from 3−SAT.

□

Language formalism

Definition

$$L(\mathcal{P}) = L(\mathcal{A}_D) \cap \left(L(\mathcal{A}_I) \,\text{⧔}\, \bigcup_{k \geq 1} \,\text{⧔}_{i=1}^{k}\, L(\mathcal{A}) \right)$$

Where

- $L(\mathcal{P})$ is the language of all possible infinite runs.

Language formalism

Definition

$$L(\mathcal{P}) = L(\mathcal{A}_D) \cap \left(L(\mathcal{A}_l) \between \bigcup_{k \geq 1} \between_{i=1}^{k} L(\mathcal{A}) \right)$$

Where

- $L(\mathcal{P})$ is the language of all possible infinite runs.
- The automata recognize languages over $\Sigma_D = \{w(d), r(d) \mid d \in D\}$.
- $\between$ is the shuffle operations over languages.
- $\mathcal{A}_D$ is an automaton recognizing correct sequences of read and write operations.
- $\mathcal{A}_l$ is the automaton of the leader.
- $\mathcal{A}$ is the automaton of the protocol.

Language formalism

Definition

$$L(\mathcal{P}) = L(\mathcal{A}_D) \cap \left(L(\mathcal{A}_l) \between \bigcup_{k \geq 1} \between_{i=1}^{k} L(\mathcal{A}) \right)$$

Where

- $L(\mathcal{P})$ is the language of all possible infinite runs.
- The automata recognize languages over $\Sigma_D = \{w(d), r(d) \mid d \in D\}$.
- $\between$ is the shuffle operations over languages.
- $\mathcal{A}_D$ is an automaton recognizing correct sequences of read and write operations.
- $\mathcal{A}_l$ is the automaton of the leader.
- $\mathcal{A}$ is the automaton of the protocol.

Given a Bchi automaton $\mathcal{A}_\varphi$, decide whether $L(\mathcal{P}) \cap L(\mathcal{A}_\varphi) = \emptyset$.

1 The model

2 (Non-)Deterministic Model Checking

3 Probabilistic case
- Probabilistic semantics
- Cut-off property
- Existence of a cut-off
- Complexity aspects
- A linear example
- PSPACE hardness
- Upper Bound

Markov Chain

Definition (Law of motion)

We consider $(\Gamma, \rightarrow)$ as a Markov Chain.

$$\Pr(\gamma \rightarrow \gamma') = \frac{1}{|\mathrm{Post}(\gamma)|}$$

Markov Chain

Definition (Law of motion)

We consider $(\Gamma, \rightarrow)$ as a Markov Chain.

$$\Pr(\gamma \rightarrow \gamma') = \frac{1}{|\mathrm{Post}(\gamma)|}$$

Let $(q_0, d_0) \in Q \times D$, a parameter n.
For $X \subseteq \Gamma$, we denote $\mathbb{P}^n(X)$ the probability to eventually reach some $\gamma \in X$ from (q_0^n, d_0).

Markov Chain

Definition (Law of motion)

We consider $(\Gamma, \rightarrow)$ as a Markov Chain.

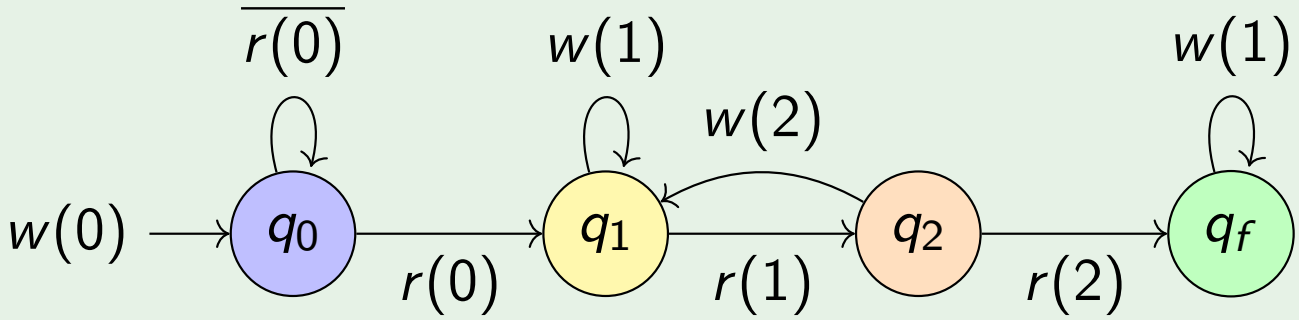
$$\Pr(\gamma \rightarrow \gamma') = \frac{1}{|\mathrm{Post}(\gamma)|}$$

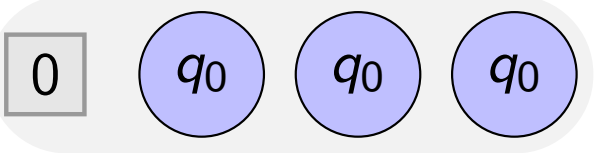
Let $(q_0, d_0) \in Q \times D$, a parameter n.
For $X \subseteq \Gamma$, we denote $\mathbb{P}^n(X)$ the probability to eventually reach some $\gamma \in X$ from (q_0^n, d_0).

Qualitative goal

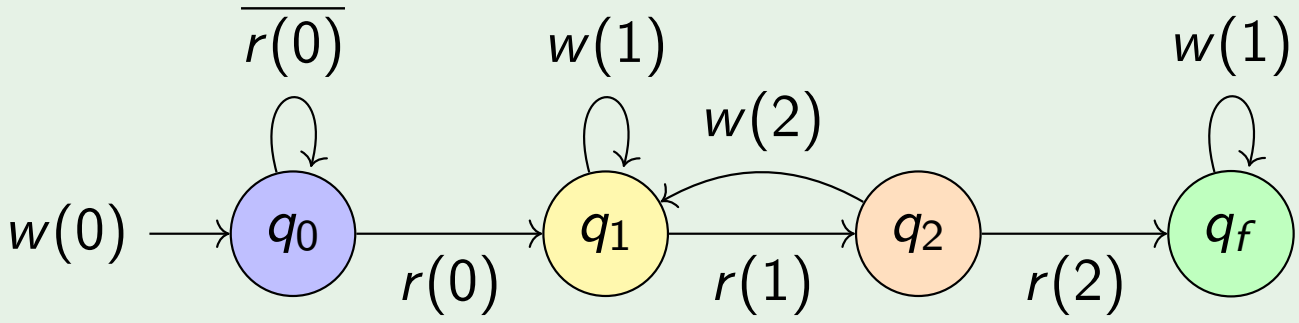
Let $q_f \in Q$.
Estimate $\mathbb{P}^n(\uparrow q_f)$

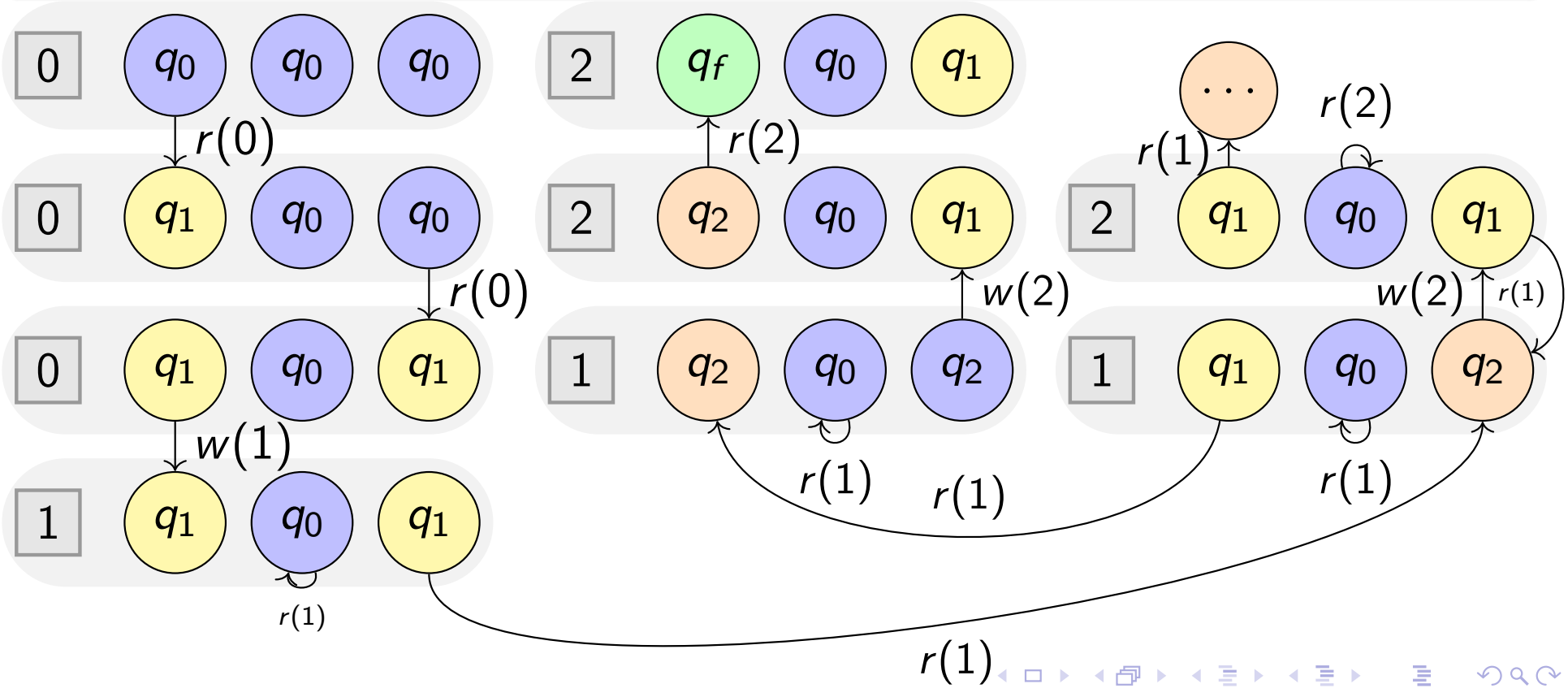
Example



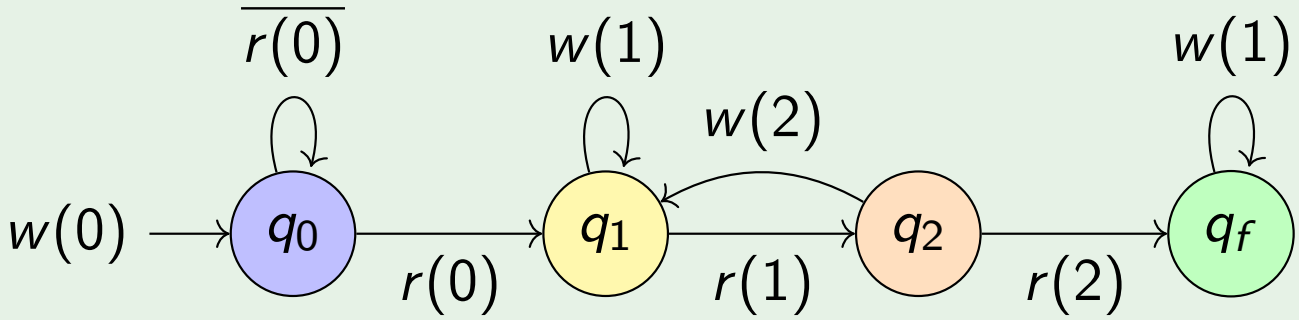


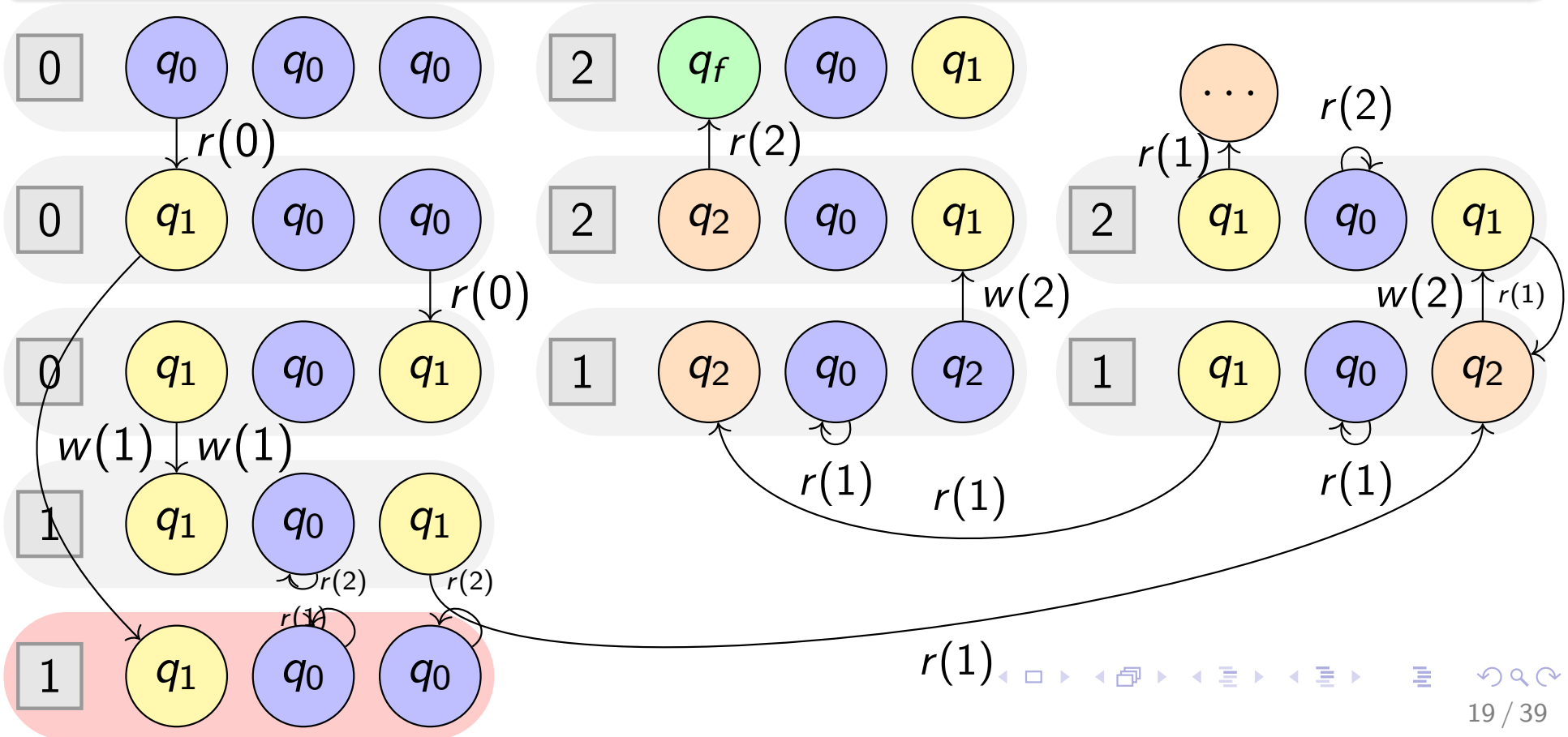
Example


$\overline{r(0)}$
$w(1)$
$w(1)$
$w(2)$
$w(0)$
q_0
q_1
q_2
q_f
$r(0)$
$r(1)$
$r(2)$


0
q_0 q_0 q_0
$r(0)$
0
q_1 q_0 q_0
$r(0)$
0
q_1 q_0 q_1
$w(1)$
1
q_1 q_0 q_1
$r(1)$
2
q_f q_0 q_1
$r(2)$
2
q_2 q_0 q_1
$w(2)$
1
q_2 q_0 q_2
$r(1)$ $r(1)$
$\cdots$
$r(1)$
$r(2)$
2
q_1 q_0 q_1
$w(2)$
$r(1)$
1
q_1 q_0 q_2
$r(1)$
$r(1)$

Example


$\overline{r(0)}$
$w(1)$
$w(1)$
$w(2)$
$w(0)$
q_0
q_1
q_2
q_f
$r(0)$
$r(1)$
$r(2)$


0
2
1
q_0
q_1
q_2
q_f
$r(0)$
$r(2)$
$w(1)$
$w(2)$
$r(1)$
$r(2)$
$\cdots$

Remarks

Lemma (Qualitative assumption)

The properties $\mathbb{P}^n(\uparrow q_f) > 0$ *and* $\mathbb{P}^n(\uparrow q_f) = 1$ *does* <u>not</u> *depend on the actual probabilities.*

Remarks

Lemma (Qualitative assumption)

The properties $\mathbb{P}^n(\uparrow q_f) > 0$ *and* $\mathbb{P}^n(\uparrow q_f) = 1$ *does not depend on the actual probabilities.*

We have already solved the case $\mathbb{P}^n(\uparrow q_f) > 0$: it corresponds to finding a path to $\uparrow q_f$.

Remarks

Lemma (Qualitative assumption)

The properties $\mathbb{P}^n(\uparrow q_f) > 0$ *and* $\mathbb{P}^n(\uparrow q_f) = 1$ *does not depend on the actual probabilities.*

We have already solved the case $\mathbb{P}^n(\uparrow q_f) > 0$: it corresponds to finding a path to $\uparrow q_f$.

Lemma (Discretization)

$$\mathbb{P}^n(\uparrow q_f) = 0 \Leftrightarrow \mathrm{Post}^*((q_0^n, d_0)) \cap \mathrm{Pre}^*(\uparrow q_f) = \emptyset$$

Remarks

Lemma (Qualitative assumption)

The properties $\mathbb{P}^n(\uparrow q_f) > 0$ *and* $\mathbb{P}^n(\uparrow q_f) = 1$ *does not depend on the actual probabilities.*

We have already solved the case $\mathbb{P}^n(\uparrow q_f) > 0$: it corresponds to finding a path to $\uparrow q_f$.

Lemma (Discretization)

$$\mathbb{P}^n(\uparrow q_f) = 0 \Leftrightarrow \mathrm{Post}^*((q_0^n, d_0)) \cap \mathrm{Pre}^*(\uparrow q_f) = \emptyset$$

$$\mathbb{P}^n(\uparrow q_f) = 1 \Leftrightarrow \mathrm{Post}^*((q_0^n, d_0)) \subseteq \mathrm{Pre}^*(\uparrow q_f)$$

Remarks

Lemma (Qualitative assumption)

The properties $\mathbb{P}^n(\uparrow q_f) > 0$ *and* $\mathbb{P}^n(\uparrow q_f) = 1$ *does not depend on the actual probabilities.*

We have already solved the case $\mathbb{P}^n(\uparrow q_f) > 0$: it corresponds to finding a path to $\uparrow q_f$.

Lemma (Discretization)

$$\mathbb{P}^n(\uparrow q_f) = 0 \Leftrightarrow \mathrm{Post}^*((q_0^n, d_0)) \cap \mathrm{Pre}^*(\uparrow q_f) = \emptyset$$

$$\mathbb{P}^n(\uparrow q_f) = 1 \Leftrightarrow \mathrm{Post}^*((q_0^n, d_0)) \subseteq \mathrm{Pre}^*(\uparrow q_f)$$

- We focus now on the almost-sure ($\mathrm{Pr}^n(\uparrow q_f) = 1$ problem).
- Both the scheduler and processes are ~~non-deterministic~~ stochastic
- No atomicity
- No monotonicity a priori
- For fixed parameter n, can be encoded as a Petri Net

What we are looking for

Some limit behaviour, if possible

Definition (Cut-off)

Le N a parameter. If $\forall n \geq N \ \mathbb{P}^n(\uparrow q_f) = 1$ or $\forall n \geq N \ \mathbb{P}^n(\uparrow q_f) < 1$, then N is a cut-off.

What we are looking for

Some limit behaviour, if possible

Definition (Cut-off)

Le N a parameter. If $\forall n \geq N \ \mathbb{P}^n(\uparrow q_f) = 1$ or $\forall n \geq N \ \mathbb{P}^n(\uparrow q_f) < 1$, then N is a cut-off.

- First case is said positive, second case negative
- Non-atomicity is crucial

Upward closed sets and well-quasi-orders

Definition (Well-quasi-ordering (wqo))

A quasi-ordering $\preceq$ on a set X such that any infinite sequence of elements $x_0, x_1 \ldots$ from X contains an increasing pair $x_i \preceq x_j$ with $i < j$.

Upward closed sets and well-quasi-orders

Definition (Well-quasi-ordering (wqo))

A quasi-ordering $\preceq$ on a set X such that any infinite sequence of elements $x_0, x_1 \ldots$ from X contains an increasing pair $x_i \preceq x_j$ with $i < j$.

Lemma (Upward-closed set)

Let $Y \subseteq X$, such that $\forall \gamma \preceq \gamma' \ \gamma \in Y \Rightarrow \gamma' \in Y$, then Y is generated by $\min(Y)$*:*

$$Y = \uparrow \min(Y) = \left\{ \gamma' \mid \exists \gamma \in \min(Y) \ \gamma \preceq \gamma' \right\}$$

Upward closed sets and well-quasi-orders

Definition (Well-quasi-ordering (wqo))

A quasi-ordering $\preceq$ on a set X such that any infinite sequence of elements $x_0, x_1 \ldots$ from X contains an increasing pair $x_i \preceq x_j$ with $i < j$.

Lemma (Upward-closed set)

Let $Y \subseteq X$, *such that* $\forall \gamma \preceq \gamma' \ \gamma \in Y \Rightarrow \gamma' \in Y$, *then* Y *is generated by* $\min(Y)$*:*

$$Y = \uparrow \min(Y) = \left\{\gamma' \mid \exists \gamma \in \min(Y) \ \gamma \preceq \gamma'\right\}$$

$\preceq$ *is wqo so* $\min(Y)$ *is finite.*

Upward closed sets and well-quasi-orders

Definition (Well-quasi-ordering (wqo))

A quasi-ordering $\preceq$ on a set X such that any infinite sequence of elements $x_0, x_1 \ldots$ from X contains an increasing pair $x_i \preceq x_j$ with $i < j$.

Lemma (Upward-closed set)

Let $Y \subseteq X$, such that $\forall \gamma \preceq \gamma' \ \gamma \in Y \Rightarrow \gamma' \in Y$, then Y is generated by $\min(Y)$*:*

$$Y = \uparrow \min(Y) = \left\{\gamma' \mid \exists \gamma \in \min(Y) \ \gamma \preceq \gamma'\right\}$$

$\preceq$ is wqo so $\min(Y)$ *is finite.*

Main idea: express $\mathrm{Pre}^*(\uparrow q_f)$ and $\mathrm{Post}^*((q_0^k, d_0))$ as upward-sets to "discretize" the problem.

The right partial order

Definition

$$\gamma \preceq \gamma' \Leftrightarrow v(\gamma) = v(\gamma') \wedge \forall q \; \gamma(q) \leq \gamma'(q)$$

$\preceq$ is a well quasi-order.

- $\mathrm{Pre}^*(\uparrow q_f)$ is upward-closed
- $\mathrm{Post}^*((q_0^n, d_0))$ is ...

The right partial order

Definition

$$\gamma \preceq \gamma' \Leftrightarrow v(\gamma) = v(\gamma') \wedge \forall q\ \gamma(q) \leq \gamma'(q)$$

$\preceq$ is a well quasi-order.

- $\mathrm{Pre}^*(\uparrow q_f)$ is upward-closed
- $\mathrm{Post}^*((q_0^n, d_0))$ is ...

Lemma (Mimicking process)

Let $(q_0^k, d_0) \to^* \gamma$ *and* q *such that* $\gamma(q) > 0$. *Then,* $(q_0^{k+1}, d_0) \to^* \gamma + q$.

The right partial order

Definition

$$\gamma \preceq \gamma' \Leftrightarrow v(\gamma) = v(\gamma') \wedge \forall q\ \gamma(q) \leq \gamma'(q) \wedge \overline{S}(\gamma) = \overline{S}(\gamma')$$

$\preceq$ is a well quasi-order.

- $\mathrm{Pre}^*(\uparrow q_f)$ is upward-closed
- $\mathrm{Post}^*(\uparrow(q_0^n, d_0))$ is ... upward-closed

Lemma (Mimicking process)

Let $(q_0^k, d_0) \to^* \gamma$ *and* q *such that* $\gamma(q) > 0$. *Then,* $(q_0^{k+1}, d_0) \to^* \gamma + q$.

Cut-off

We write

$$\mathrm{Post}^*(\uparrow (q_0, d_0)) = \cup_{i=1}^{k} \uparrow \gamma_i \quad \mathrm{Pre}^*(\uparrow q_f) = \cup_{j=1}^{k} \uparrow \eta_j$$

Cut-off

We write

$$\mathrm{Post}^*(\uparrow (q_0, d_0)) = \cup_{i=1}^{k} \uparrow \gamma_i \quad \mathrm{Pre}^*(\uparrow q_f) = \cup_{j=1}^{k} \uparrow \eta_j$$

$$\mathrm{Post}^*(\uparrow (q_0' d_0)) \subseteq \mathrm{Pre}^*(\uparrow q_f)$$

Cut-off

We write

$$\mathrm{Post}^*(\uparrow (q_0, d_0)) = \cup_{i=1}^{k} \uparrow \gamma_i \quad \mathrm{Pre}^*(\uparrow q_f) = \cup_{j=1}^{k} \uparrow \eta_j$$

$$\mathrm{Post}^*(\uparrow (q_0' d_0)) \subseteq \mathrm{Pre}^*(\uparrow q_f)$$

$$\Leftrightarrow$$

$$\forall i \; \exists j \; \eta_j \preceq \gamma_i$$

Cut-off

We write

$$\mathrm{Post}^*(\uparrow (q_0, d_0)) = \cup_{i=1}^{k} \uparrow \gamma_i \quad \mathrm{Pre}^*(\uparrow q_f) = \cup_{j=1}^{k} \uparrow \eta_j$$

$$\mathrm{Post}^*(\uparrow (q_0' d_0)) \subseteq \mathrm{Pre}^*(\uparrow q_f)$$

$$\Leftrightarrow$$

$$\forall i \; \exists j \; \eta_j \preceq \gamma_i$$

$$\Leftrightarrow$$

n is a positive cut-off

Cut-off

We write

$$\mathrm{Post}^*(\uparrow (q_0, d_0)) = \cup_{i=1}^{k} \uparrow \gamma_i \quad \mathrm{Pre}^*(\uparrow q_f) = \cup_{j=1}^{k} \uparrow \eta_j$$

$$\mathrm{Post}^*(\uparrow (q_0' d_0)) \subseteq \mathrm{Pre}^*(\uparrow q_f)$$

$$\Leftrightarrow$$

$$\forall i \; \exists j \; \eta_j \preceq \gamma_i$$

$$\Leftrightarrow$$

n is a positive cut-off

What about the negative cut-off case ?

Negative case

$$\mathrm{Post}^*(\uparrow (q_0, d_0)) = \cup_{i=1}^{k} \uparrow \gamma_i$$

- If there exists γ_i such that $\forall j\ \overline{S}(\gamma_i) \neq \overline{S}(\eta_j)$, then ...

Negative case

$$\mathrm{Post}^*(\uparrow (q_0, d_0)) = \cup_{i=1}^{k} \uparrow \gamma_i$$

- If there exists γ_i such that $\forall j\ \overline{S}(\gamma_i) \neq \overline{S}(\eta_j)$, then ... $\forall j\ \eta_j \not\preceq \gamma_i$, so n is negative cut-off

Negative case

$$\mathrm{Post}^*(\uparrow (q_0, d_0)) = \cup_{i=1}^{k} \uparrow \gamma_i$$

- If there exists γ_i such that $\forall j\ \overline{S}(\gamma_i) \neq \overline{S}(\eta_j)$, then ... $\forall j\ \eta_j \not\preceq \gamma_i$, so n is negative cut-off
  Corresponds to the symbolic graph analysis.

Negative case

$$\mathrm{Post}^*(\uparrow (q_0, d_0)) = \cup_{i=1}^{k} \uparrow \gamma_i$$

- If there exists γ_i such that $\forall j\ \overline{S}(\gamma_i) \neq \overline{S}(\eta_j)$, then ... $\forall j\ \eta_j \not\preceq \gamma_i$, so n is negative cut-off
  Corresponds to the symbolic graph analysis.
- The converse is false

Negative case

$$\mathrm{Post}^*(\uparrow (q_0, d_0)) = \cup_{i=1}^{k} \uparrow \gamma_i$$

- If there exists γ_i such that $\forall j\ \overline{S}(\gamma_i) \neq \overline{S}(\eta_j)$, then ... $\forall j\ \eta_j \not\preceq \gamma_i$, so n is negative cut-off
  Corresponds to the symbolic graph analysis.
- The converse is false

How does

$$\min \mathrm{Post}^*(\uparrow (q_0, d_0)) = \{\gamma_{1,n} \dots \gamma_{k_n,n}\}$$

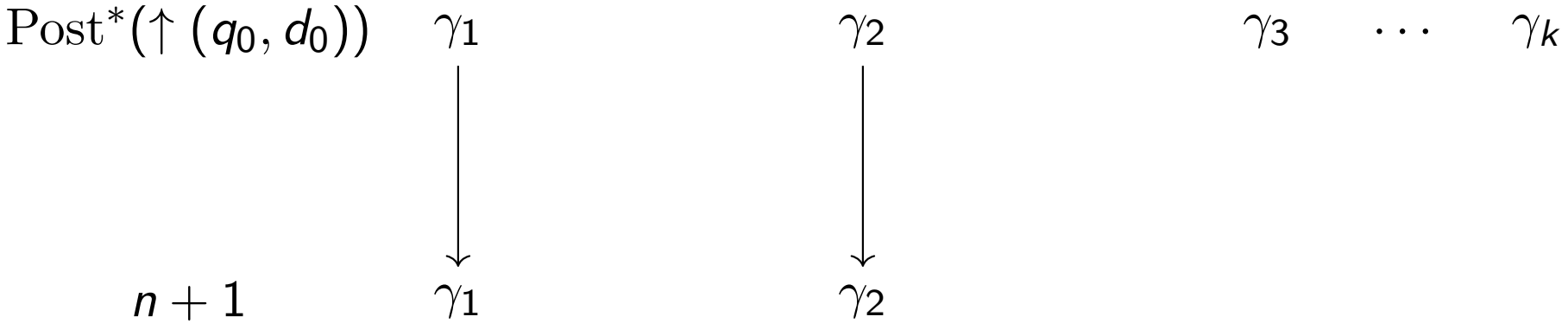
varies w.r.t n ?

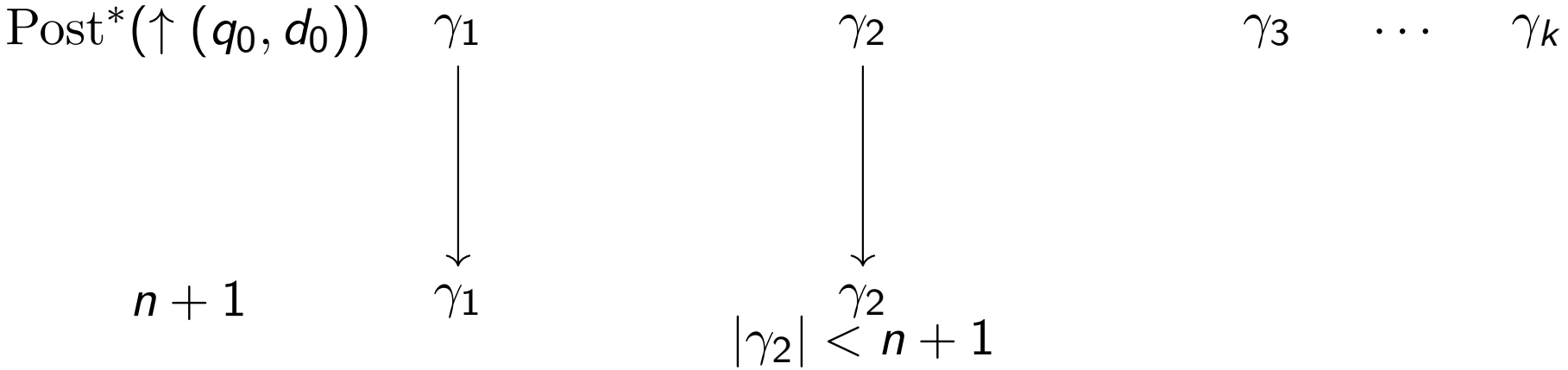
$\mathrm{Post}^*(\uparrow(q_0, d_0))$ γ_1 γ_2 γ_3 $\cdots$ γ_k

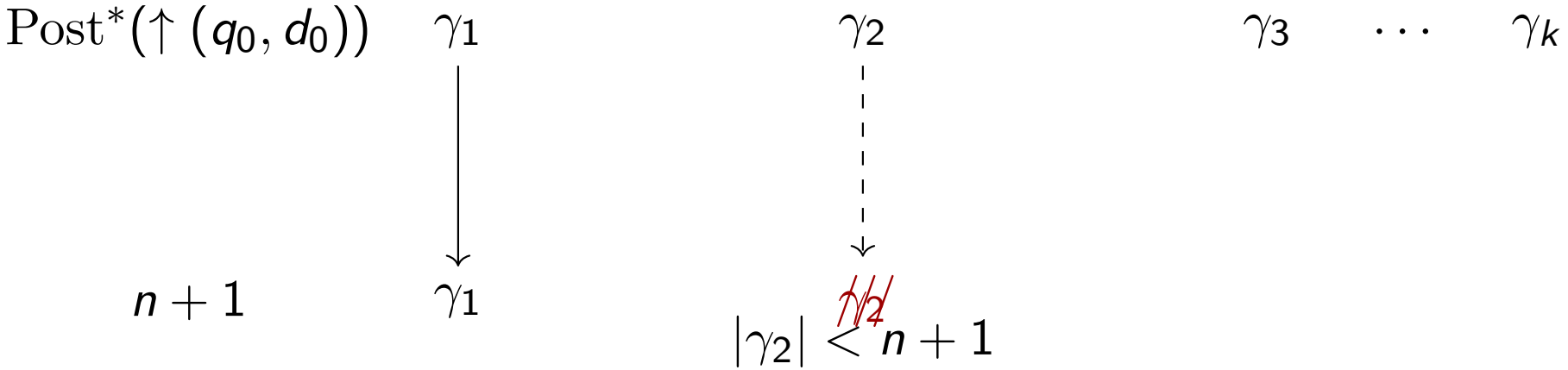
$\mathrm{Post}^*(\uparrow(q_0, d_0))$ γ_1 γ_2 γ_3 $\cdots$ γ_k

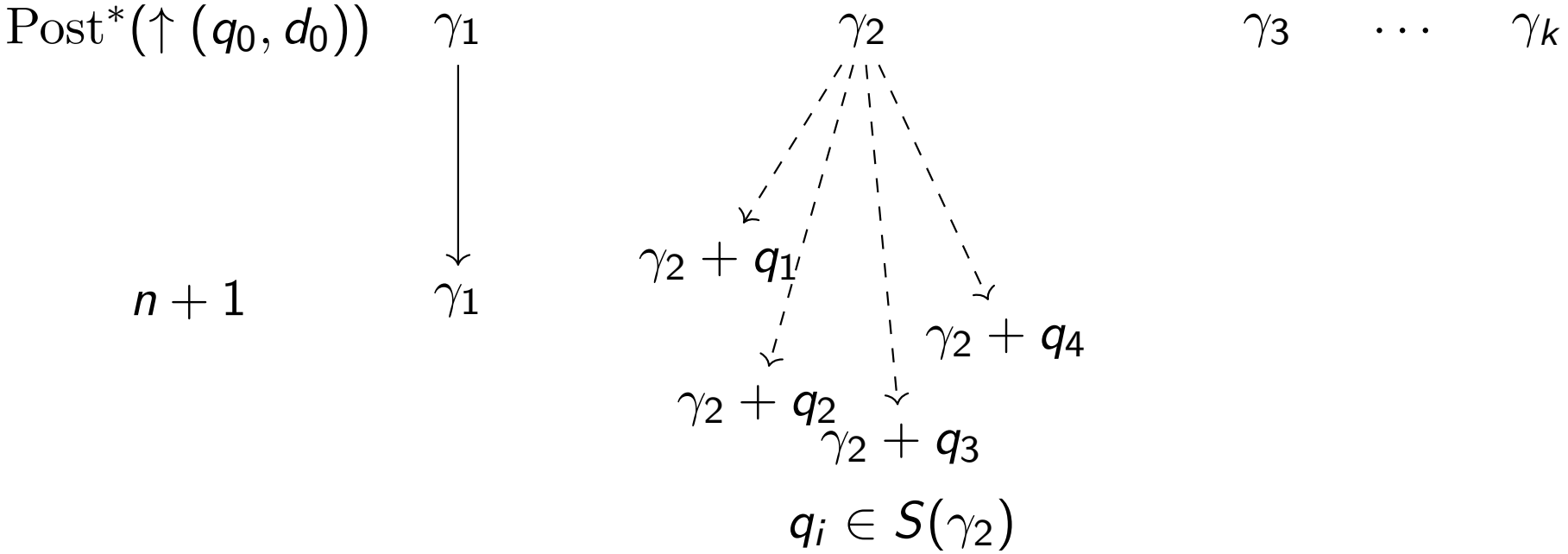
$n+1$

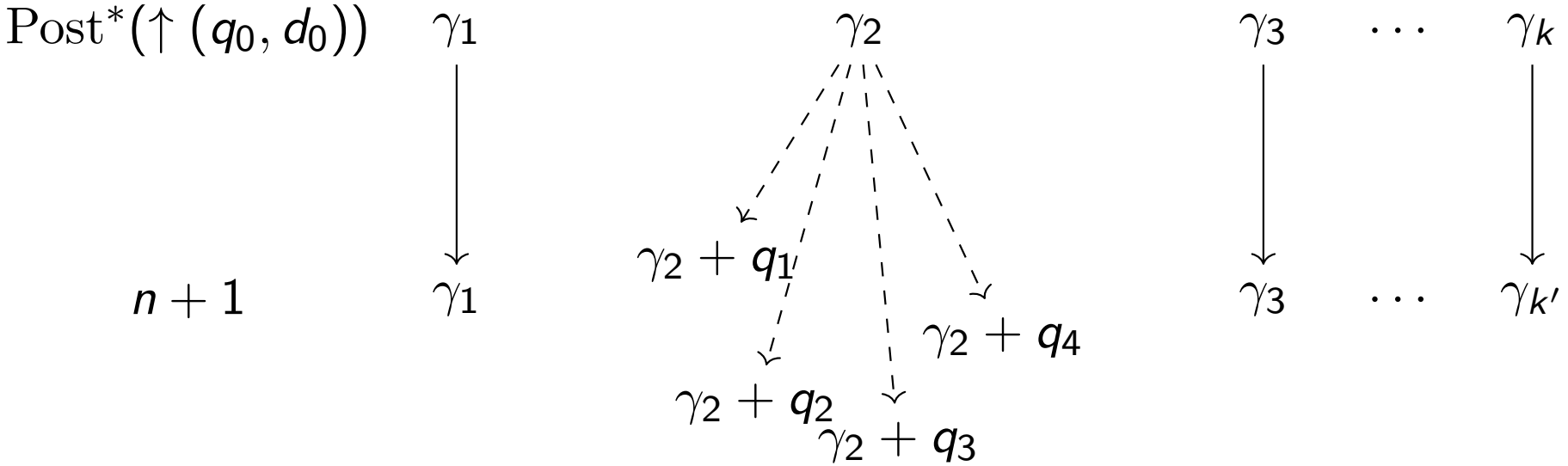

$\mathrm{Post}^*(\uparrow(q_0, d_0))$
γ_1
γ_2
γ_3
$\cdots$
γ_k
$n+1$
γ_1

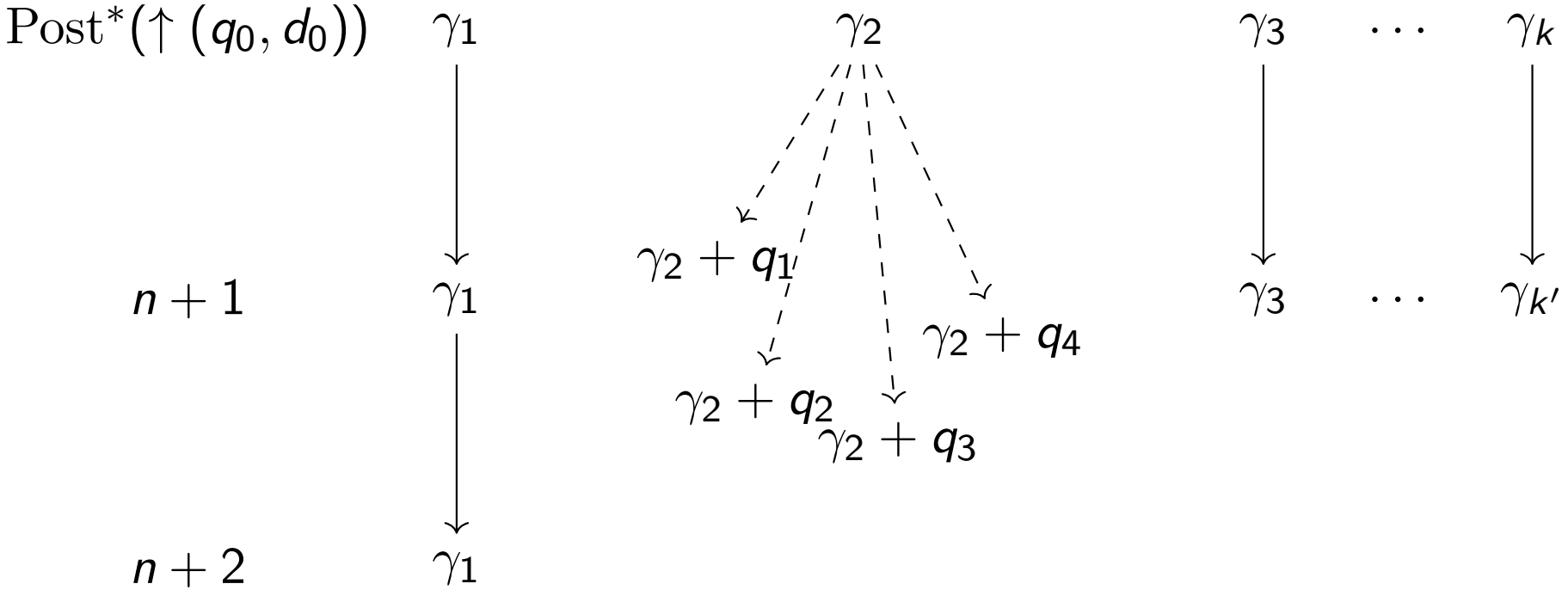

$\mathrm{Post}^*(\uparrow(q_0, d_0))$
γ_1
γ_2
γ_3
$\cdots$
γ_k
$n+1$
γ_1
γ_2

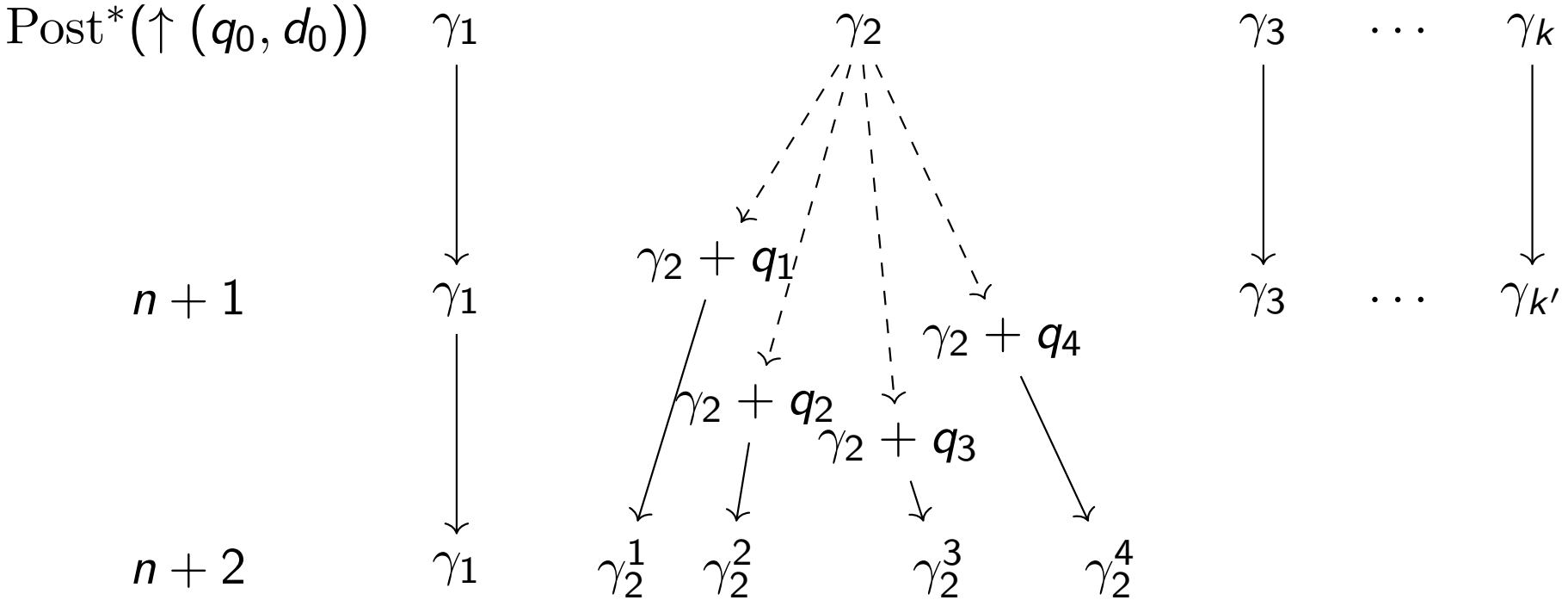

$\mathrm{Post}^*(\uparrow(q_0, d_0))$
γ_1
γ_2
γ_3
$\cdots$
γ_k
$n+1$
γ_1
γ_2
$|\gamma_2| < n+1$

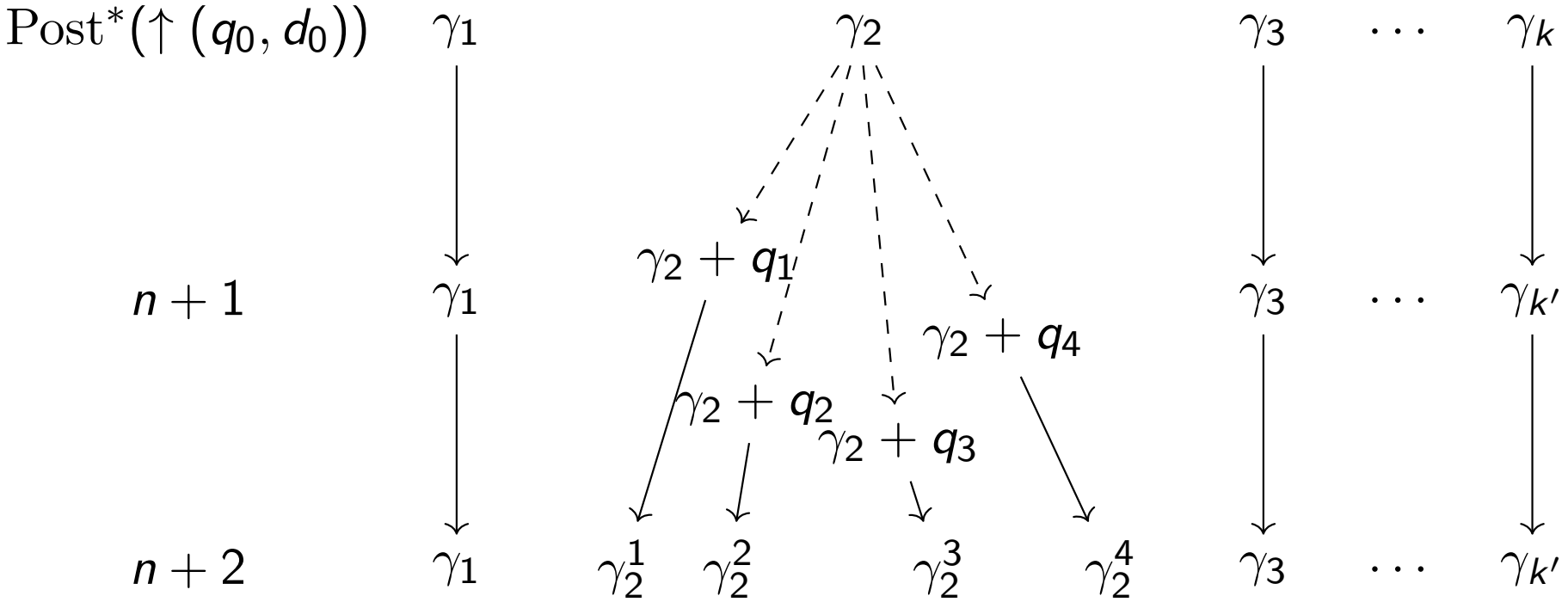

$\mathrm{Post}^*(\uparrow(q_0, d_0))$
γ_1
γ_2
γ_3
$\cdots$
γ_k
$n+1$
γ_1
γ_2
$|\gamma_2| < n+1$


$\mathrm{Post}^*(\uparrow(q_0, d_0))$
γ_1
γ_2
γ_3
$\cdots$
γ_k
$n+1$
γ_1
$\gamma_2 + q_1$
$\gamma_2 + q_4$
$\gamma_2 + q_2$
$\gamma_2 + q_3$
$q_i \in S(\gamma_2)$


$\mathrm{Post}^*(\uparrow(q_0, d_0))$
γ_1
γ_2
γ_3
$\cdots$
γ_k
$\gamma_2 + q_1$
$\gamma_2 + q_4$
$\gamma_2 + q_2$
$\gamma_2 + q_3$
$n+1$
γ_1
γ_3
$\cdots$
$\gamma_{k'}$


$\mathrm{Post}^*(\uparrow(q_0, d_0))$
γ_1
γ_2
γ_3
$\cdots$
γ_k
$n+1$
γ_1
$\gamma_2 + q_1$
$\gamma_2 + q_4$
$\gamma_2 + q_2$
$\gamma_2 + q_3$
γ_3
$\cdots$
$\gamma_{k'}$
$n+2$
γ_1


$\mathrm{Post}^*(\uparrow(q_0, d_0))$
γ_1
γ_2
γ_3
$\cdots$
γ_k
$n+1$
γ_1
$\gamma_2 + q_1$
$\gamma_2 + q_2$
$\gamma_2 + q_3$
$\gamma_2 + q_4$
γ_3
$\cdots$
$\gamma_{k'}$
$n+2$
γ_1
γ_2^1
γ_2^2
γ_2^3
γ_2^4


$\mathrm{Post}^*(\uparrow(q_0, d_0))$
γ_1
γ_2
γ_3
$\cdots$
γ_k
$n+1$
γ_1
$\gamma_2 + q_1$
γ_3
$\cdots$
$\gamma_{k'}$
$\gamma_2 + q_4$
$\gamma_2 + q_2$
$\gamma_2 + q_3$
$n+2$
γ_1
γ_2^1
γ_2^2
γ_2^3
γ_2^4
γ_3
$\cdots$
$\gamma_{k'}$

Variation of the basis

1. Start with $X_1 = \{\gamma_1 \dots \gamma_k\} = \min \mathrm{Post}^*(\uparrow (q_0, d_0))$

Variation of the basis

1. Start with $X_1 = \{\gamma_1 \dots \gamma_k\} = \min \mathrm{Post}^*(\uparrow (q_0, d_0))$
2. Compute

$$\{\gamma \mid \gamma \in X_n, |\gamma| > n\} \uplus \{\gamma + q \mid \gamma \in X_n, |\gamma| = n, q \in S(\gamma)\}$$

Variation of the basis

1. Start with $X_1 = \{\gamma_1 \dots \gamma_k\} = \min \mathrm{Post}^*(\uparrow (q_0, d_0))$
2. Compute

$$\{\gamma \mid \gamma \in X_n, |\gamma| > n\} \uplus \{\gamma + q \mid \gamma \in X_n, |\gamma| = n, q \in S(\gamma)\} = Y_{n+1}$$

3. Take $X_{n+1} = \min Y_{n+1}$

Variation of the basis

1. Start with $X_1 = \{\gamma_1 \dots \gamma_k\} = \min \mathrm{Post}^*(\uparrow (q_0, d_0))$
2. Compute

$$\{\gamma \mid \gamma \in X_n, |\gamma| > n\} \uplus \{\gamma + q \mid \gamma \in X_n, |\gamma| = n, q \in S(\gamma)\} = Y_{n+1}$$

3. Take $X_{n+1} = \min Y_{n+1}$

Goal

Keep track of a "problematic" generator $\gamma \in X_k$ as $k \to \infty$.

Definition

Assume

$$\mathrm{Pre}^*(\uparrow q_f) = \cup_{j=1}^{k} \uparrow \eta_j$$

and let $\gamma \in \mathrm{Post}^*(\uparrow (q_0, d_0))$. *We define:*

$$A(\gamma) = \bigcap_{j=1}^{m} \left\{ q \in S(\gamma) \;\middle|\; \forall k \geq 0 \; \eta_j \not\preceq \gamma + q^k \right\}$$

Definition

Assume

$$\mathrm{Pre}^*(\uparrow q_f) = \cup_{j=1}^{k} \uparrow \eta_j$$

and let $\gamma \in \mathrm{Post}^*(\uparrow (q_0, d_0))$. *We define:*

$$A(\gamma) = \bigcap_{j=1}^{m} \left\{ q \in S(\gamma) \;\middle|\; \forall k \geq 0 \; \eta_j \not\preceq \gamma + q^k \right\}$$

Theorem (Negative cut-off)

If $A(\gamma) \neq \emptyset$. *Then* $N = |\gamma|$ *is a negative cut-off.*

Positive cut-off

Lemma (Positive cut-off)

Assume $A(\gamma) = \emptyset$. *Then there exists* $N(\gamma) \geq |\gamma|$ *such that*

$$(\uparrow \gamma) \cap \mathrm{Post}^* \left(q_0^{\geq N(\gamma)}, d_0 \right) \subseteq \mathrm{Pre}^*(\uparrow q_f)$$

Positive cut-off

Lemma (Positive cut-off)

Assume $A(\gamma) = \emptyset$. *Then there exists* $N(\gamma) \geq |\gamma|$ *such that*

$$(\uparrow \gamma) \cap \mathrm{Post}^* \left(q_0^{\geq N(\gamma)}, d_0 \right) \subseteq \mathrm{Pre}^*(\uparrow q_f)$$

Moreover, $N(\gamma)$ *is polynomial in the size of* γ *and the* η_j.

Positive cut-off

Lemma (Positive cut-off)

Assume $A(\gamma) = \emptyset$. Then there exists $N(\gamma) \geq |\gamma|$ such that

$$(\uparrow \gamma) \cap \mathrm{Post}^* \left(q_0^{\geq N(\gamma)}, d_0 \right) \subseteq \mathrm{Pre}^*(\uparrow q_f)$$

Moreover, $N(\gamma)$ is polynomial in the size of γ and the η_j.

Proof.

For any $q \in S(\gamma)$, there exists j_q such that $q \notin \left\{ q \;\middle|\; \forall k \geq 0 \; \eta_{j_q} \not\preceq \gamma + q^k \right\}$ so there exists k_q such that $\eta_{j_q} \preceq \gamma + q^{k_q}$.
Define $N(\gamma) = |\gamma| + \sum_{q \in S(\gamma)} k_q$. □

Existential solution

Theorem

Given a protocol $\mathcal{P}$ there always exists either a positive cut-off either a negative cut-off N.
The probability to reach $\uparrow q_f$ is eventually 1 *or eventually strictly less than* 1.

- Non-constructive proof
- We never computed the γ_i and η_j
- If computed, we can give a polynomial bound of N in their size
- Deciding the positive or negative case ?

Existential solution

Theorem

Given a protocol $\mathcal{P}$ there always exists either a positive cut-off either a negative cut-off N.
The probability to reach $\uparrow q_f$ is eventually 1 *or eventually strictly less than* 1*.*

- Non-constructive proof
- We never computed the γ_i and η_j
- If computed, we can give a polynomial bound of N in their size
- Deciding the positive or negative case ?
- Simulate the Markov chain with N initial processes ?

Negative cut-off: the easy case

Remark

If $\mathrm{Post}^*((\{q_0\}, d_0)) \not\subseteq \mathrm{Pre}^*(\uparrow q_f)$ in G_{symb}, then $\mathbb{P}^n(\uparrow q_f) < 1$ for n large enough (negative cut-off).

Negative cut-off: the easy case

Remark

If $\mathrm{Post}^*((\{q_0\}, d_0)) \not\subseteq \mathrm{Pre}^*(\uparrow q_f)$ in G_{symb}, then $\mathbb{P}^n(\uparrow q_f) < 1$ for n large enough (negative cut-off).

The converse is not true

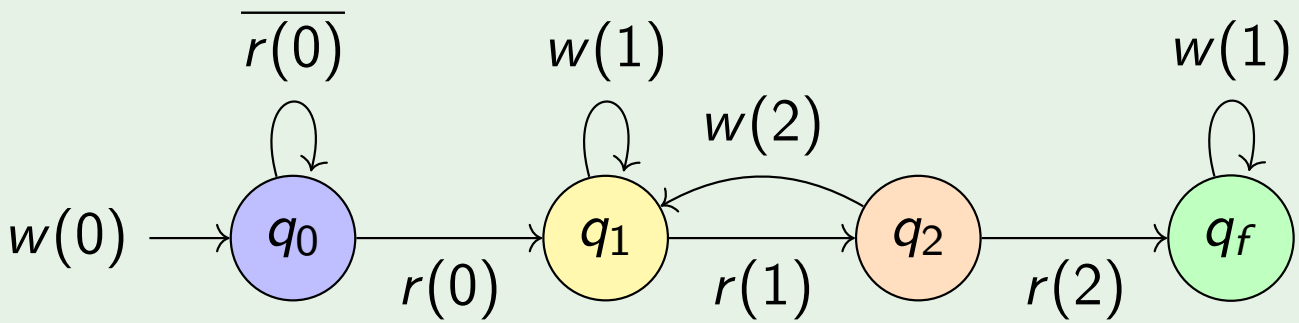
Negative cut-off: the easy case

Remark

If $\mathrm{Post}^*((\{q_0\}, d_0)) \not\subseteq \mathrm{Pre}^*(\uparrow q_f)$ in G_{symb}, then $\mathbb{P}^n(\uparrow q_f) < 1$ for n large enough (negative cut-off).

The converse is not true

Example



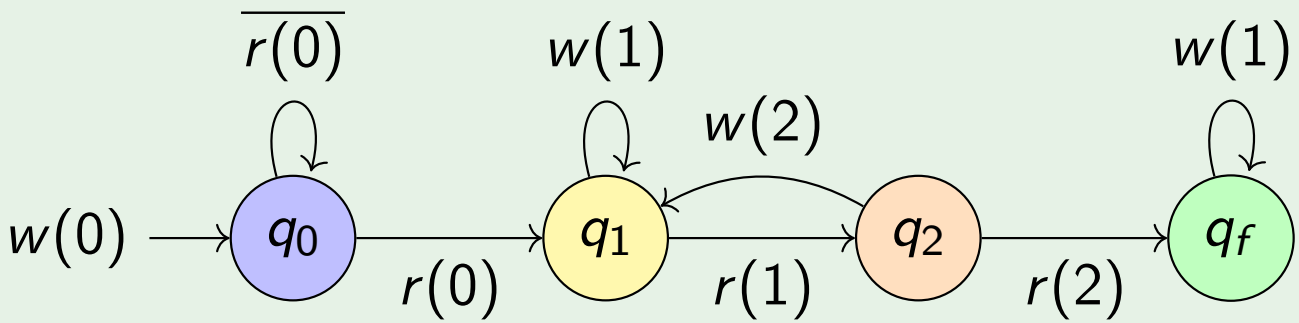
Negative cut-off: the easy case

Remark

If $\mathrm{Post}^*((\{q_0\}, d_0)) \not\subseteq \mathrm{Pre}^*(\uparrow q_f)$ in G_{symb}, then $\mathbb{P}^n(\uparrow q_f) < 1$ for n large enough (negative cut-off).

The converse is not true

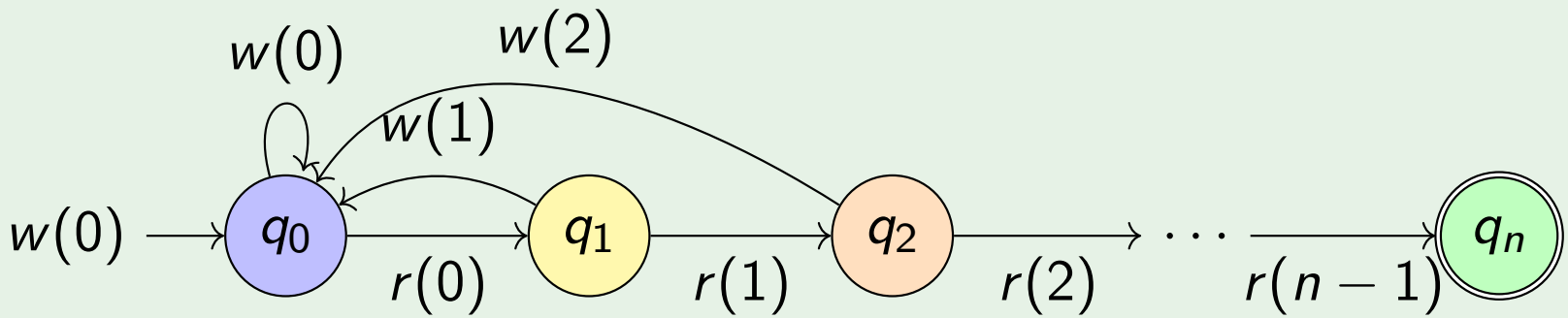
Example



$$(q_0^n, 0) \xrightarrow{r(0)} (q_0^{n-1} q_1, 0) \xrightarrow{w(0)} (q_0^{n-1} q_1, 1) \not\to^* \uparrow q_f$$

Linear example

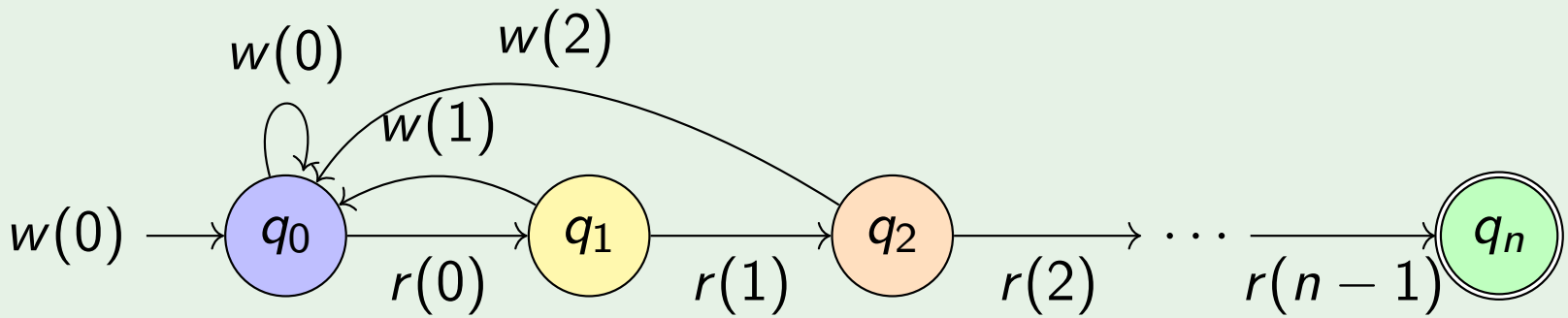
Example



Cut-off value ?

Linear example

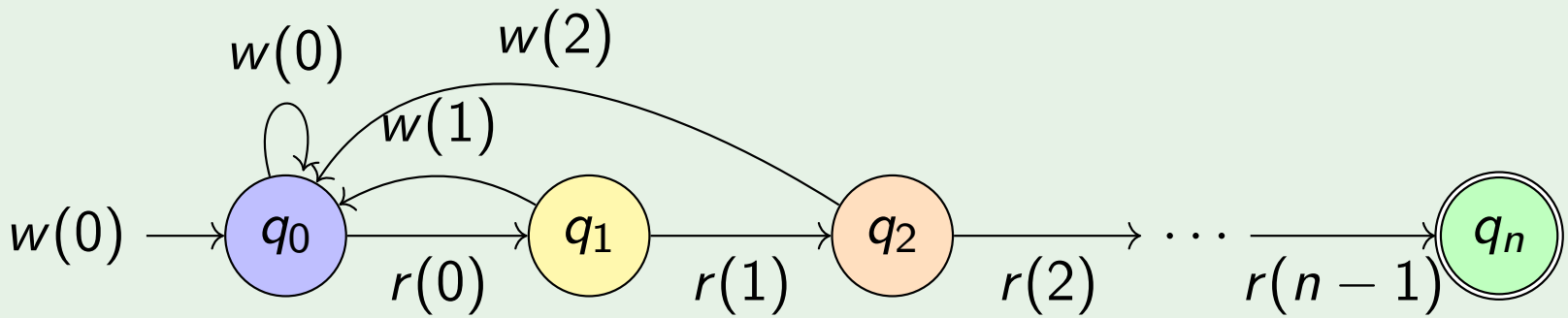
Example



Cut-off value ? The cut-off is positive and equals n.

Linear example

Example



Cut-off value ? The cut-off is positive and equals n.

Invariant:

$$\forall j \leq m \ \sum_{k=0}^{j} \gamma(q_k) \geq j + \mathbb{1}_{v(\gamma)=j+1}$$

PSPACE-hardness

Decision Problem

- INPUT: a protocol $\mathcal{P}$
- OUTPUT: whether the cut-off is positive or negative

PSPACE-hardness

Decision Problem

- INPUT: a protocol $\mathcal{P}$
- OUTPUT: whether the cut-off is positive or negative

- So far, all examples have linear size cut-off
- Verifying if the cut-off is positive can be done by building the Markov Chain

PSPACE-hardness

Decision Problem

- INPUT: a protocol $\mathcal{P}$
- OUTPUT: whether the cut-off is positive or negative

- So far, all examples have linear size cut-off
- Verifying if the cut-off is positive can be done by building the Markov Chain

Theorem

The cut-off decision problem is PSPACE-hard.

Sketch.

We reduce the halting of a linear bounded Turing machine $\mathcal{M}$.

- A given tape position i containing letter x is coded by a fixed state
- The current head position is coded in the register

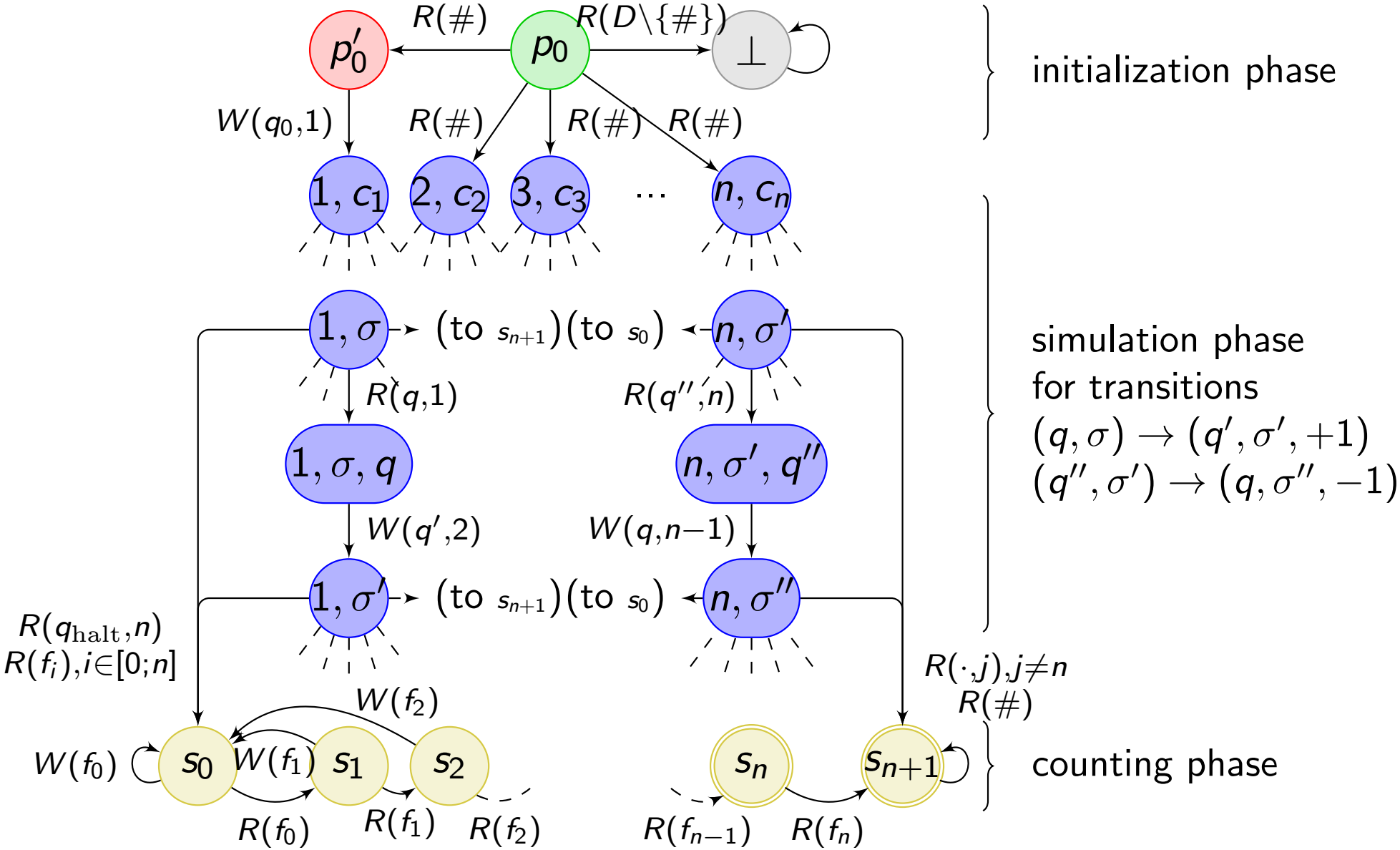
Sketch.

We reduce the halting of a linear bounded Turing machine $\mathcal{M}$.

- A given tape position i containing letter x is coded by a fixed state
- The current head position is coded in the register
- If the number of states is too big, we cannot ensure proper encoding
- Key idea: we code improper encoding/non-termination by $\mathbb{P}(\uparrow q_f) = 1$
- The previous module ensures $\uparrow q_f$ if too many processes encoded the machine
- We assume the machine starts from first tape position and accepts only on last tape position.

We build $\mathcal{P}$ protocol such that

$$\mathbb{P}^{\geq n}(\uparrow q_f) = 1 \iff \mathcal{M} \text{ does } \underline{\text{not}} \text{ terminate}$$


p'_0
$R(\#)$
p_0
$R(D\backslash\{\#\})$
$\bot$
initialization phase
$W(q_0,1)$
$R(\#)$
$R(\#)$
$R(\#)$
$1, c_1$
$2, c_2$
$3, c_3$
$\dots$
n, c_n
$1, \sigma$
(to s_{n+1})(to s_0)
n, σ'
simulation phase
for transitions
$(q, \sigma) \to (q', \sigma', +1)$
$(q'', \sigma') \to (q, \sigma'', -1)$
$R(q,1)$
$R(q'',n)$
$1, \sigma, q$
n, σ', q''
$W(q',2)$
$W(q,n-1)$
$1, \sigma'$
(to s_{n+1})(to s_0)
n, σ''
$R(q_{\text{halt}},n)$
$R(f_i),i\in[0;n]$
$R(\cdot,j),j\neq n$
$R(\#)$
$W(f_2)$
$W(f_0)$
s_0
$W(f_1)$
s_1
s_2
s_n
s_{n+1}
counting phase
$R(f_0)$
$R(f_1)$
$R(f_2)$
$R(f_{n-1})$
$R(f_n)$

Consequences

- Negative cut-off can be exponential.
- No clue about positive cut-off.

Upper bound ?

- Existence theorem gives a cut-off polynomial in the size of the basis of $\mathrm{Post}^*(\uparrow (q_0, d_0))$ and $\mathrm{Pre}^*(\uparrow q_f)$.
- Rackoff's theorem: $\mathrm{Pre}^*(\uparrow q_f)$ can be bounded by M doubly-exponential in $|\mathcal{P}|$.
- No bound on the Post^*.

Upper bound ?

- Existence theorem gives a cut-off polynomial in the size of the basis of $\mathrm{Post}^*(\uparrow (q_0, d_0))$ and $\mathrm{Pre}^*(\uparrow q_f)$.
- Rackoff's theorem: $\mathrm{Pre}^*(\uparrow q_f)$ can be bounded by M doubly-exponential in $|\mathcal{P}|$.
- No bound on the Post^*.
- Idea: refine the symbolic graph to keep track of up to M processes in each state.
- Such graph is still doubly-exponential in $|\mathcal{P}|$
- Guessing a path can be done in EXPSPACE.

Summary and Perspectives

- Simple model but still non-trivial model
- Non-atomicity ensures regularity hence decidability.

Summary and Perspectives

- Simple model but still non-trivial model
- Non-atomicity ensures regularity hence decidability.

- Other properties (is $\uparrow q_f = \{(q_f^k, d) \mid k, d\}$ an harder property ?)
- More registers, leader process.
- Hardness result with atomic operations ?
- Strategies
- Reasonable Polynomial upper-bound ?

Thank you for your attention