Reachability in Networks of Register Protocols under Stochastic Schedulers

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

Cassting ETAPS Workshop, 03/04/2016

Reachability in Register Protocols

Almost sure reachability

Cut-off constructions

Definition (Distributed protocol)

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

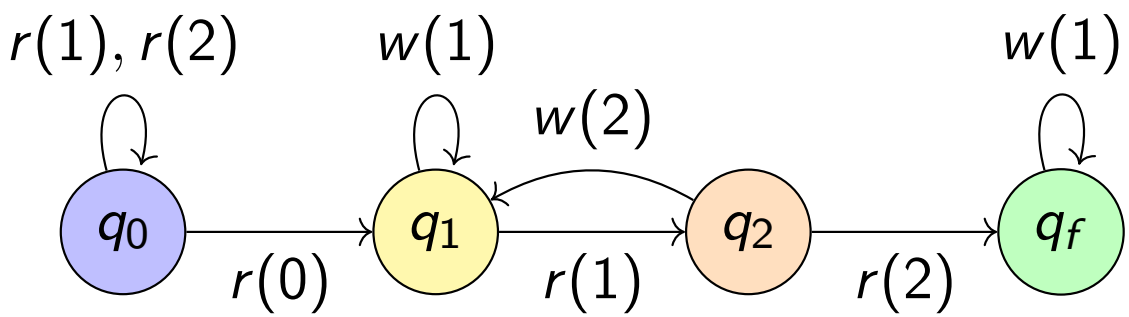
- Q: control states
- D: possible values of the register
- T: transitions of the form $p \xrightarrow{r(d)} q$ and $p \xrightarrow{w(d)} q$ for $p, q \in Q$, $d \in D$.

Definition (Distributed protocol)

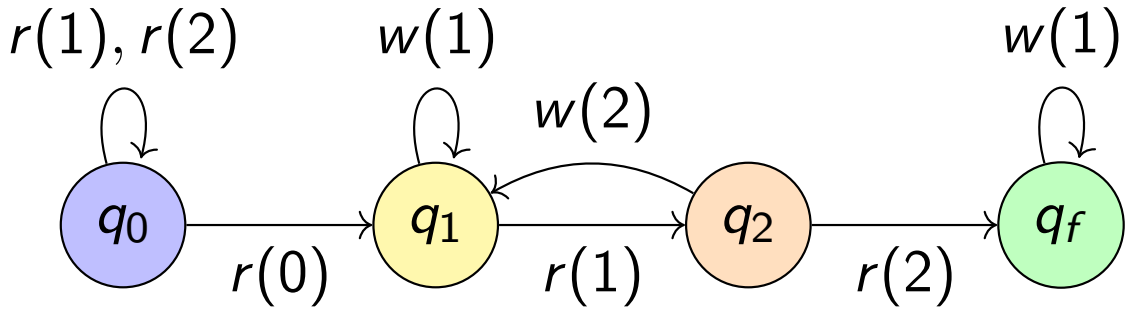
A distributed protocol is given by $\mathcal{P} = \langle Q, D, T \rangle$

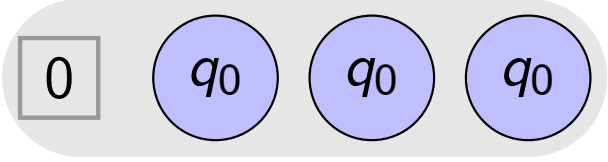
- Q: control states
- D: possible values of the register
- T: transitions of the form $p \xrightarrow{r(d)} q$ and $p \xrightarrow{w(d)} q$ for $p, q \in Q$, $d \in D$.

Example

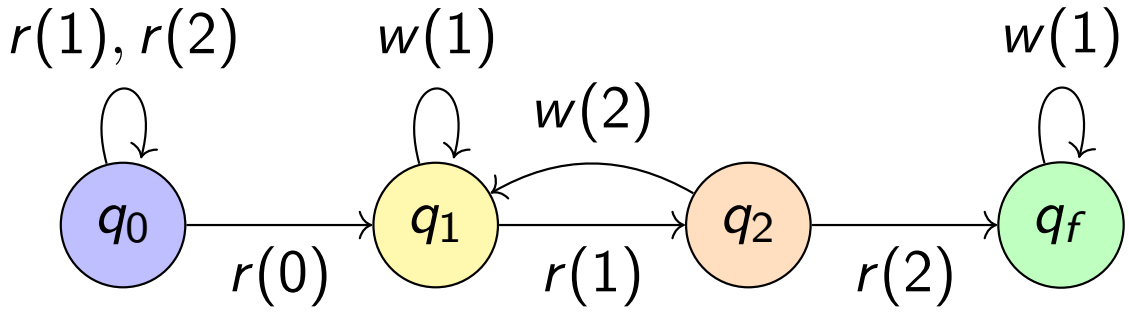


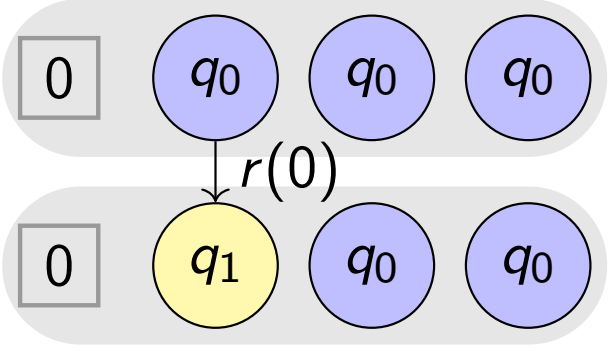
Semantics



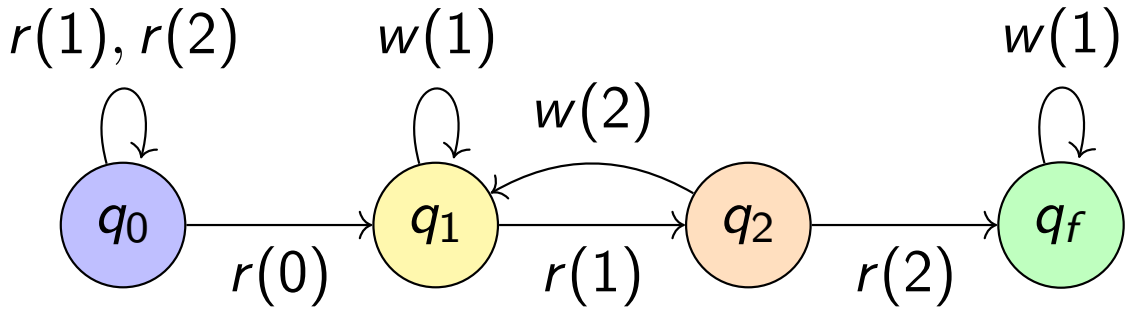


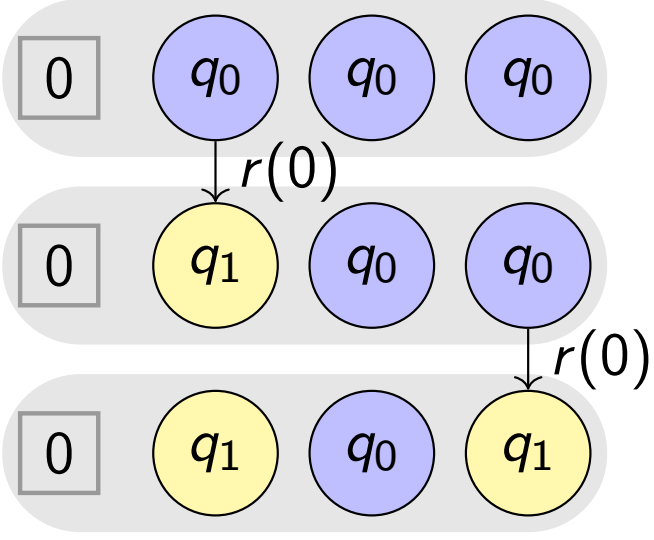
Semantics



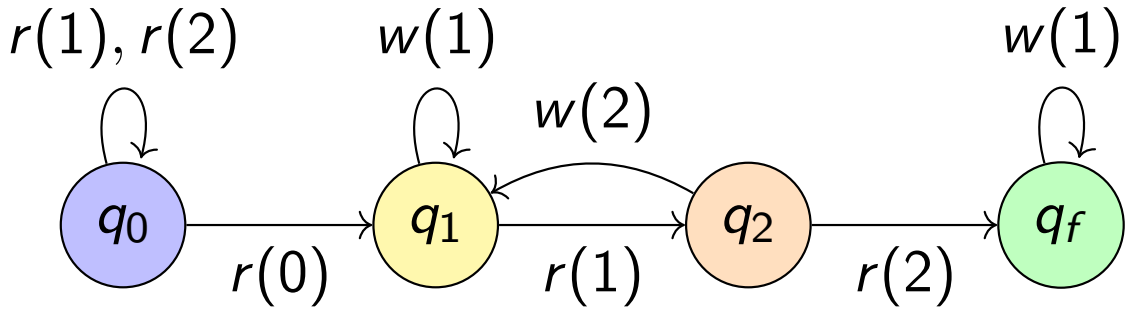


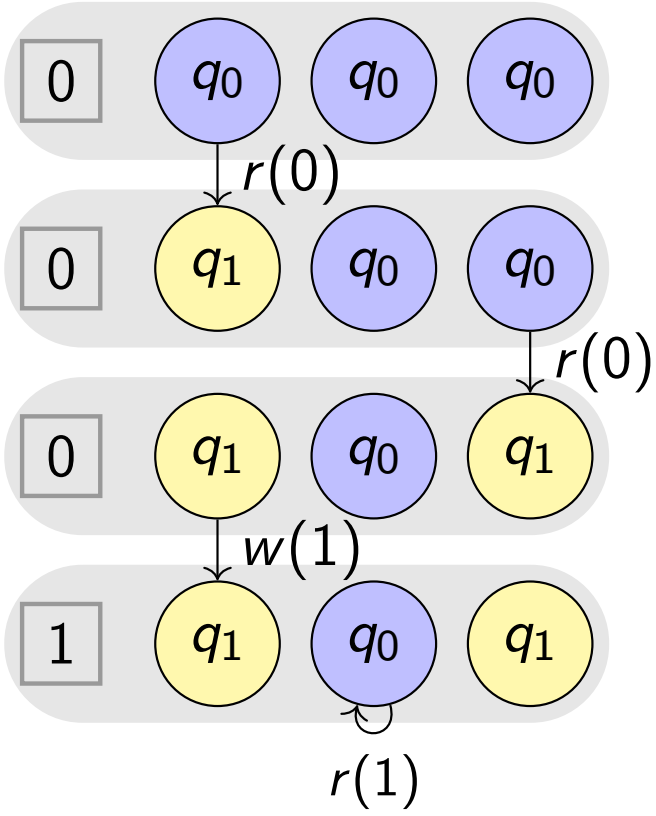
Semantics



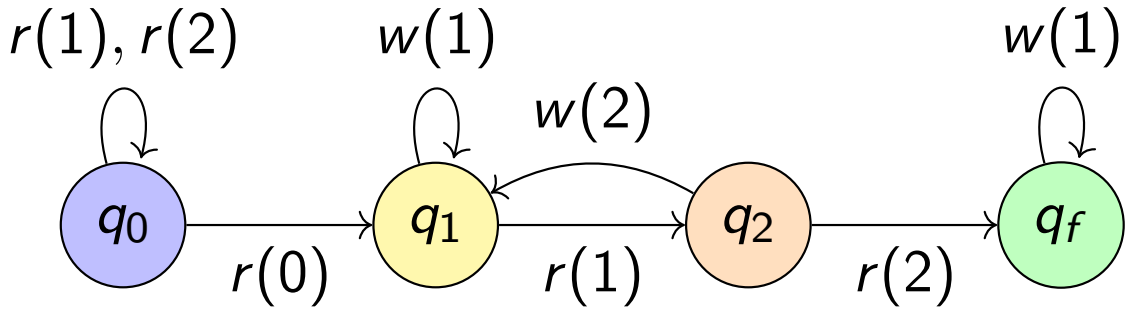


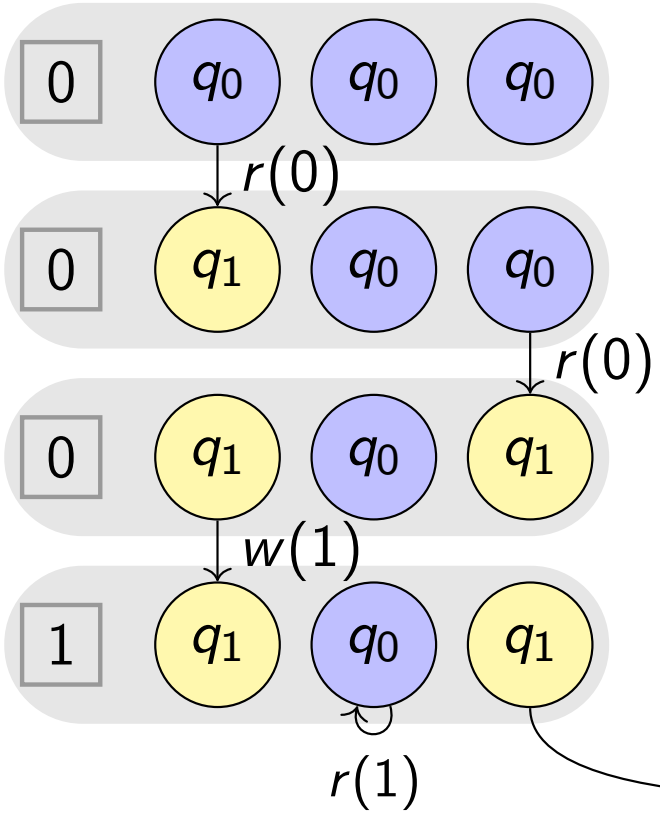
Semantics

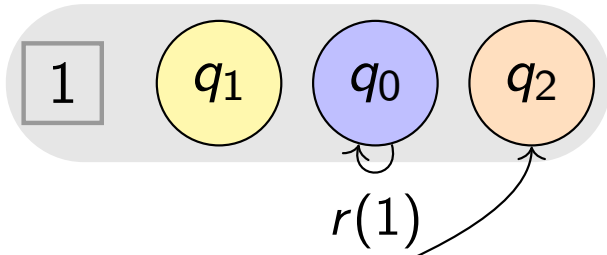

$r(1), r(2)$
$w(1)$
$w(1)$
$w(2)$
q_0
q_1
q_2
q_f
$r(0)$
$r(1)$
$r(2)$


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
$r(1)$

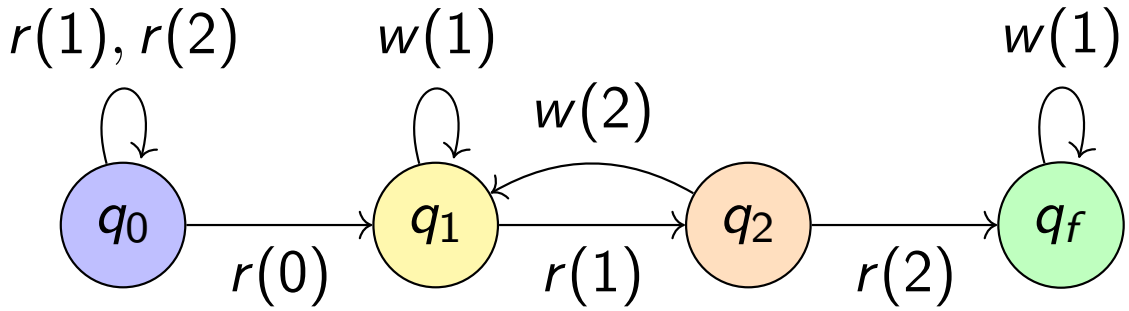
Semantics

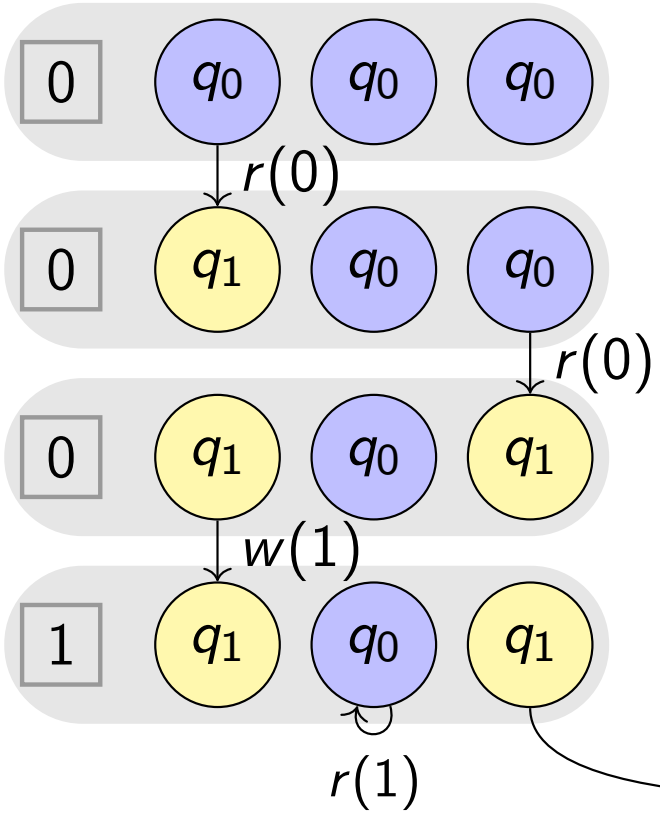

r(1), r(2)
w(1)
w(1)
w(2)
q0
q1
q2
qf
r(0)
r(1)
r(2)

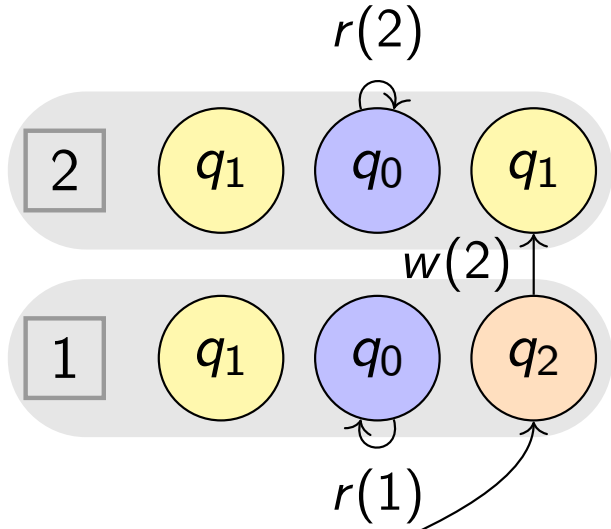

0
q0
q0
q0
r(0)
0
q1
q0
q0
r(0)
0
q1
q0
q1
w(1)
1
q1
q0
q1
r(1)
r(1)

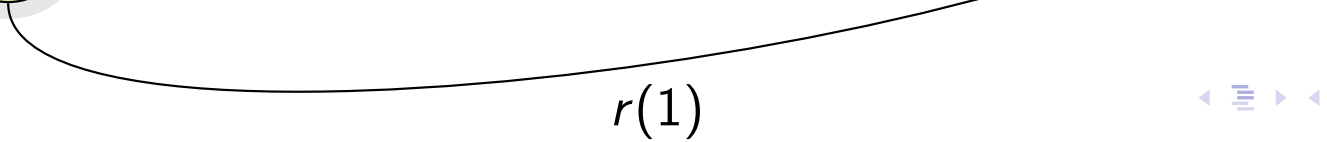

1
q1
q0
q2
r(1)

Semantics

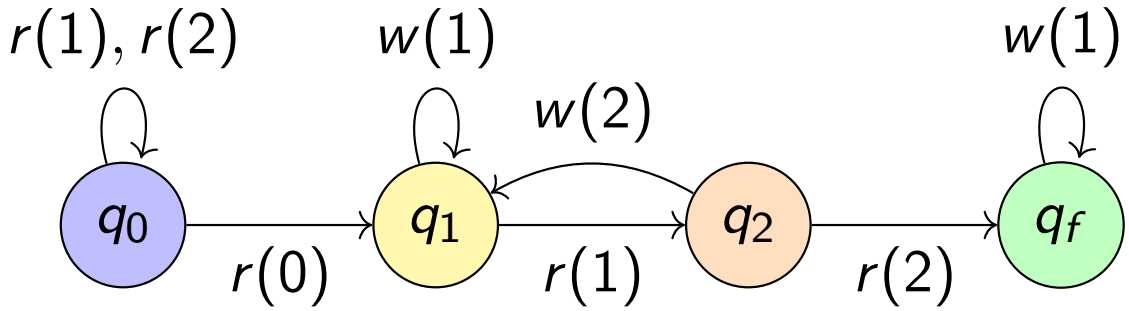

r(1), r(2)
w(1)
w(1)
w(2)
q0
q1
q2
qf
r(0)
r(1)
r(2)

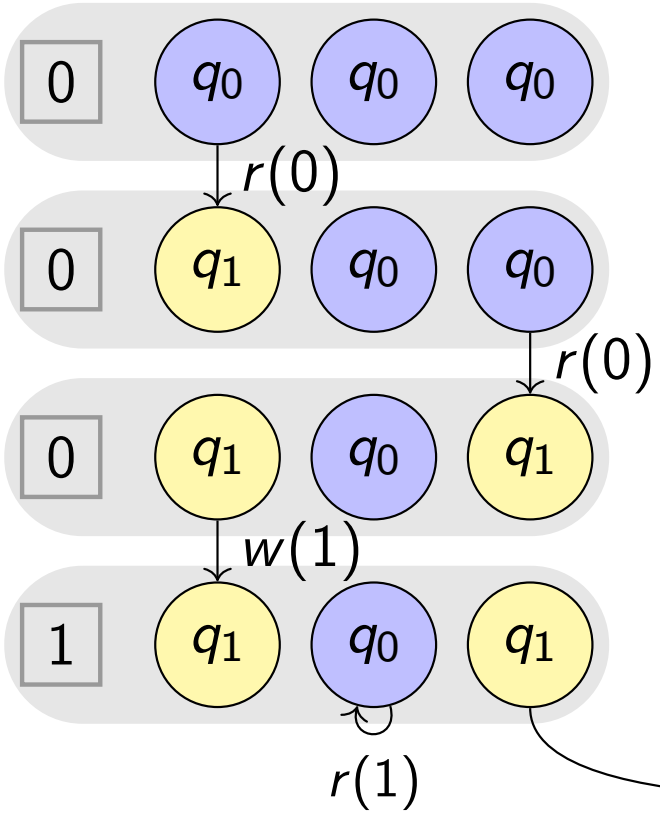

0
q0
q0
q0
r(0)
0
q1
q0
q0
r(0)
0
q1
q0
q1
w(1)
1
q1
q0
q1
r(1)

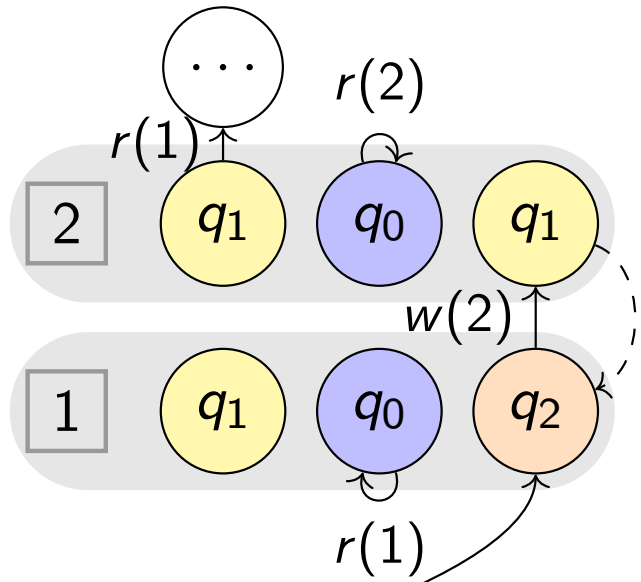

r(2)
2
q1
q0
q1
w(2)
1
q1
q0
q2
r(1)


r(1)

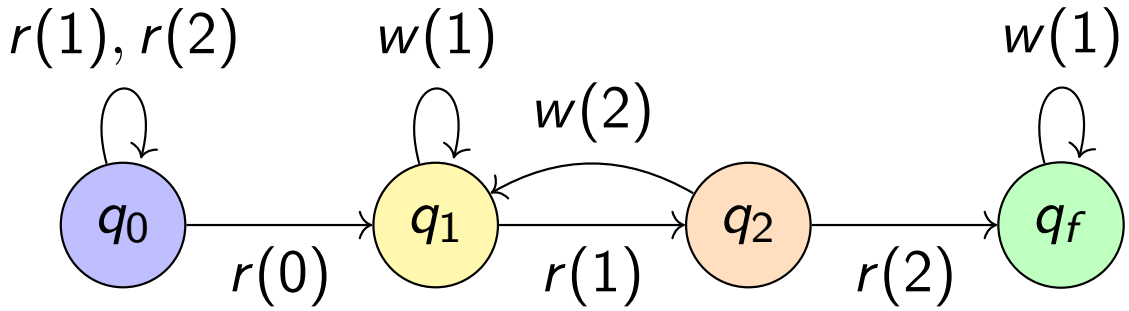
Semantics

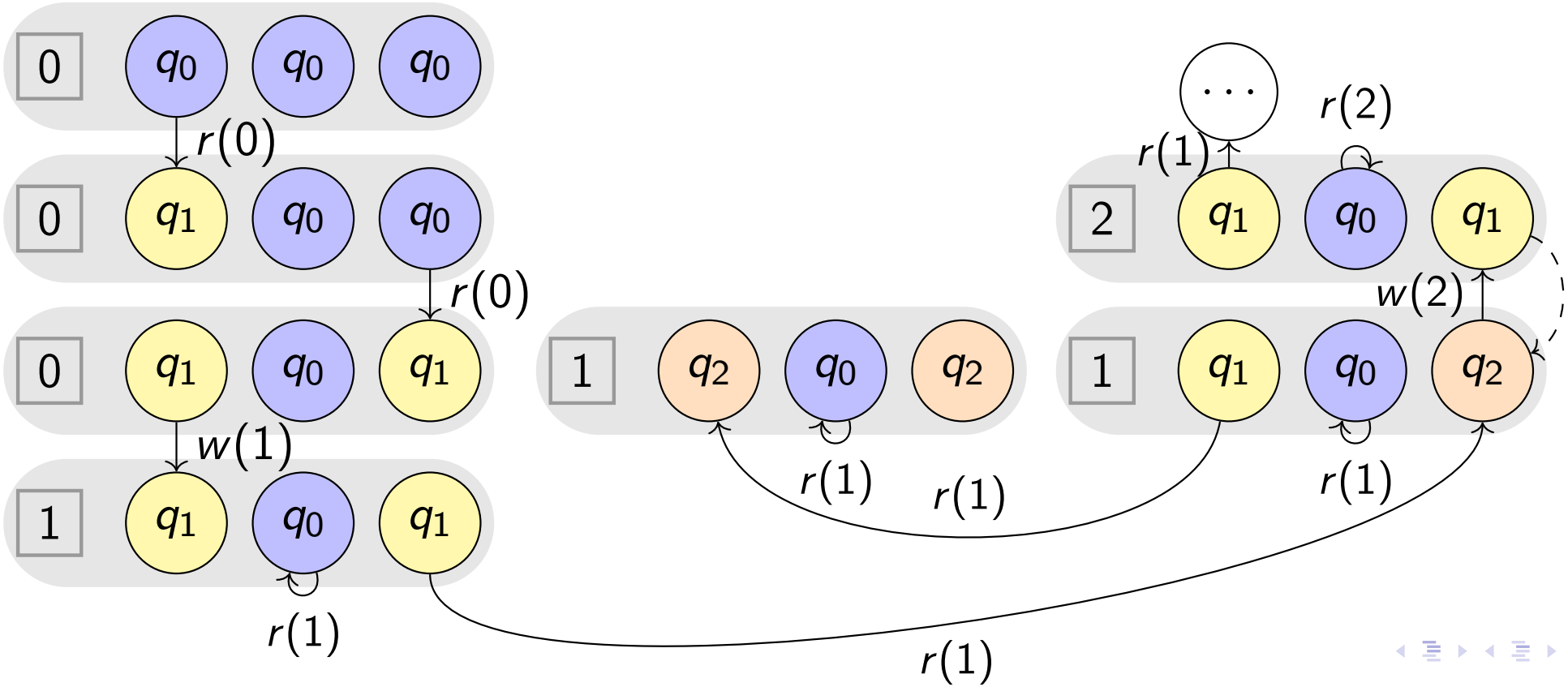

r(1), r(2)
w(1)
w(1)
w(2)
q0
q1
q2
qf
r(0)
r(1)
r(2)


0
q0
q0
q0
r(0)
0
q1
q0
q0
r(0)
0
q1
q0
q1
w(1)
1
q1
q0
q1
r(1)
r(1)

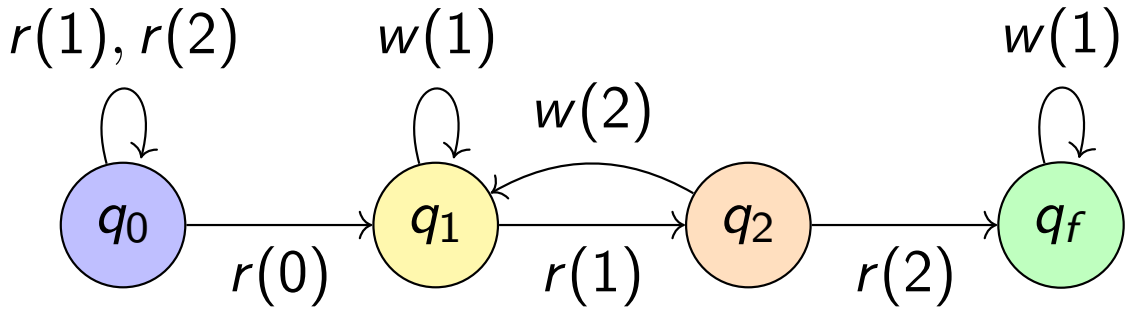

...
r(2)
r(1)
2
q1
q0
q1
w(2)
1
q1
q0
q2
r(1)

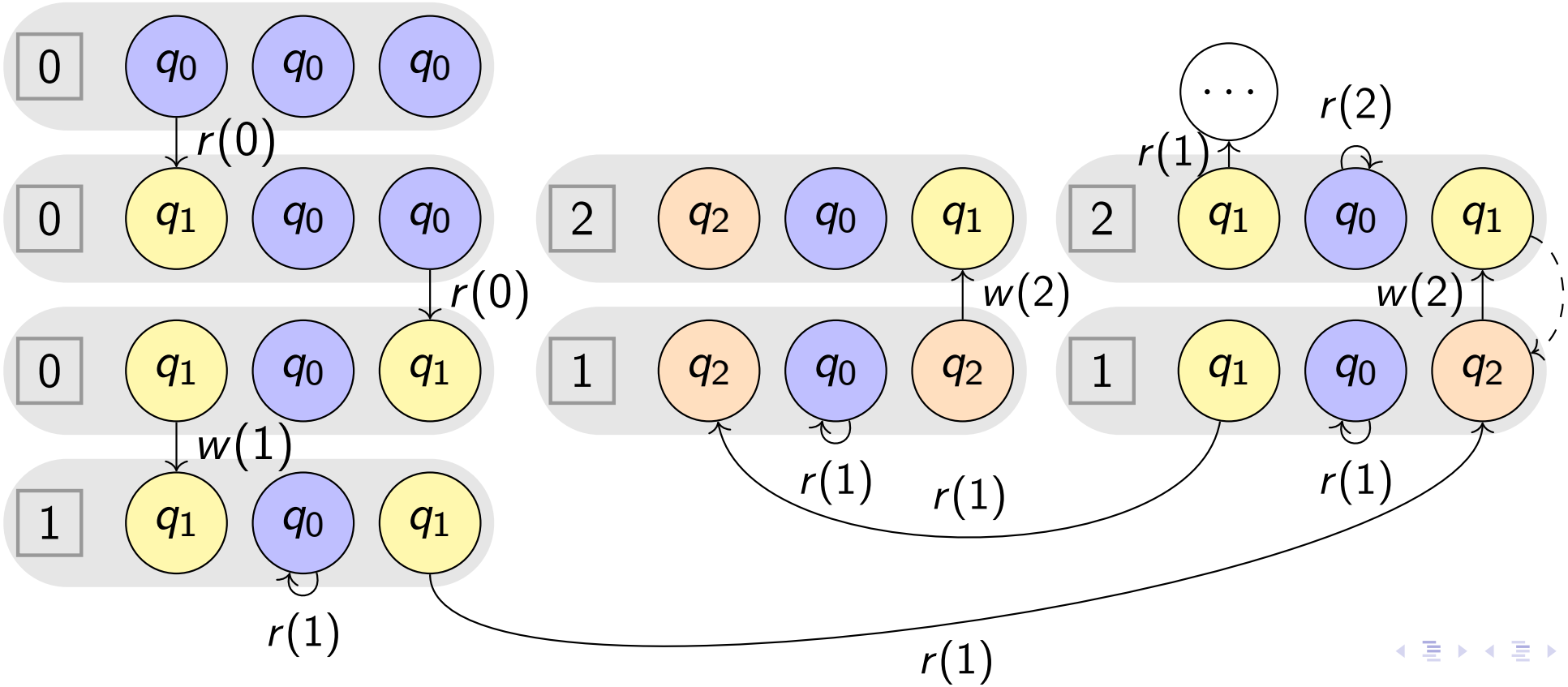
Semantics


r(1), r(2)
w(1)
w(1)
w(2)
q0
q1
q2
qf
r(0)
r(1)
r(2)

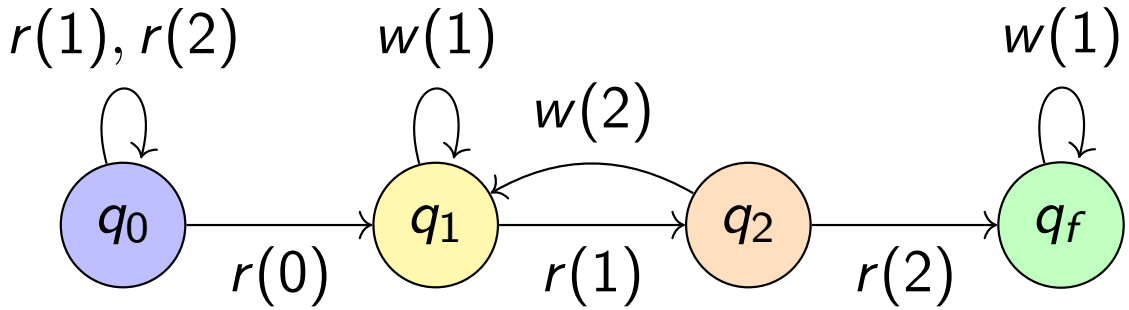

0
q0
q0
q0
r(0)
0
q1
q0
q0
r(0)
0
q1
q0
q1
w(1)
1
q1
q0
q1
r(1)
1
q2
q0
q2
r(1)
r(1)
...
r(1)
r(2)
2
q1
q0
q1
w(2)
1
q1
q0
q2
r(1)
r(1)

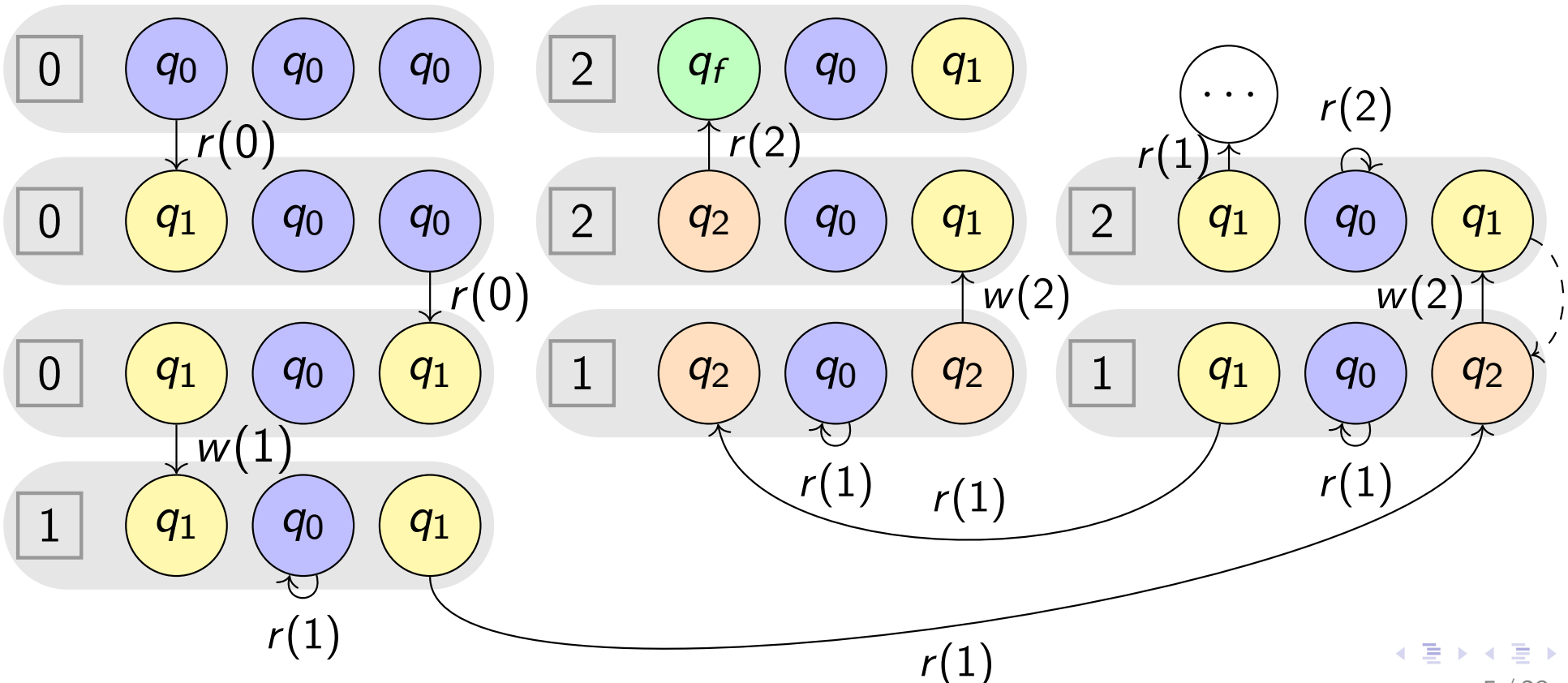
Semantics


r(1), r(2)
w(1)
w(2)
w(1)
q0
q1
q2
qf
r(0)
r(1)
r(2)


0
q0
q0
q0
r(0)
0
q1
q0
q0
r(0)
0
q1
q0
q1
w(1)
1
q1
q0
q1
r(1)
2
q2
q0
q1
w(2)
1
q2
q0
q2
r(1)
r(1)
...
r(1)
r(2)
2
q1
q0
q1
w(2)
1
q1
q0
q2
r(1)
r(1)

Semantics


r(1), r(2)
w(1)
w(2)
w(1)
q0
q1
q2
qf
r(0)
r(1)
r(2)


0
q0
q0
q0
r(0)
0
q1
q0
q0
r(0)
0
q1
q0
q1
w(1)
1
q1
q0
q1
r(1)
2
qf
q0
q1
r(2)
2
q2
q0
q1
w(2)
1
q2
q0
q2
r(1)
r(1)
r(1)
r(2)
r(1)
2
q1
q0
q1
w(2)
1
q1
q0
q2
r(1)
r(1)

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)
- $\mathrm{Pre}(X)$, $\mathrm{Post}(X)$
- $+$, $-$ 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)
- $\mathrm{Pre}(X)$, $\mathrm{Post}(X)$
- $+$, $-$ 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)

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 $\langle q_0^{|\gamma|}, d_0 \rangle$?

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 $\langle q_l + q_0^{|\gamma|-1}, d_0 \rangle$?

- 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)

We construct G_{symb} from the initial transition system by abstraction on the number of copies in each state.

$$\gamma \mapsto \overline{S}(\gamma) = (v(\gamma), \{q \mid \gamma(q) > 0\})$$

Symbolic graph

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

Definition (Symbolic graph)

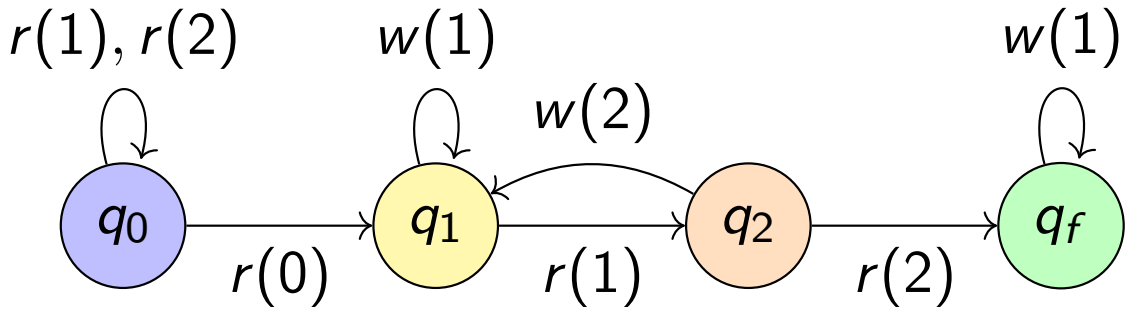
We construct G_{symb} from the initial transition system by abstraction on the number of copies in each state.

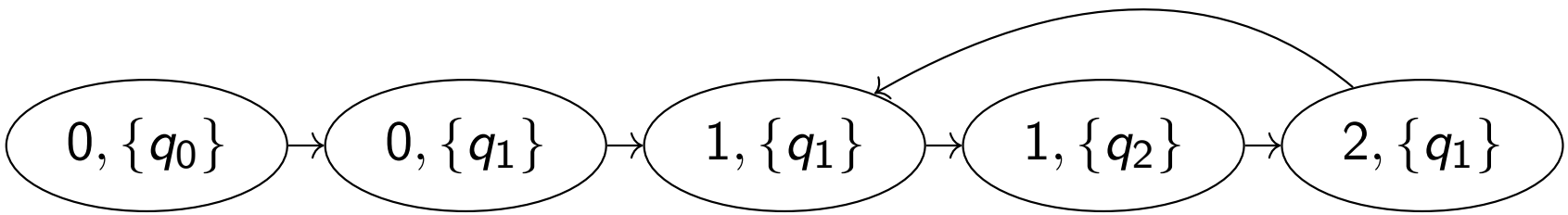
$$\gamma \mapsto \overline{S}(\gamma) = (v(\gamma), \{q \mid \gamma(q) > 0\})$$

Lemma

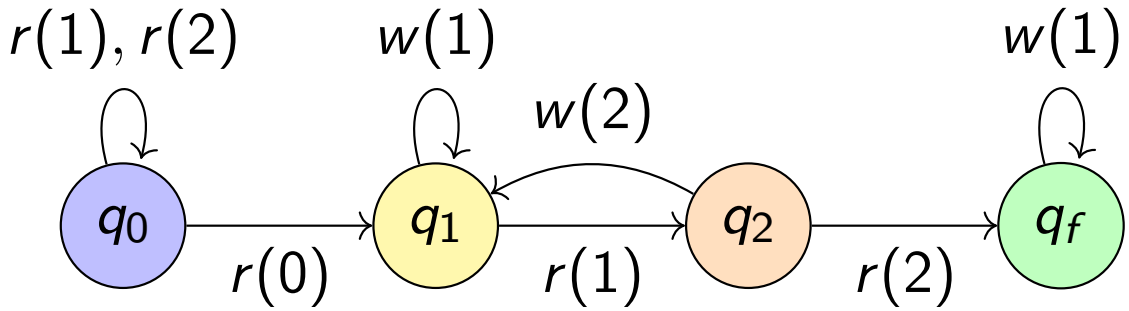
Every "concrete" run of $\mathcal{P}$ corresponds to a symbolic run. And we can reconstruct a concrete run by adding enough copies.

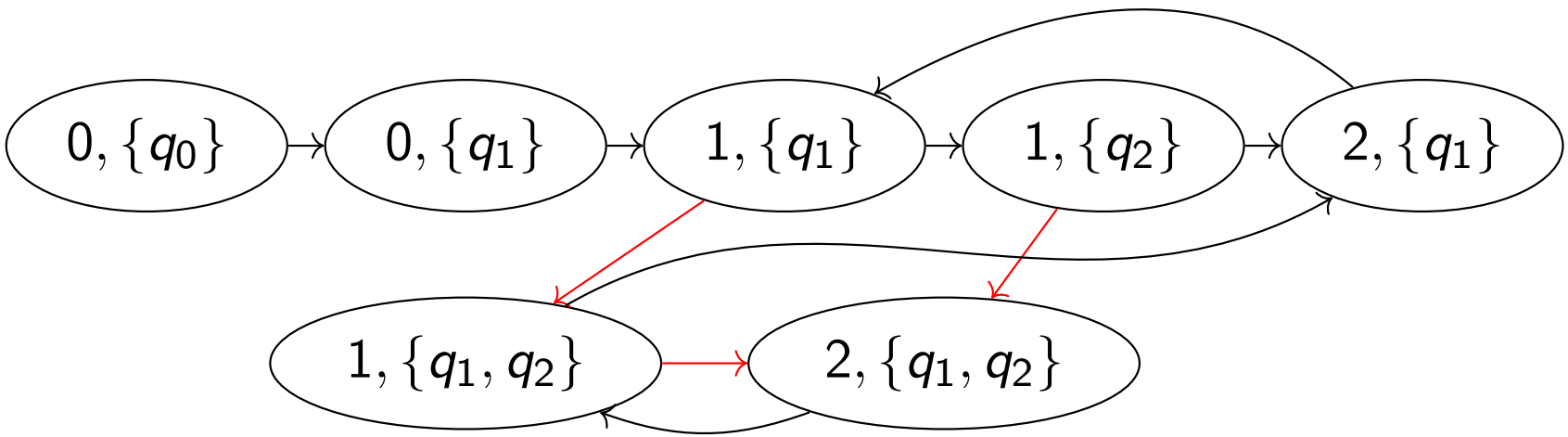
Example



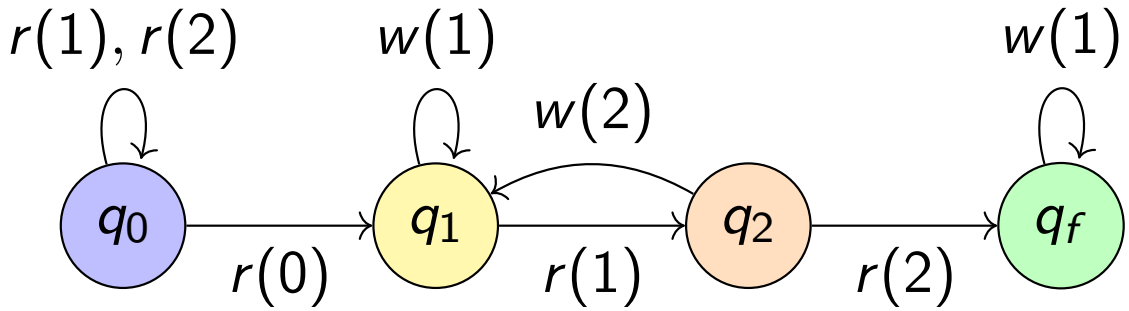


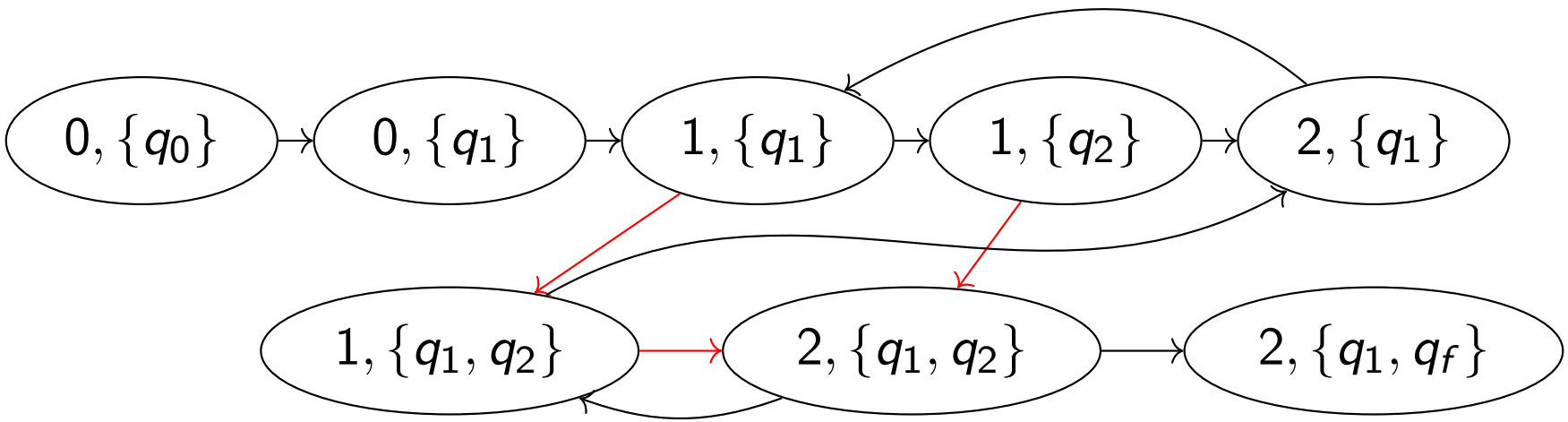
Example



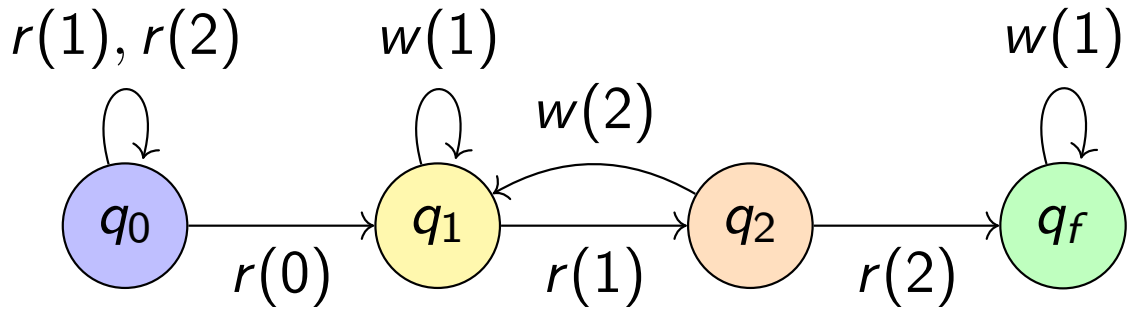


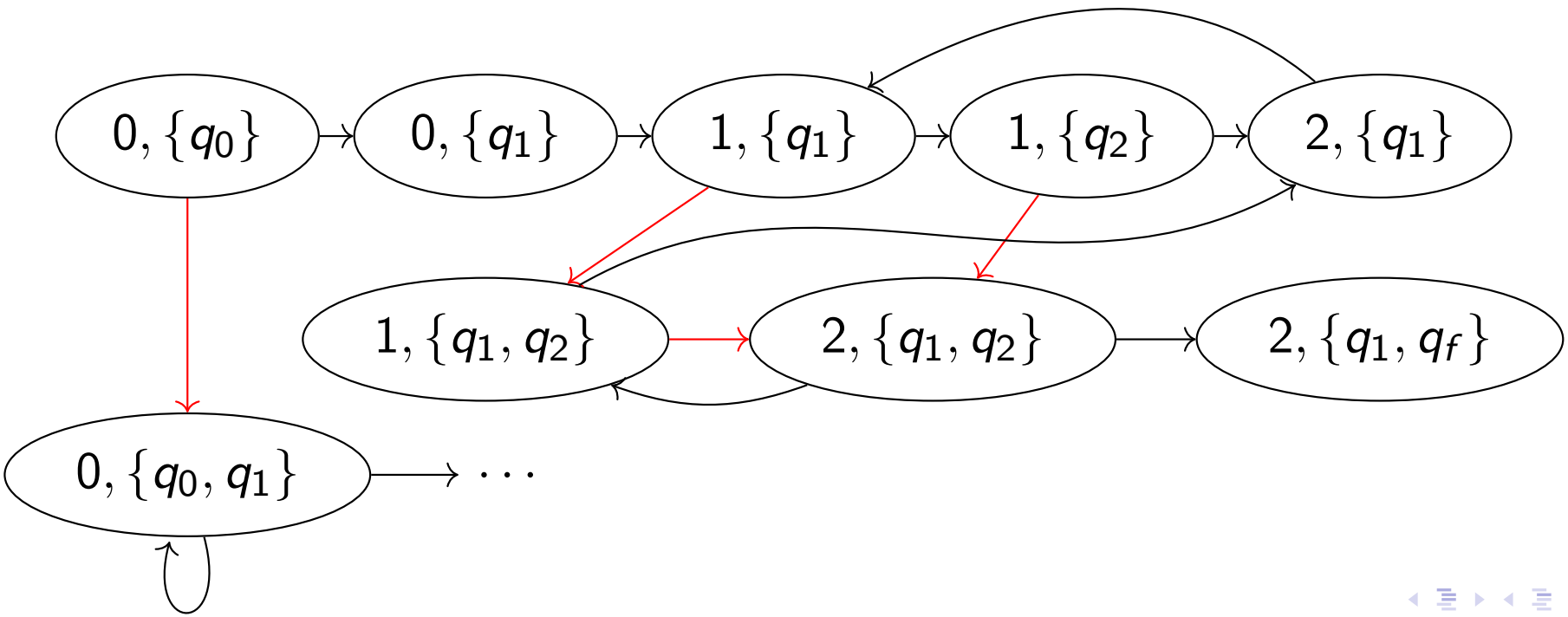
Example


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

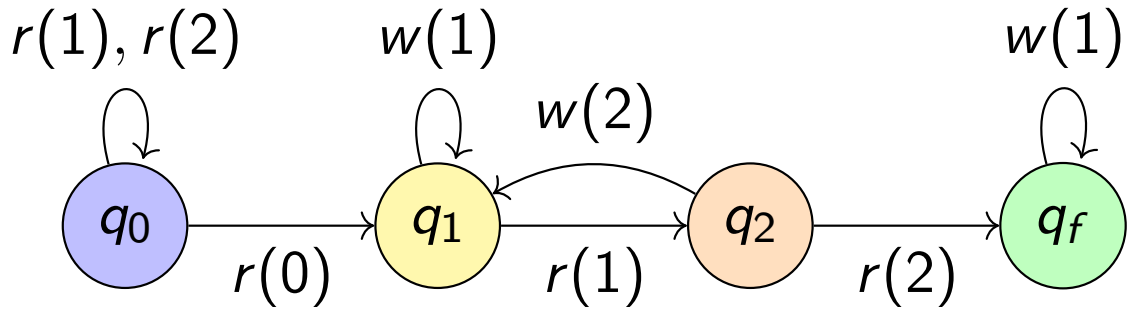

$0, \{q_0\}$
$0, \{q_1\}$
$1, \{q_1\}$
$1, \{q_2\}$
$2, \{q_1\}$
$1, \{q_1, q_2\}$
$2, \{q_1, q_2\}$
$2, \{q_1, q_f\}$

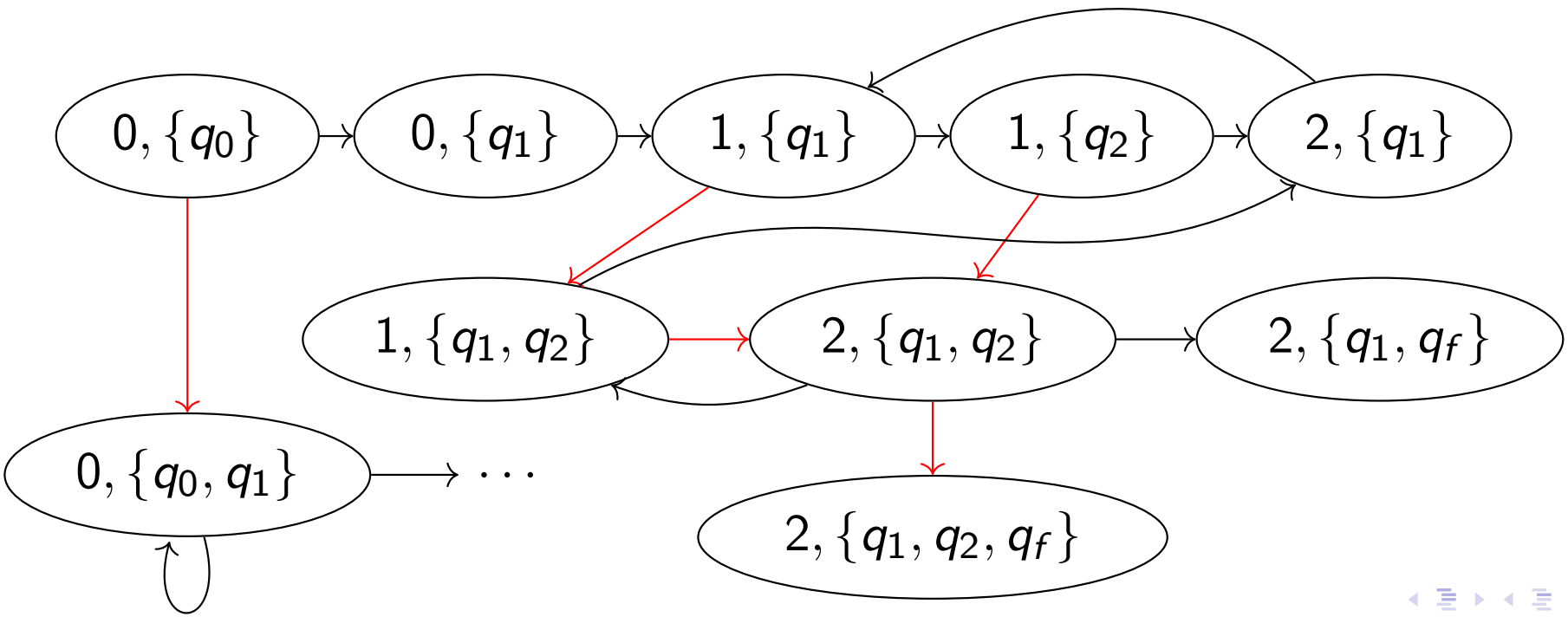
Example


r(1), r(2)
w(1)
w(2)
w(1)
q0
q1
q2
qf
r(0)
r(1)
r(2)


0, {q0}
0, {q1}
1, {q1}
1, {q2}
2, {q1}
1, {q1, q2}
2, {q1, q2}
2, {q1, qf}
0, {q0, q1}
· · ·

Example


r(1), r(2)
w(1)
w(2)
w(1)
q0
q1
q2
qf
r(0)
r(1)
r(2)


0, {q0}
0, {q1}
1, {q1}
1, {q2}
2, {q1}
1, {q1, q2}
2, {q1, q2}
2, {q1, qf}
0, {q0, q1}
...
2, {q1, q2, qf}

What the symbolic graph taught us

Theorem

Every path in G_{symb} can be transformed to have less than $4|Q| + 1$ transitions.

What the symbolic graph taught us

Theorem

Every path in G_{symb} can be transformed to have less than $4|Q| + 1$ transitions.

Theorem

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

What the symbolic graph taught us

Theorem

Every path in G_{symb} can be transformed to have less than $4|Q| + 1$ transitions.

Theorem

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

Theorem (J. Esparza, P. Ganty, and R. Majumdar., 2013)

The reachability problem with leader is NP-complete.

Reachability in Register Protocols

Almost sure reachability

- Probabilistic semantics
- Cut-off property

Cut-off constructions

Markov Chain

Definition (Law of motion)

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

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

Markov Chain

Definition (Law of motion)

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

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

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) (leader-less case).

Markov Chain

Definition (Law of motion)

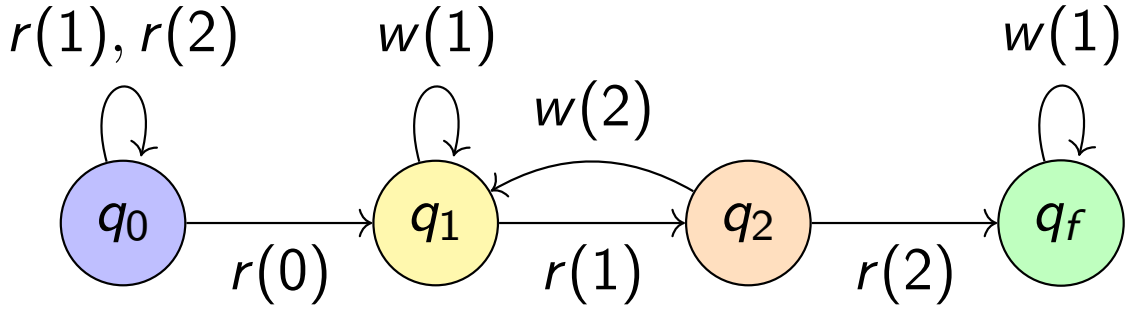
We consider $(\Gamma, \rightarrow)$ as a Markov Chain.

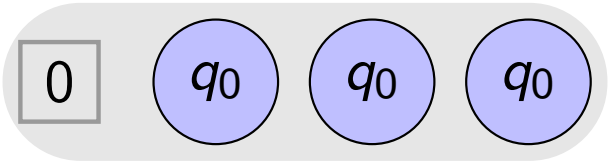
$$\forall \gamma' \in \mathrm{Post}(\gamma) \;\; \Pr(\gamma \rightarrow \gamma') = \frac{1}{|\mathrm{Post}(\gamma)|}$$

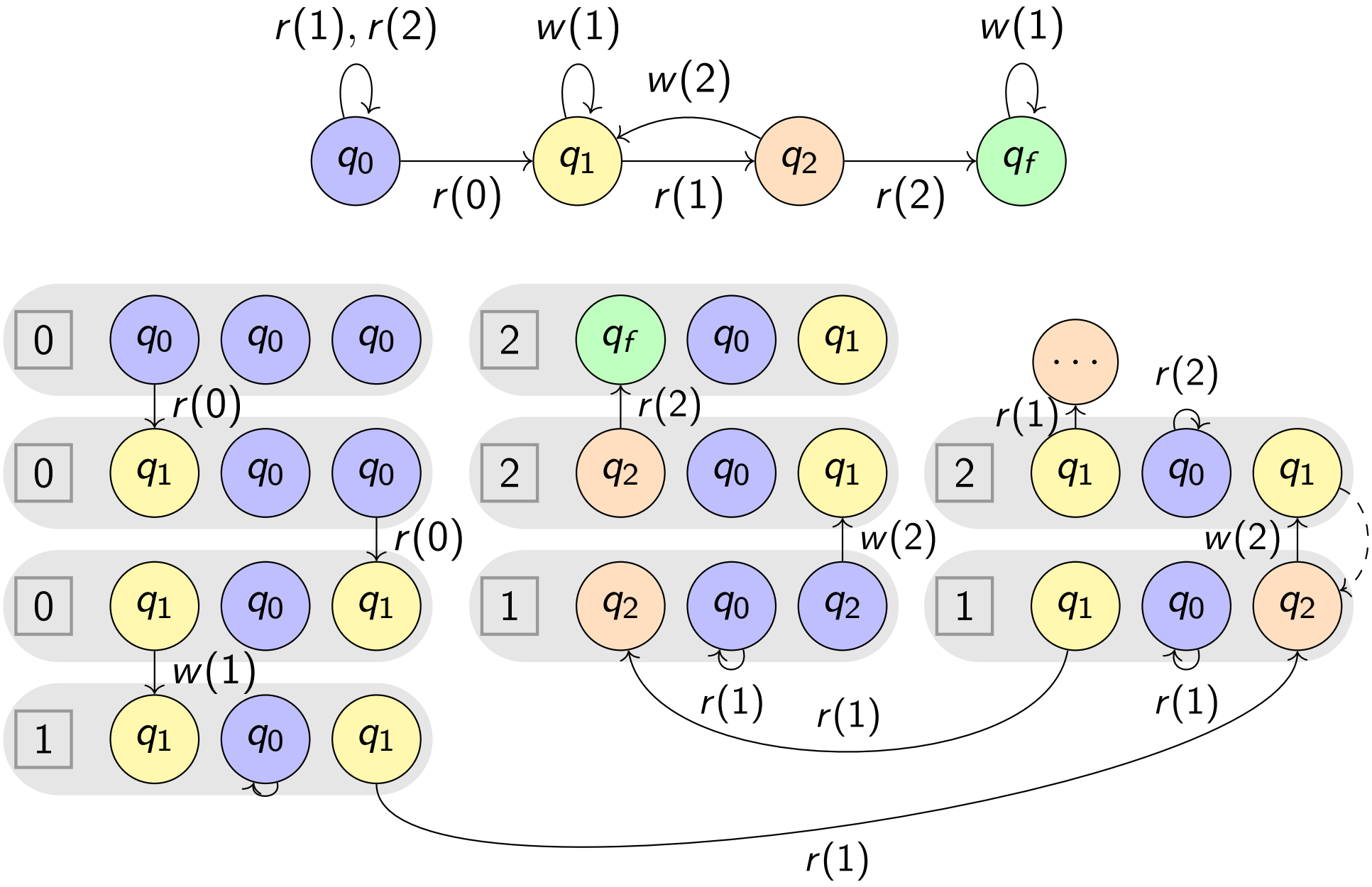
Let $(q_0, d_0) \in Q \times D$, a parameter n.
For $X \subseteq \Gamma$, we denote $\mathbb{P}^n(X)$ the probability to eventually reach some $\gamma \in X$ from (q_0^n, d_0) (leader-less case).

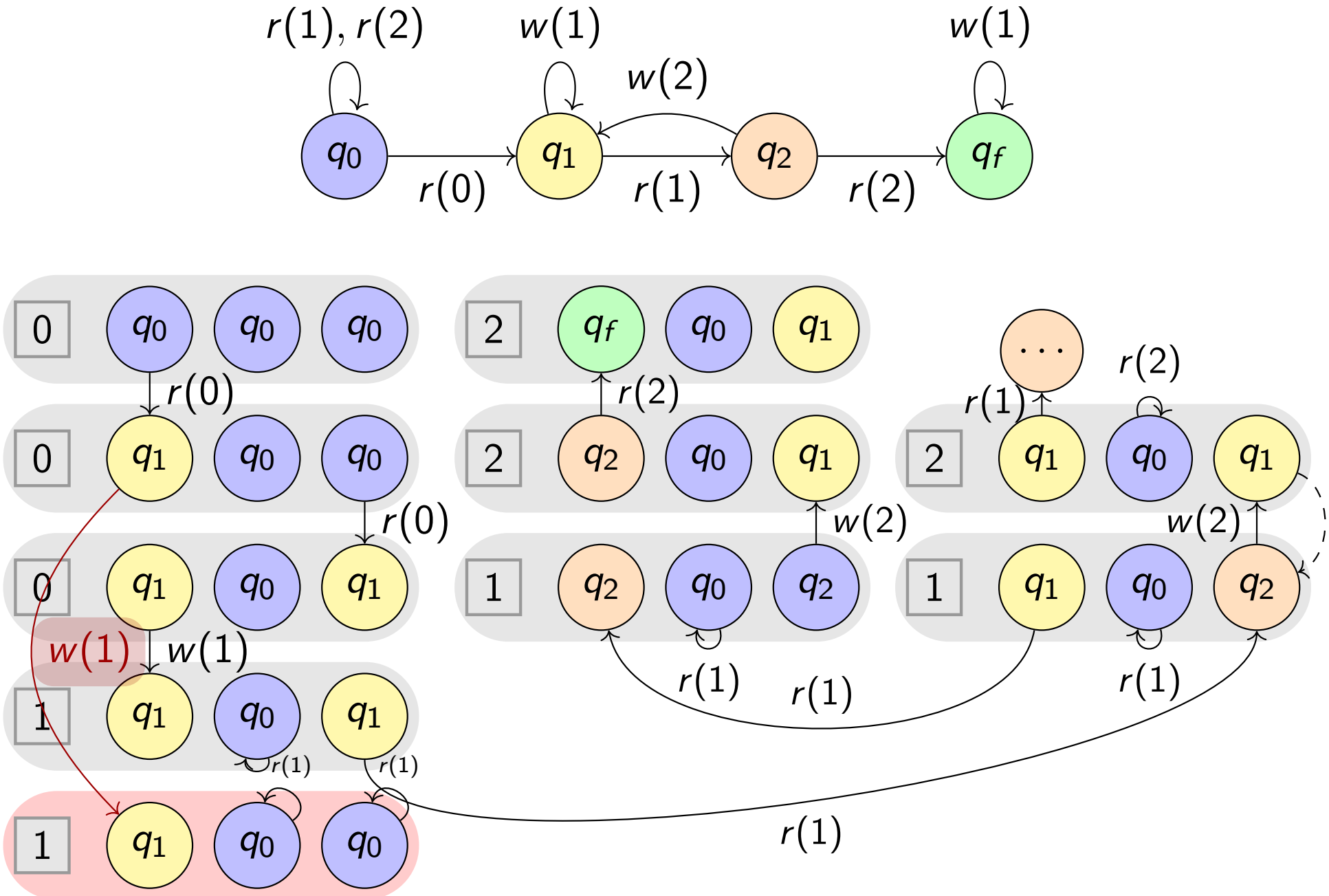
Qualitative goal

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


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


0
q_0
q_0
q_0


r(1), r(2)
w(1)
w(1)
w(2)
q0
q1
q2
qf
r(0)
r(1)
r(2)
0
2
1
r(0)
r(2)
w(2)
w(1)
r(1)
r(1)
r(1)
r(2)
r(1)
w(2)
r(1)
r(1)
...


r(1), r(2)
w(1)
w(2)
w(1)
q0
q1
q2
qf
r(0)
r(1)
r(2)
0
2
1
r(0)
r(2)
r(1)
r(2)
w(2)
w(2)
w(1)
w(1)
r(1)
r(1)
r(1)
r(1)
r(1)
r(1)

Remarks

Lemma (Qualitative assumption)

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

Remarks

Lemma (Qualitative assumption)

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

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* $\mathbb{P}^n(\uparrow q_f) = 1$ *do not depend on the actual distributions.*

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

- We focus now on the almost-sure ($\mathbb{P}^n(\uparrow q_f) = 1$ problem).
- Both the scheduler and processes are stochastic
- No atomicity
- No monotonicity a priori.

Discretization

Lemma

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

Discretization

Lemma

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

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

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.

- positive $\forall n \geq N \ \mathbb{P}^n(\uparrow q_f) = 1$
- negative $\forall n \geq N \ \mathbb{P}^n(\uparrow q_f) < 1$
- Non-atomicity is crucial.

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 based on well-quasi-orders
- The bound is polynomial ...

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 based on well-quasi-orders
- The bound is polynomial ...
- ... in the size of the elements of $\min \mathrm{Post}^*(\uparrow (q_0, d_0))$ and $\min \mathrm{Pre}^*(\uparrow q_f)$
- How to effeciently decide the type of the cut-off ?

Negative cut-off: the easy case

Remark

Almost-sure reachability in the concrete system implies Almost-sure reachability in G_{symb}.

Negative cut-off: the easy case

Remark

Almost-sure reachability in the concrete system implies Almost-sure reachability in G_{symb}.

The converse is not true

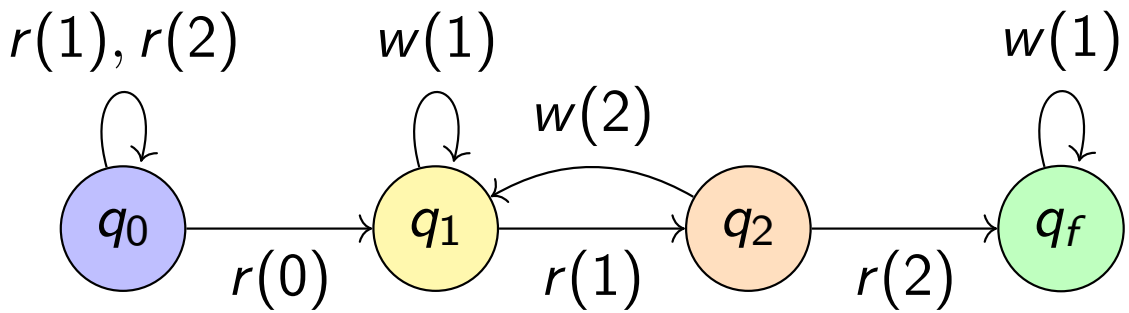
Negative cut-off: the easy case

Remark

Almost-sure reachability in the concrete system implies Almost-sure reachability in G_{symb}.

The converse is not true

Example



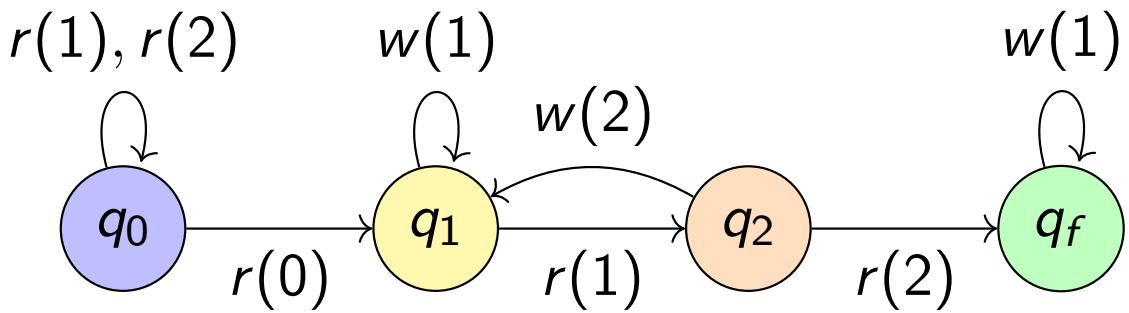
Negative cut-off: the easy case

Remark

Almost-sure reachability in the concrete system implies Almost-sure reachability in G_{symb}.

The converse is not true

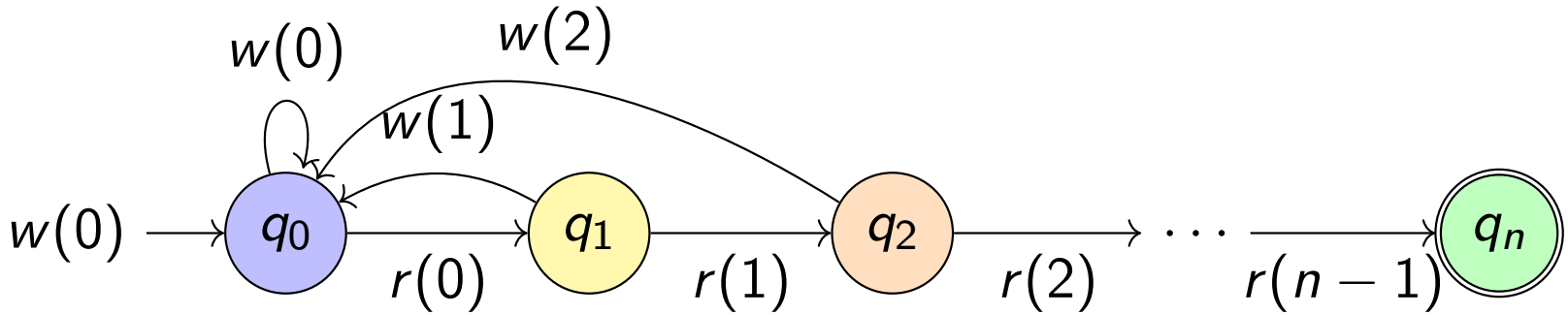
Example



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

Linear example

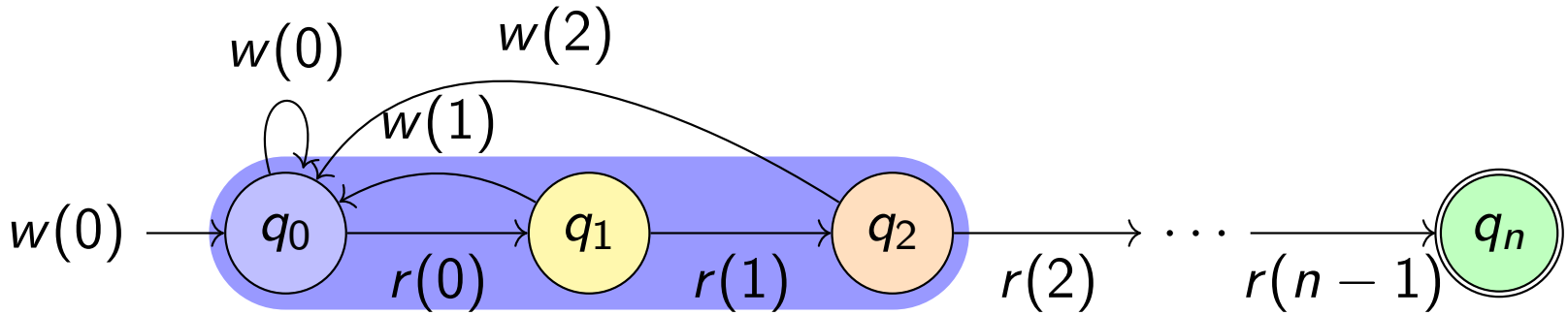
Example



Cut-off value ?

Linear example

Example

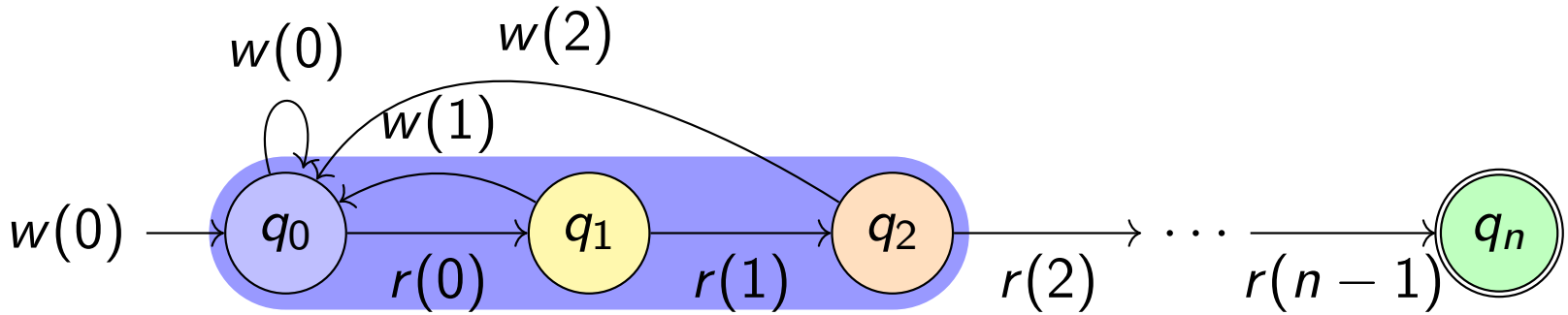


Cut-off value ?
Invariant (with m initial processes):

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

Linear example

Example



Cut-off value ? The cut-off is positive and equals n.
Invariant (with m initial processes):

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

Consequences

- Checking that few processes are in the same set of states
- Main tool to ensure proper encodings with negative cut-offs.

Consequences

- Checking that few processes are in the same set of states
- Main tool to ensure proper encodings with negative cut-offs.
- We can encode a n-bits counter (exponential size negative cut-offs).
- Can encode a linearly-bounded Turing Machine

Decision Problem

- INPUT: a protocol $\mathcal{P}$, $q_0, q_f \in Q$ and $d_0 \in D$.
- OUTPUT: whether the cut-off is positive or negative.

The cut-off decision problem is PSPACE-hard.

Upper bound ?

- Rackoff's theorem: $\min \mathrm{Pre}^*(\uparrow q_f)$ can be bounded by M doubly-exponential in $|\mathcal{P}|$.
- No bound on the $\min \mathrm{Post}^*(\uparrow (q_0, d_0))$.

Upper bound ?

- Rackoff's theorem: $\min \mathrm{Pre}^*(\uparrow q_f)$ can be bounded by M doubly-exponential in $|\mathcal{P}|$.
- No bound on the $\min \mathrm{Post}^*(\uparrow (q_0, d_0))$.
- Idea: refine the symbolic graph to keep track of up to M processes.

Theorem

Deciding whether the cut-off is positive can be done in EXPSPACE.

Summary and Perspectives

Summary and Perspectives

- Almost sure reachability without leader: always a cut-off value.
- At least linear in the (worst) **positive** case.
- At least exponential in the (worst) **negative** case.
- The decision problem is PSPACE hard and in EXPSPACE.

Summary and Perspectives

- Almost sure reachability without leader: always a cut-off value.
- At least linear in the (worst) **positive** case.
- At least exponential in the (worst) **negative** case.
- The decision problem is PSPACE hard and in EXPSPACE.

- What happens with atomic operations ?
- More registers, leader process.
- Other properties (safety, LTL, limit-sure)
- (Local) Strategy synthesis ?

Summary and Perspectives

- Almost sure reachability without leader: always a cut-off value.
- At least linear in the (worst) **positive** case.
- At least exponential in the (worst) **negative** case.
- The decision problem is PSPACE hard and in EXPSPACE.

- What happens with atomic operations ?
- More registers, leader process.
- Other properties (safety, LTL, limit-sure)
- (Local) Strategy synthesis ?

Thank you for your attention