Cut-off properties in asynchronous probabilistic distributed protocol

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

Sixth Cassting Meeting 2015

Definition (Distributed protocol)

A distributed protocol is given by $\mathcal{P} = \langle Q, D, (q_0, d_0), T, q_f \rangle$

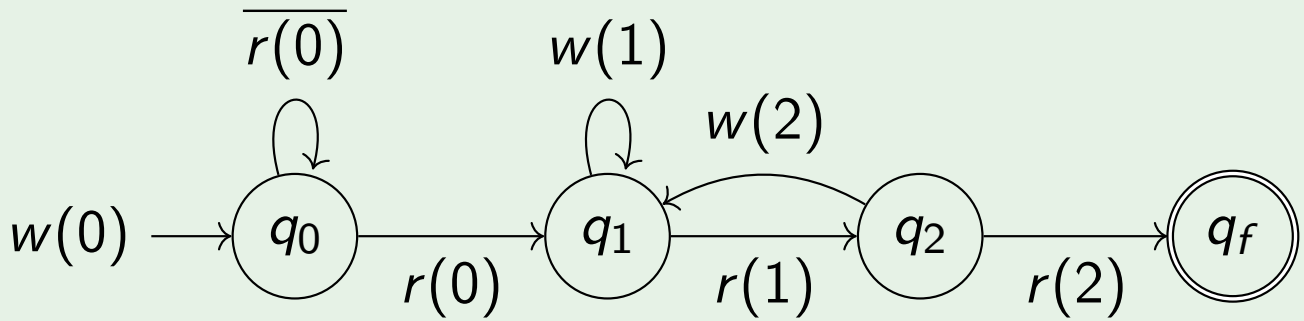
- Q: control states
- D: possible values of the register
- $(q_0, d_0) \in Q \times D$: initial state with an initial value
- T: transitions of the form $p \xrightarrow{r(d)} q$ and $p \xrightarrow{w(d)} q$ for $p, q \in Q$, $d \in D$.
- q_f: final state

Definition (Distributed protocol)

A distributed protocol is given by $\mathcal{P} = \langle Q, D, (q_0, d_0), T, q_f \rangle$

- Q: control states
- D: possible values of the register
- $(q_0, d_0) \in Q \times D$: initial state with an initial value
- T: transitions of the form $p \xrightarrow{r(d)} q$ and $p \xrightarrow{w(d)} q$ for $p, q \in Q$, $d \in D$.
- q_f: final state

Example



Definition (Configuration of the protocol)

$$\gamma = (f, d)$$

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

Definition (Configuration of the protocol)

$$\gamma = (f, d)$$

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

Definition (Semantics)

$(f, d) \to (f', d')$ if $f' = f - q + q'$ with either

- $q \xrightarrow{w(d')} q'$
- or $d = d'$ and $q \xrightarrow{r(d)} q'$

Markov Chain

Definition (Law of motion)

Let $\mathrm{Succ}(\gamma) = \{\gamma' \mid \gamma \to \gamma'\}$ and let fix $\mathcal{U}(\gamma)$ a distribution with support $\mathrm{Succ}(\gamma)$.

Markov Chain

Definition (Law of motion)

Let $\mathrm{Succ}(\gamma) = \{\gamma' \mid \gamma \to \gamma'\}$ and let fix $\mathcal{U}(\gamma)$ a distribution with support $\mathrm{Succ}(\gamma)$. For a fixed $n \in \mathbb{N}$, the system is a Markov Chain with initial state (q_0^n, d_0).

Markov Chain

Definition (Law of motion)

Let $\mathrm{Succ}(\gamma) = \{\gamma' \mid \gamma \to \gamma'\}$ and let fix $\mathcal{U}(\gamma)$ a distribution with support $\mathrm{Succ}(\gamma)$. For a fixed $n \in \mathbb{N}$, the system is a Markov Chain with initial state (q_0^n, d_0). We denote $\mathbb{P}_n(\gamma)$ the probability to eventually reach γ.

Qualitative goal

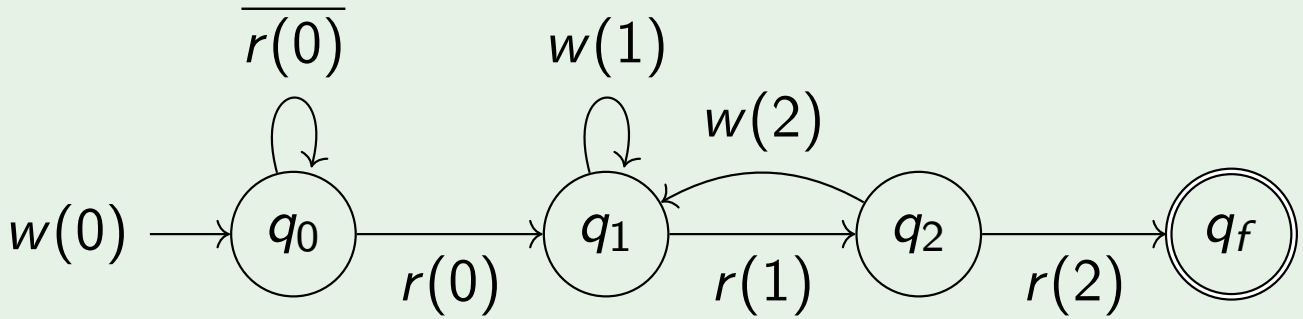
Estimate $\mathbb{P}_n(\diamond q_f)$ $(\diamond q_f = \{\gamma \mid \gamma(q_f) > 0\})$

Markov Chain

Qualitative goal

Estimate $\mathbb{P}_n(\diamond q_f)$ $(\diamond q_f = \{\gamma \mid \gamma(q_f) > 0\})$

Example



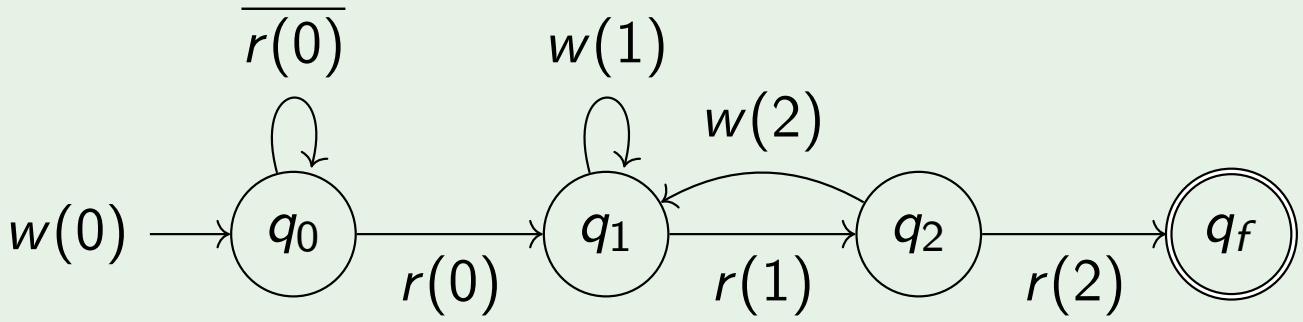
$$\longrightarrow 0, q_0^3 \longrightarrow 0, q_0^2 q_1 \to 0, q_0^1 q_1^2 \longrightarrow 0, q_1^3 \longrightarrow 1, q_1^3 \longrightarrow 1, q_1^2 q_2 \to 1, q_1 q_2^2$$

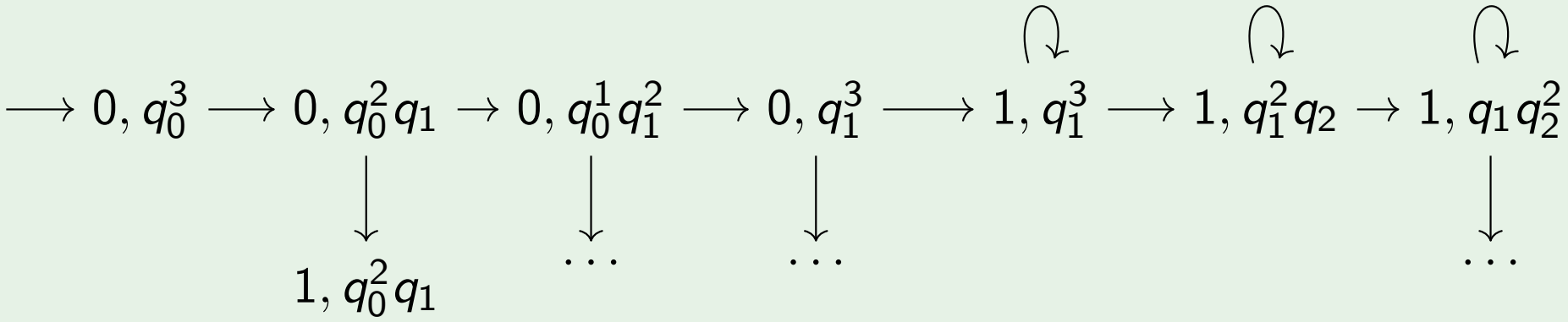
Markov Chain

Qualitative goal

Estimate $\mathbb{P}_n(\diamond q_f)$ $(\diamond q_f = \{\gamma \mid \gamma(q_f) > 0\})$

Example



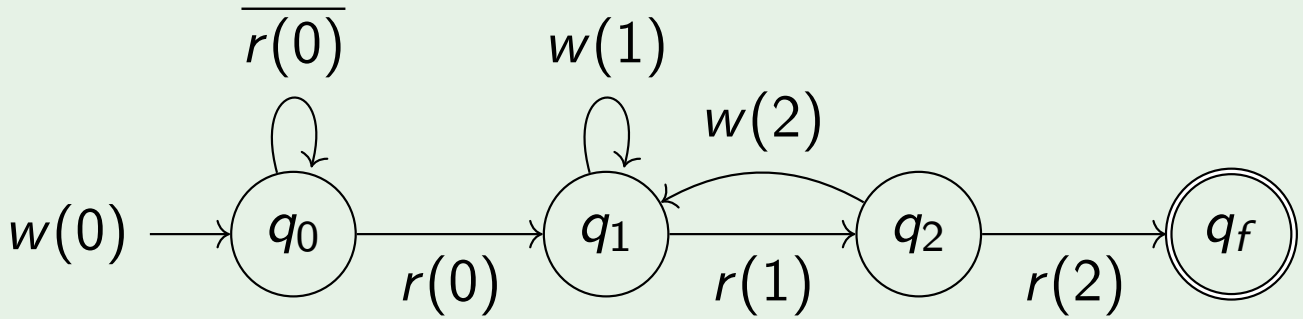


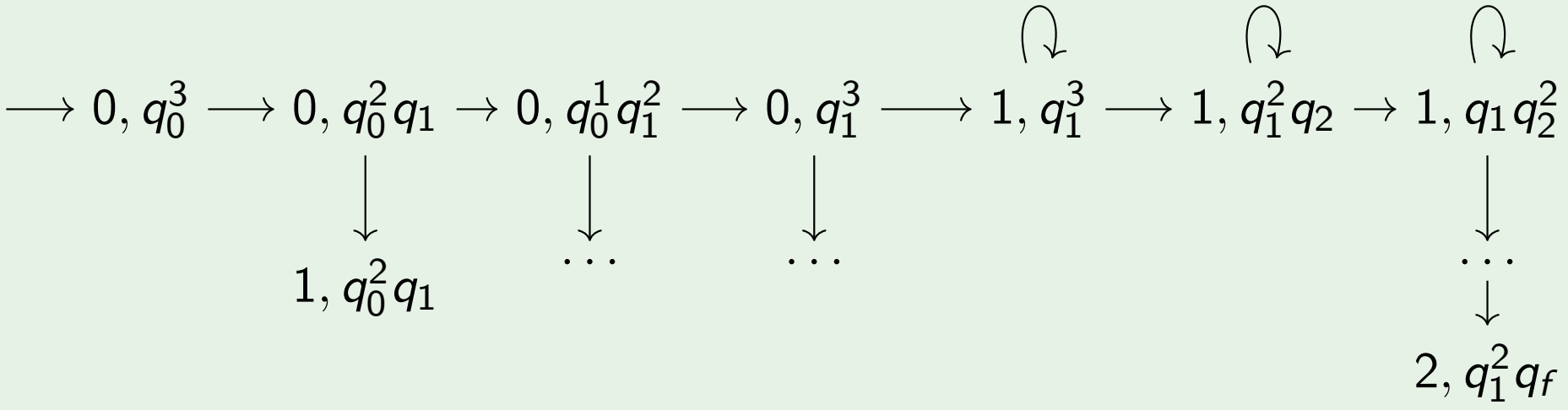
Markov Chain

Qualitative goal

Estimate $\mathbb{P}_n(\diamond q_f)$ $(\diamond q_f = \{\gamma \mid \gamma(q_f) > 0\})$

Example





Remarks

Lemma (Important remark)

For $B \in \{\{0\}, (0,1), \{1\}\}$, the property $\mathbb{P}_n(\diamond q_f) \in B$ does not depend on the actual distributions

Remarks

Lemma (Important remark)

For $B \in \{\{0\}, (0,1), \{1\}\}$, the property $\mathbb{P}_n(\diamond q_f) \in B$ does not depend on the actual distributions

Lemma (Discretization)

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

Remarks

Lemma (Important remark)

For $B \in \{\{0\}, (0,1), \{1\}\}$, the property $\mathbb{P}_n(\diamond q_f) \in B$ does not depend on the actual distributions

Lemma (Discretization)

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

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

Remarks

Lemma (Important remark)

For $B \in \{\{0\}, (0,1), \{1\}\}$, the property $\mathbb{P}_n(\diamond q_f) \in B$ does not depend on the actual distributions

Lemma (Discretization)

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

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

- Both the scheduler and processes are ~~non-deterministic~~ stochastic
- No atomicity
- For fixed parameter n, can be encoded as a Petri Net

What we are looking for

Definition

Let $B \in \{\{0\}, (0,1), \{1\}\}$ and N such that $\forall n \geq N \ \mathbb{P}^n(\diamond q_f) \in B$. Then N is a cut-off.

Symbolic graph

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

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

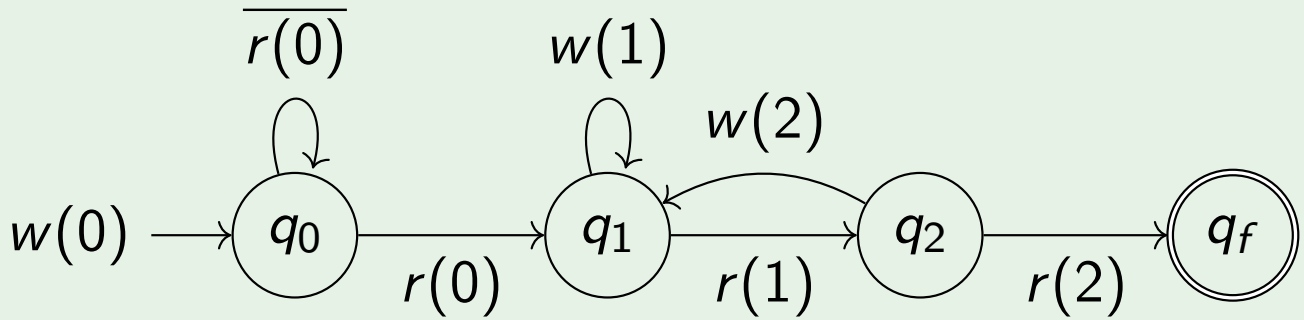
$$X_1 \backslash \{x_1, x_2\} = X_2 \backslash \{x_1, x_2\} \tag{1}$$

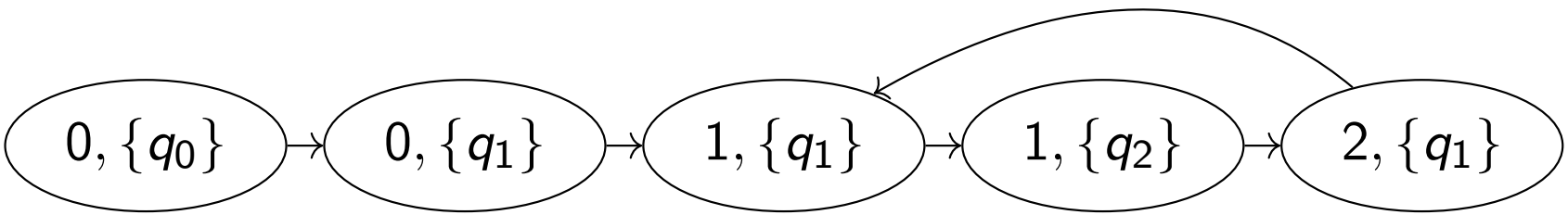
$$x_1 \xrightarrow{w(d_2)} x_2 \vee \left(x_1 \xrightarrow{r(d_2)} x_2 \wedge d_1 = d_2 \right) \tag{2}$$

Lemma

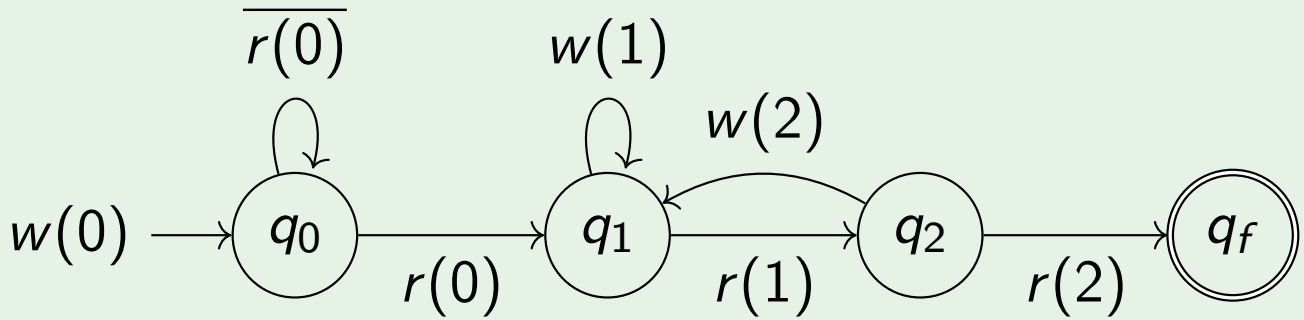
Every "concrete" run of $\mathcal{P}$ corresponds to a symbolic run.

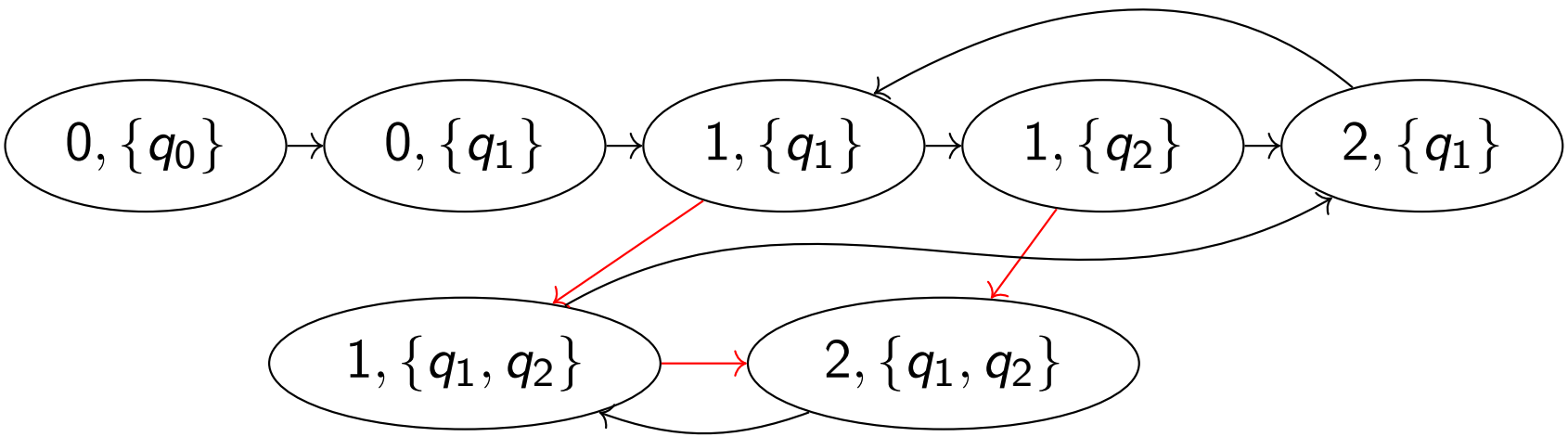
Example



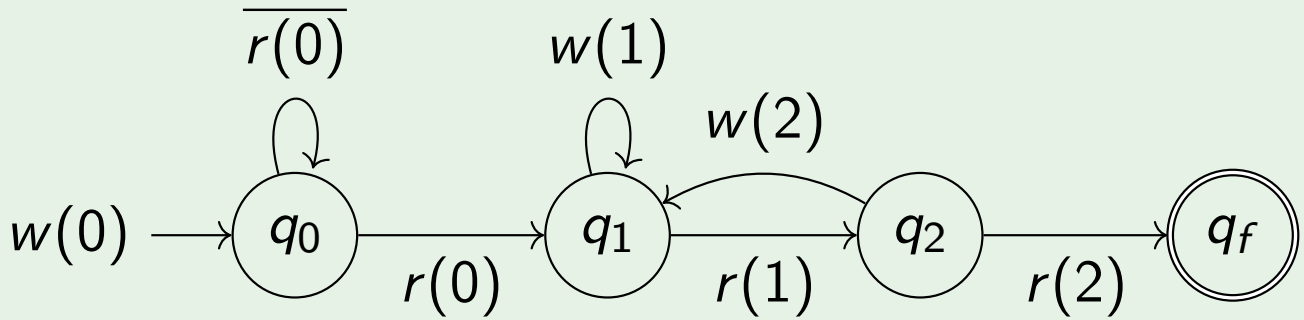


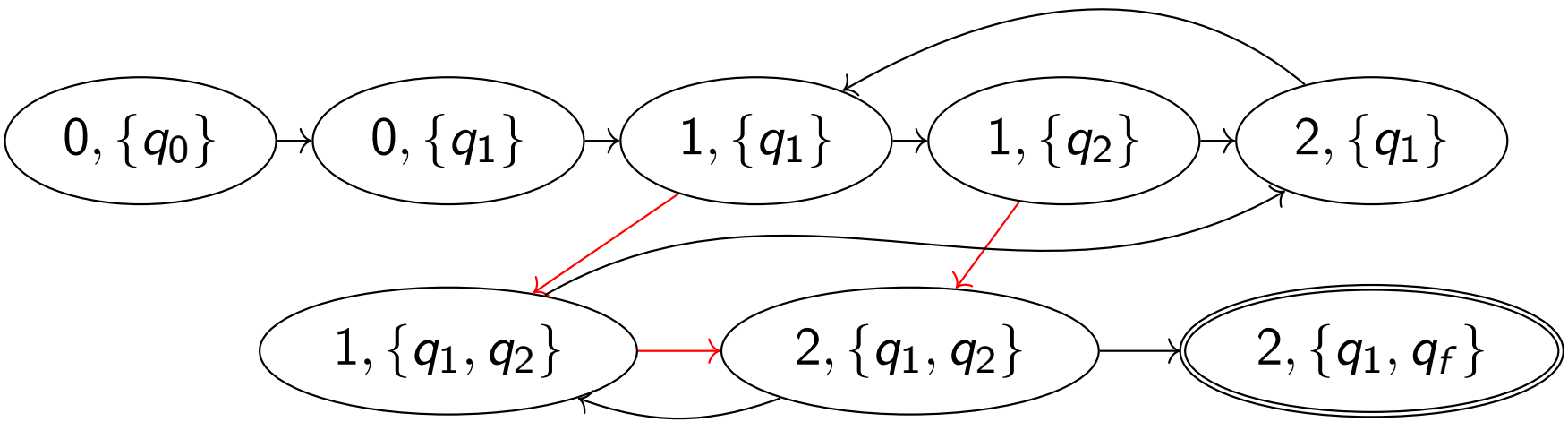
Example


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

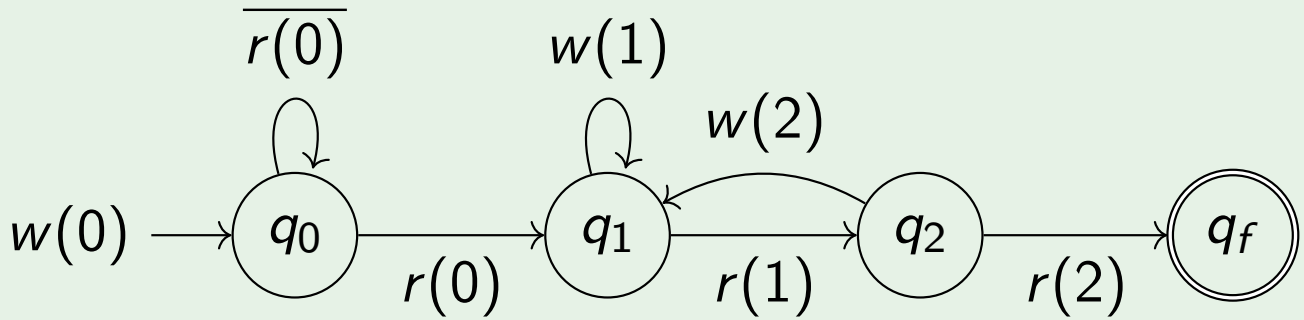

$0, \{q_0\}$
$0, \{q_1\}$
$1, \{q_1\}$
$1, \{q_2\}$
$2, \{q_1\}$
$1, \{q_1, q_2\}$
$2, \{q_1, q_2\}$

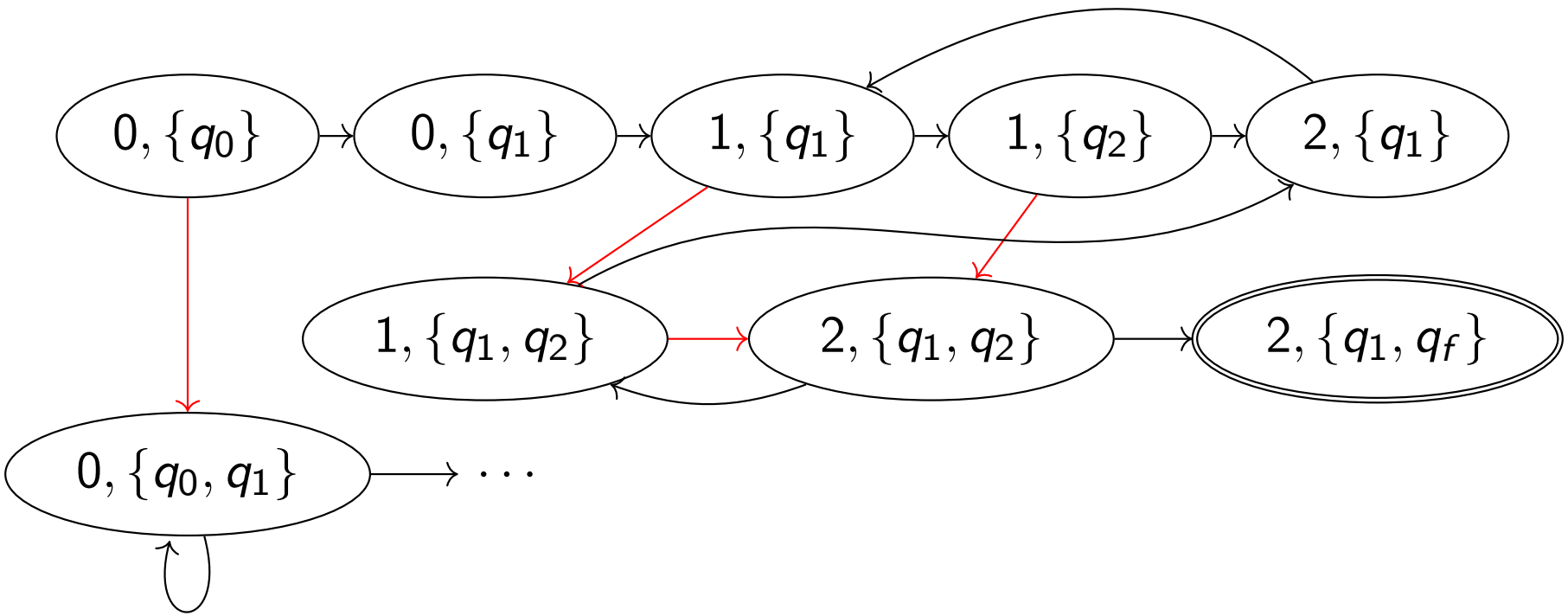
Example


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

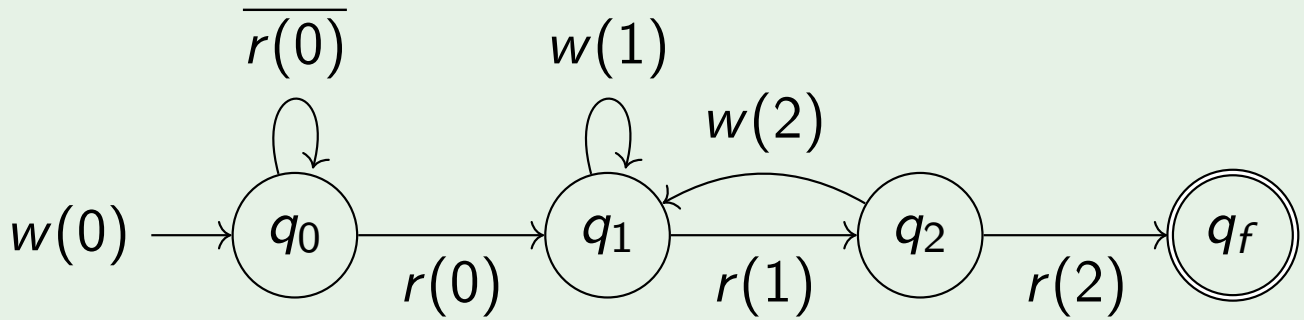

$0, \{q_0\}$
$0, \{q_1\}$
$1, \{q_1\}$
$1, \{q_2\}$
$2, \{q_1\}$
$1, \{q_1, q_2\}$
$2, \{q_1, q_2\}$
$2, \{q_1, q_f\}$

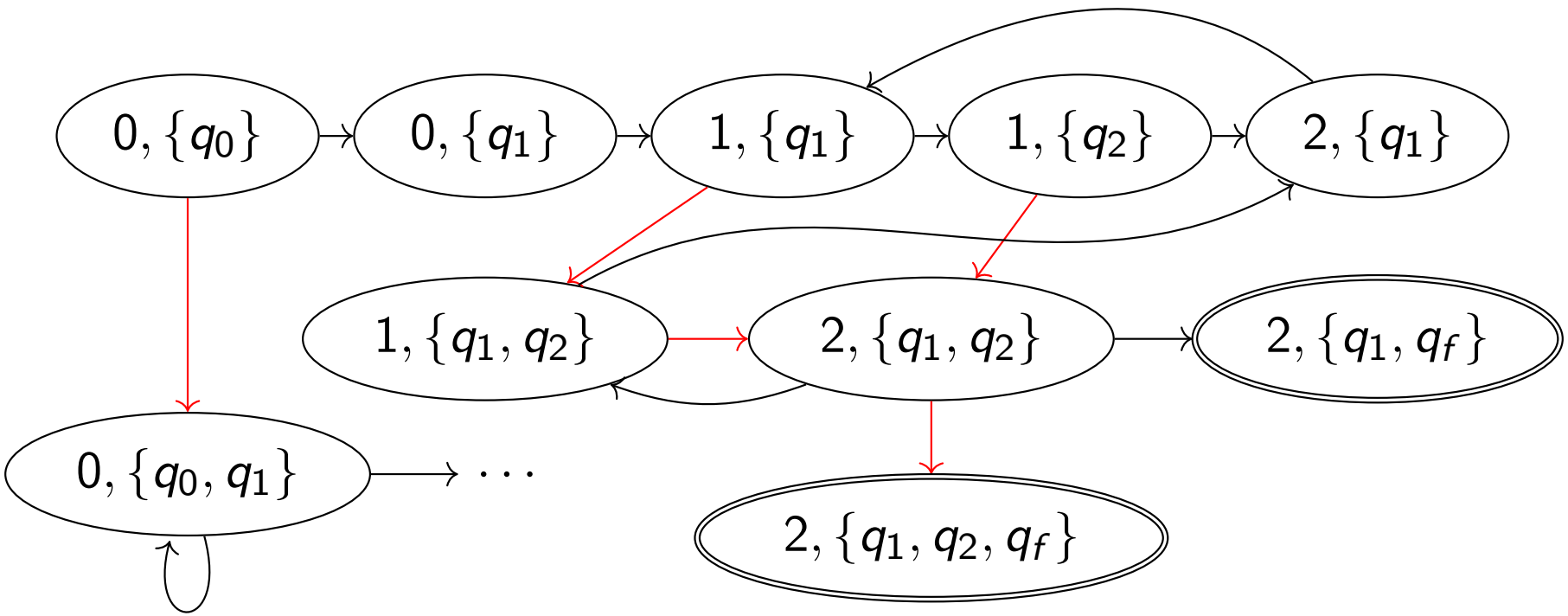
Example


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


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

Example


$\overline{r(0)}$
$w(1)$
$w(2)$
$w(0)$
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*

- $S(\gamma) = X$ *and* $v(\gamma) = d$
- $S(\gamma') = Y$ *and* $v(\gamma') = e$
- $|\gamma| = |\gamma'| \leq L$

Reconstructing the run

Lemma

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

- $S(\gamma) = X$ *and* $v(\gamma) = d$
- $S(\gamma') = Y$ *and* $v(\gamma') = e$
- $|\gamma| = |\gamma'| \leq L$

Sketch.

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

Negative cut-off: the easy case

Remark

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

Negative cut-off: the easy case

Remark

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

The converse is not true

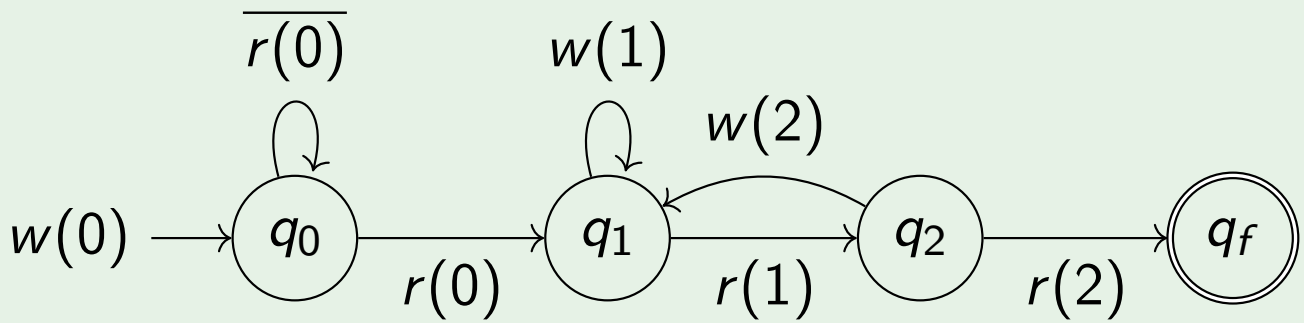
Negative cut-off: the easy case

Remark

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

The converse is not true

Example



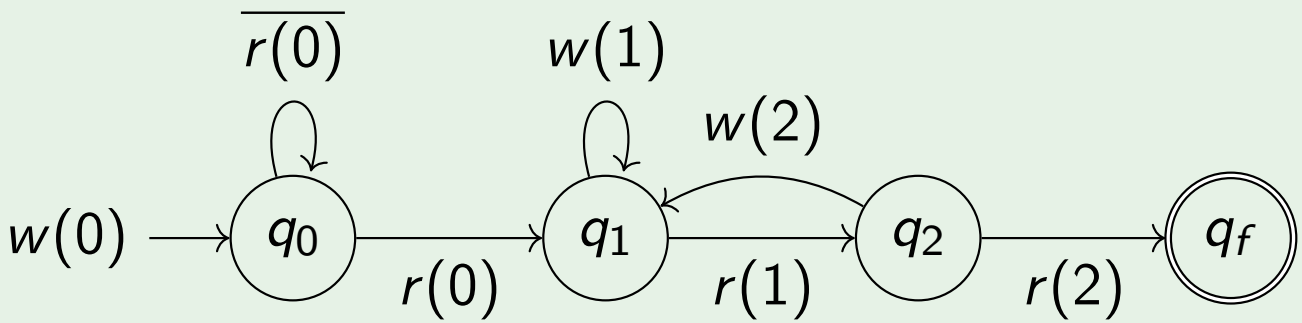
Negative cut-off: the easy case

Remark

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

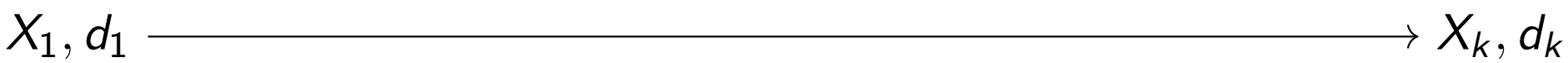
The converse is not true

Example



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

Reducing a symbolic path



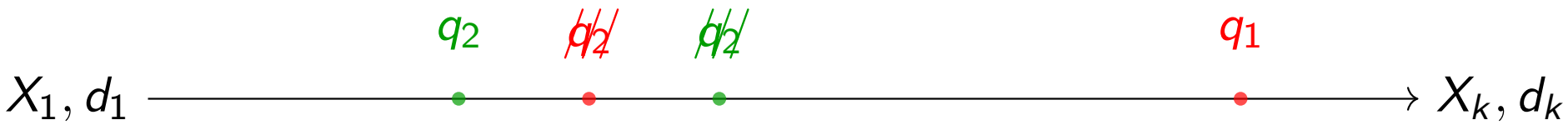
Reducing a symbolic path

Reducing a symbolic path

Reducing a symbolic path

Reducing a symbolic path

Reducing a symbolic path

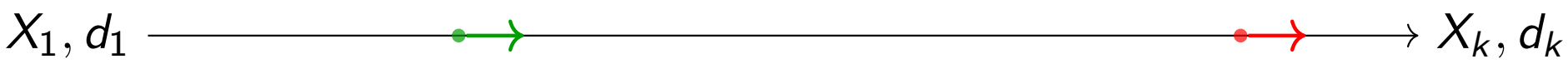


Reducing a symbolic path

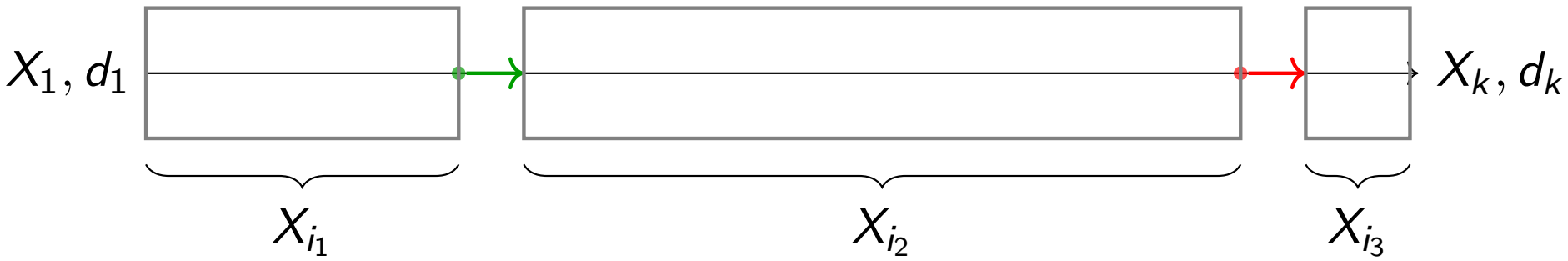
Without loss of generality

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

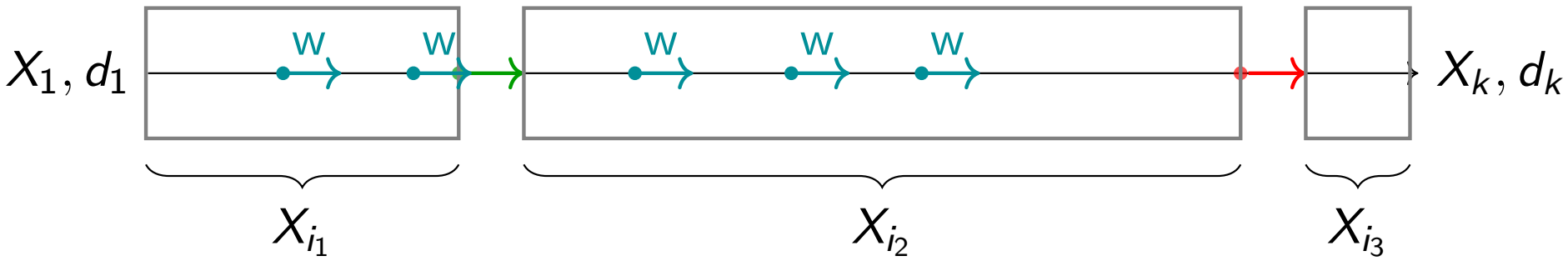
Fixed support behaviour



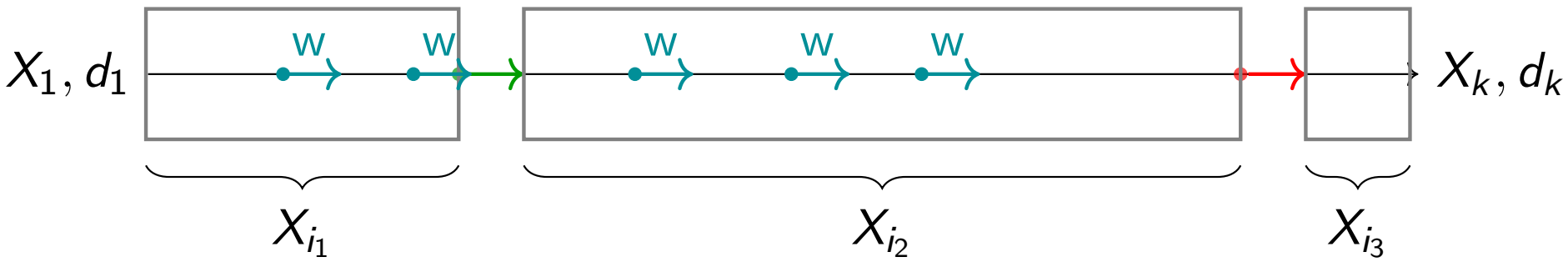
Fixed support behaviour



Fixed support behaviour



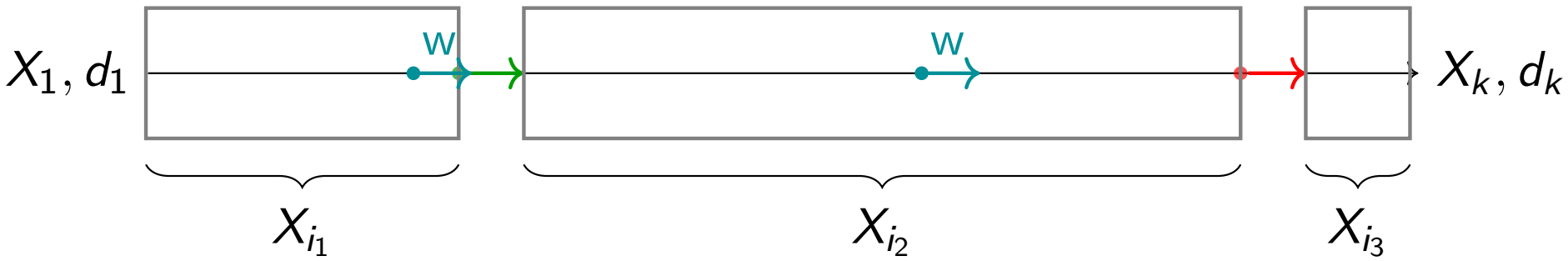
Fixed support behaviour



Key Idea

Only the last write transition is required.

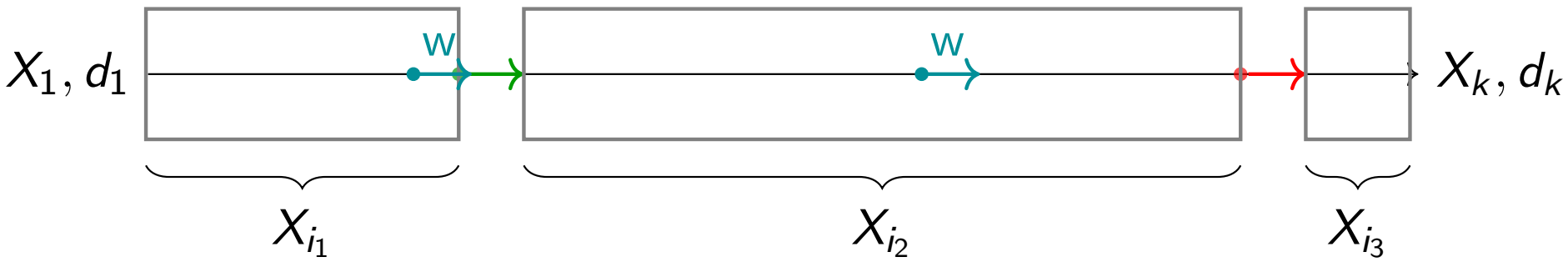
Fixed support behaviour



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 $\gamma \to^* \gamma'$ 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

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

This solves the cut-off existence problem in the case $\{0\}$ since

$$\mathbb{P}^n(\diamond q_f) > 0 \;\Rightarrow\; \mathbb{P}^{\min(n,4|Q|+1)}(\diamond q_f) > 0$$

What the symbolic graph taught us

Theorem

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

This solves the cut-off existence problem in the case $\{0\}$ since

$$\mathbb{P}^n(\diamond q_f) > 0 \;\Rightarrow\; \mathbb{P}^{\min(n,4|Q|+1)}(\diamond q_f) > 0$$

It remains to determine the 2 others cut-offs:

- The "positive" case : $\mathbb{P}^{\geq N}(\diamond q_f) \equiv 1$
- The "negative" case : $\mathbb{P}^{\geq N}(\diamond q_f) < 1$

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 $\mathrm{Pre}^*(\diamond q_f)$ and $\mathrm{Succ}^*((q_0^k, d_0))$ 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.

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

- $\mathrm{Pre}^*(\diamond q_f)$ is upward-closed
- $\mathrm{Succ}^*((q_0^n, d_0))$ 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

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

With $S(\gamma) = \{q \mid \gamma(q) > 0\}$.
$\preceq$ is a well quasi-order.

- $\mathrm{Pre}^*(\diamond q_f)$ is upward-closed
- $\mathrm{Succ}^*((q_0^{\geq n}, d_0))$ 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

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

Cut-off

We write

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

$$\mathrm{Succ}^*((q_0^{\geq 1}, d_0)) \subseteq \mathrm{Pre}^*(\diamond q_f)$$

Cut-off

We write

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

$$\mathrm{Succ}^*((q_0^{\geq 1}, d_0)) \subseteq \mathrm{Pre}^*(\diamond q_f)$$

$$\Leftrightarrow$$

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

Cut-off

We write

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

$$\mathrm{Succ}^*((q_0^{\geq 1}, d_0)) \subseteq \mathrm{Pre}^*(\diamond q_f)$$

$$\Leftrightarrow$$

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

$$\Leftrightarrow$$

n is a positive cut-off

Cut-off

We write

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

$$\mathrm{Succ}^*((q_0^{\geq 1}, d_0)) \subseteq \mathrm{Pre}^*(\diamond q_f)$$

$$\Leftrightarrow$$

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

$$\Leftrightarrow$$

n is a positive cut-off

What about the negative cut-off case ?

Negative case

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

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

Negative case

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

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

Negative case

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

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

Negative case

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

- If there exists γ_i such that $\forall j\ (S(\gamma_i), v(\gamma_i)) \neq (S(\eta_j), v(\eta_j))$, 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

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

- If there exists γ_i such that $\forall j\ (S(\gamma_i), v(\gamma_i)) \neq (S(\eta_j), v(\eta_j))$, 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

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

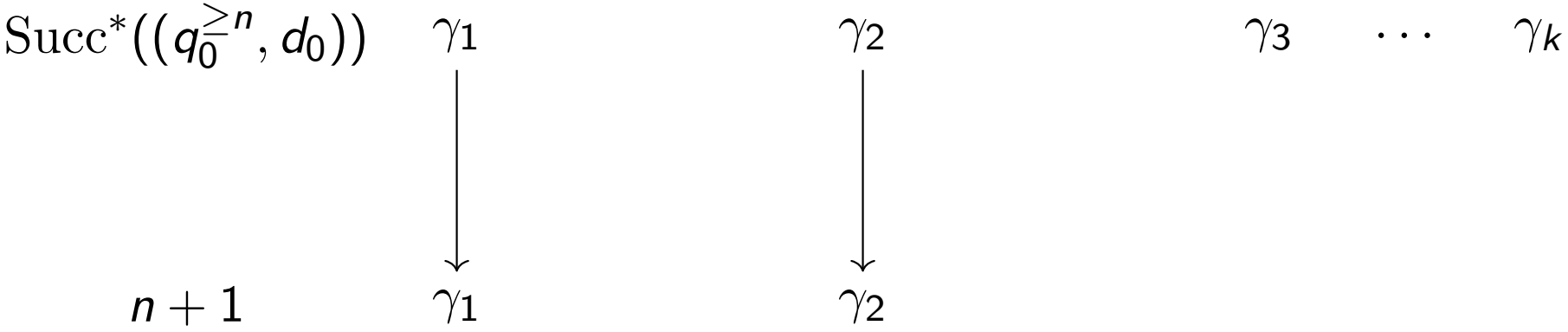
varies w.r.t n ?

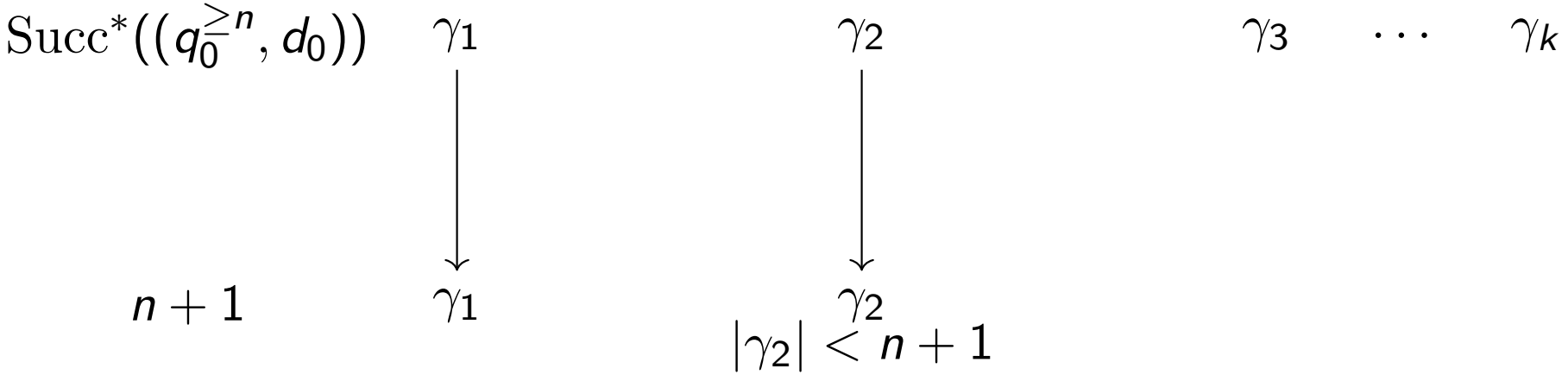
$\mathrm{Succ}^*((q_0^{\geq n}, d_0))$ $\quad \gamma_1 \quad \gamma_2 \quad \gamma_3 \quad \cdots \quad \gamma_k$

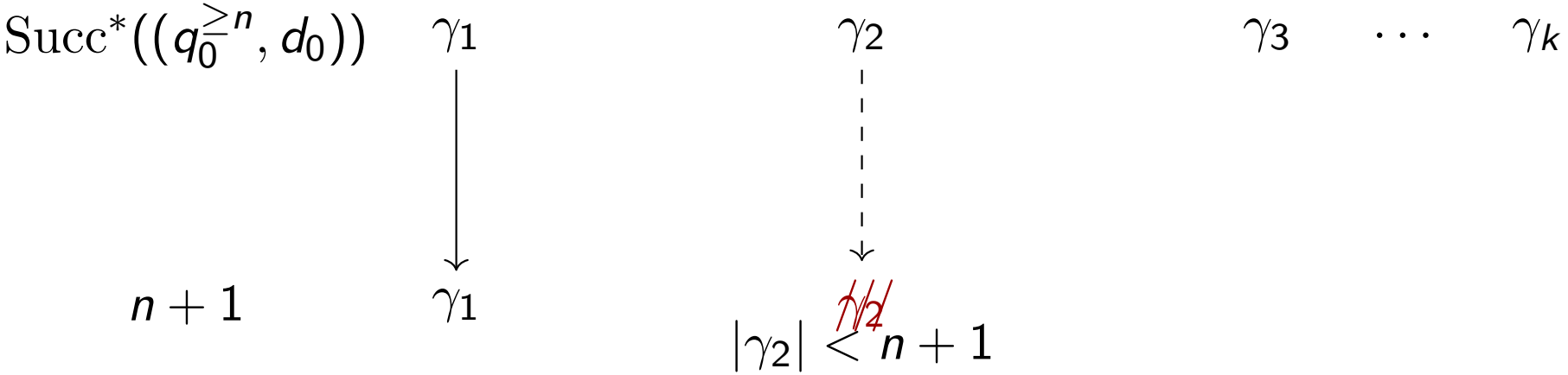
$\mathrm{Succ}^*((q_0^{\geq n}, d_0))$ γ_1 γ_2 γ_3 $\cdots$ γ_k

$n+1$

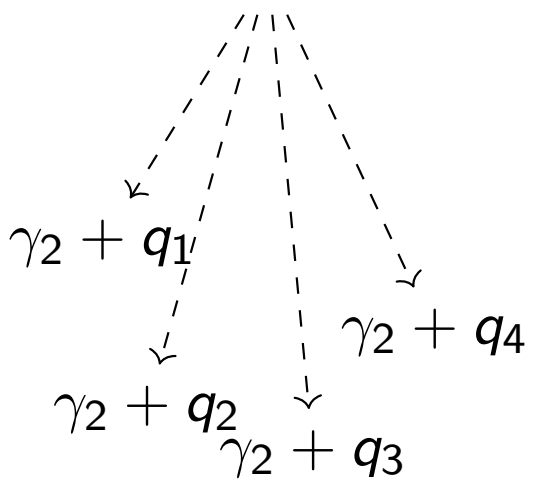
$$\begin{array}{lllll} \mathrm{Succ}^*((q_0^{\geq n}, d_0)) & \gamma_1 & \gamma_2 & \gamma_3 \quad \cdots & \gamma_k \\ & \downarrow & & & \\ n+1 & \gamma_1 & & & \end{array}$$


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


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

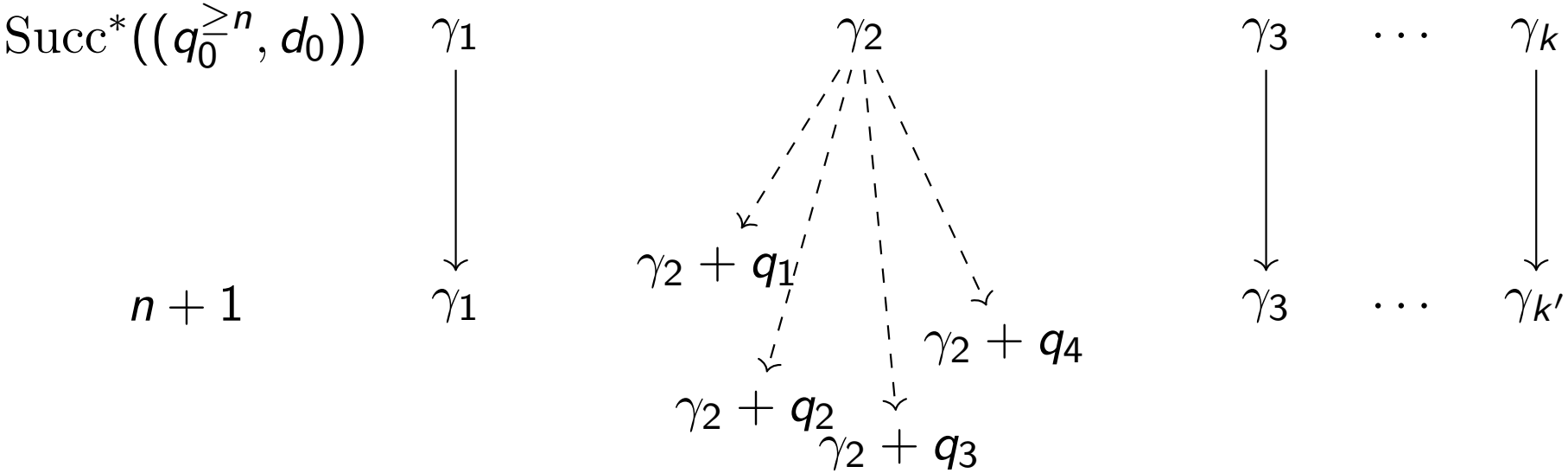

$\mathrm{Succ}^*((q_0^{\geq n}, d_0))$
γ_1
γ_2
γ_3
$\cdots$
γ_k
$n+1$
γ_1
γ_2
$|\gamma_2| < n+1$

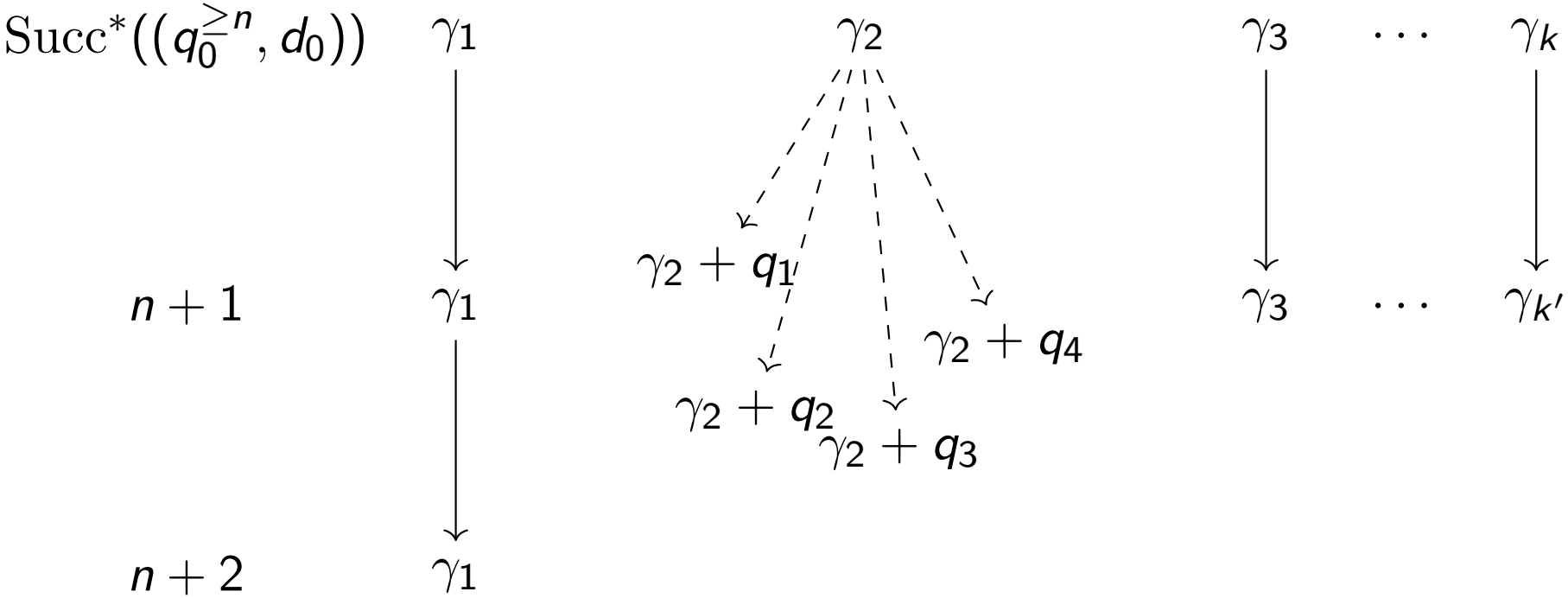
$\mathrm{Succ}^*((q_0^{\geq n}, d_0))$ γ_1 γ_2 γ_3 $\cdots$ γ_k

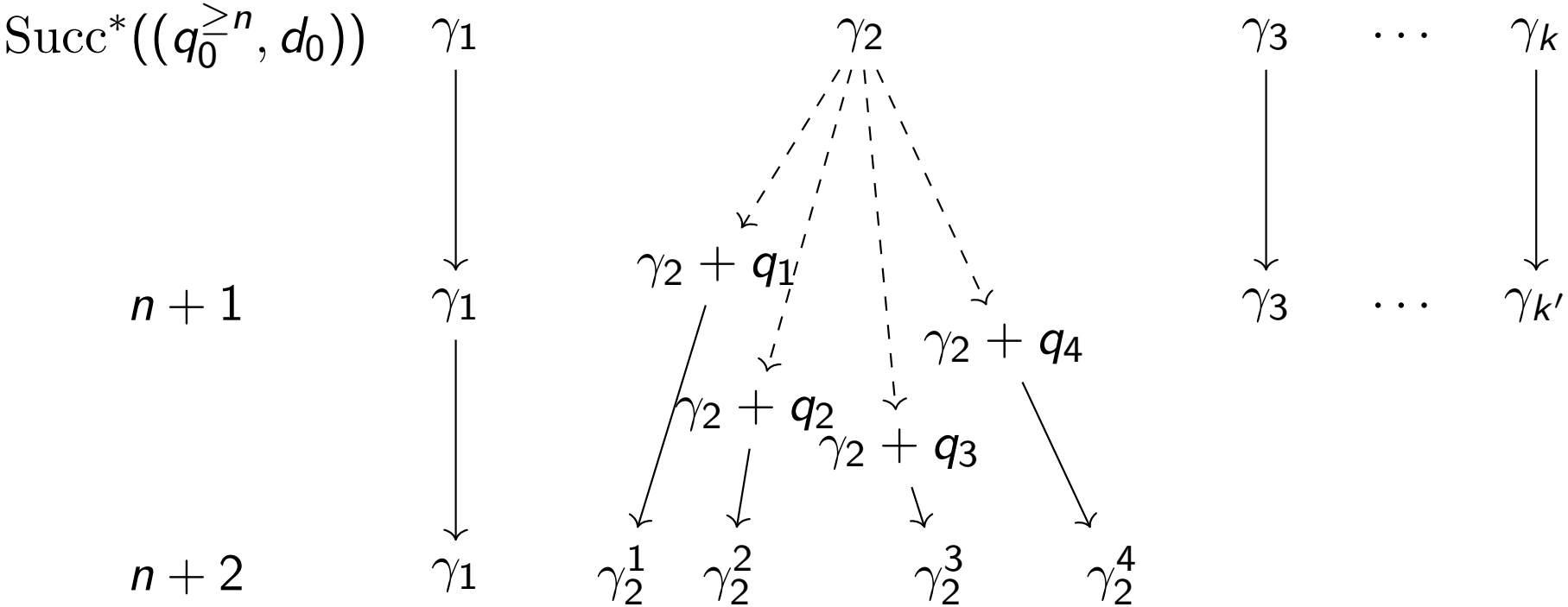


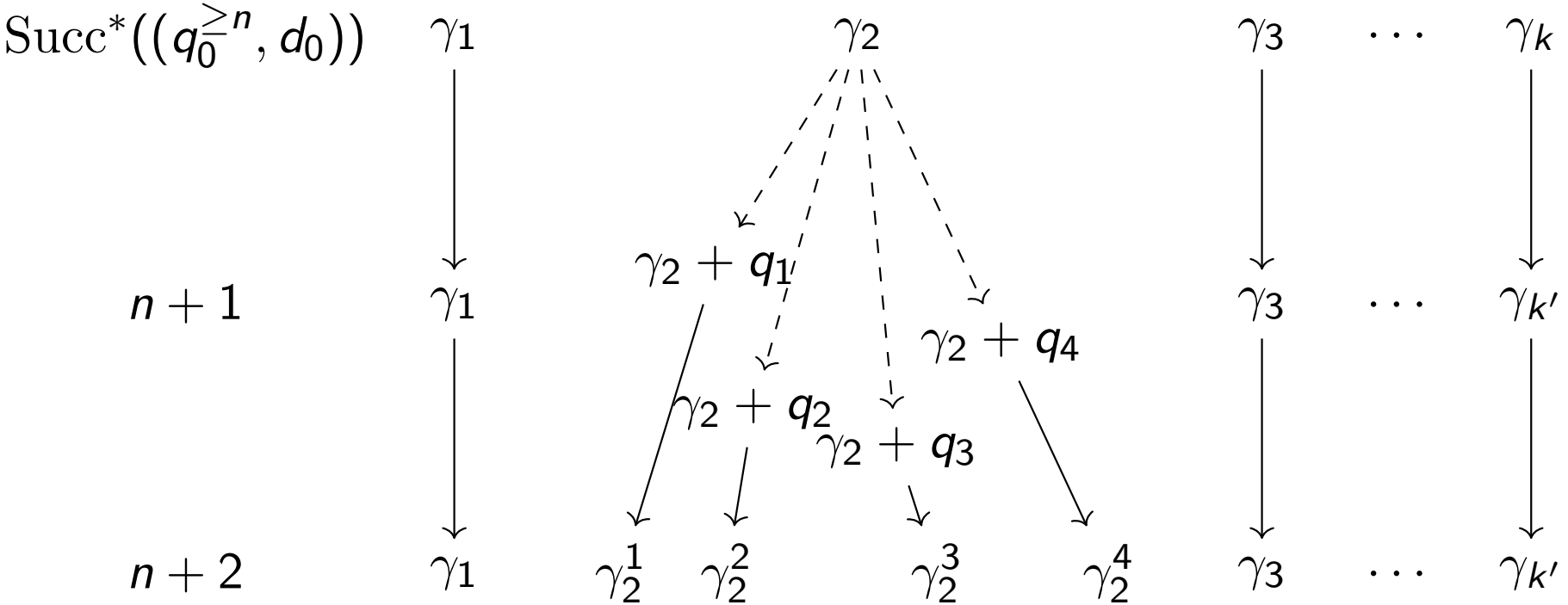
$n+1$ γ_1

$q_i \in S(\gamma_2)$


$\mathrm{Succ}^*((q_0^{\geq n}, d_0))$
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
$\cdots$
$\gamma_{k'}$


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


$\mathrm{Succ}^*((q_0^{\geq n}, d_0))$
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


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

Variation of the basis

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

Variation of the basis

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

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

and let $\gamma \in \mathrm{Succ}^*((q_0^{\geq 1}, d_0))$. *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

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

and let $\gamma \in \mathrm{Succ}^*((q_0^{\geq 1}, d_0))$. *We define:*

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

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

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

Positive cut-off

Lemma (Positive cut-off)

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

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

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

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

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 $q \notin \left\{ q \mid \forall k \geq 0 \ \eta_{j_q} \not\preceq \gamma + q^k \right\}$ 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 $\diamond q_f$ 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

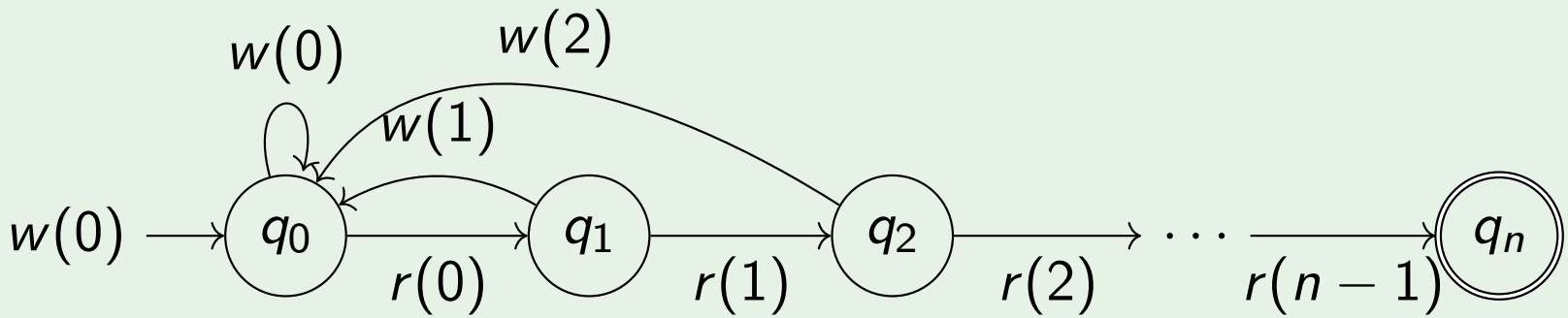
Theorem

Given a protocol $\mathcal{P}$ there always exists either a positive cut-off either a negative cut-off N.
The probability to reach $\diamond q_f$ 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 ?

Linear example

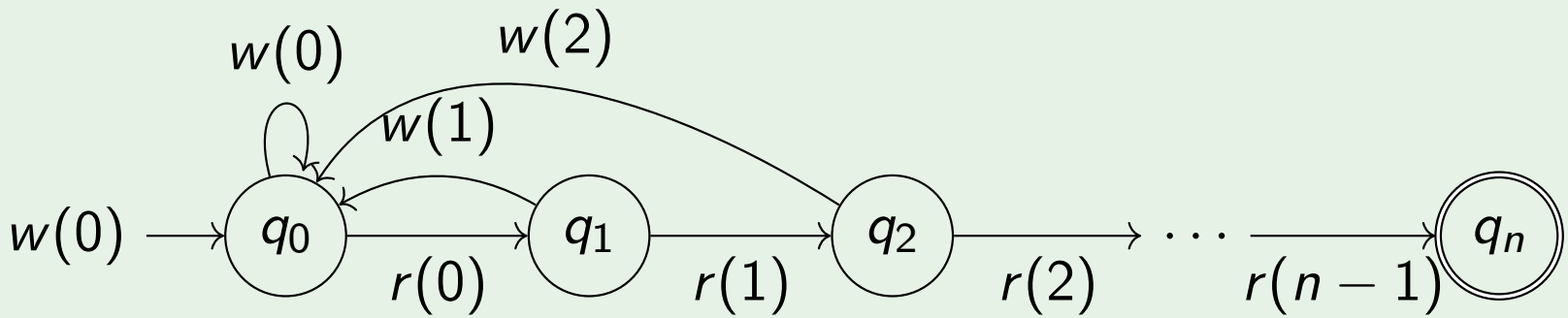
Example



Cut-off value ?

Linear example

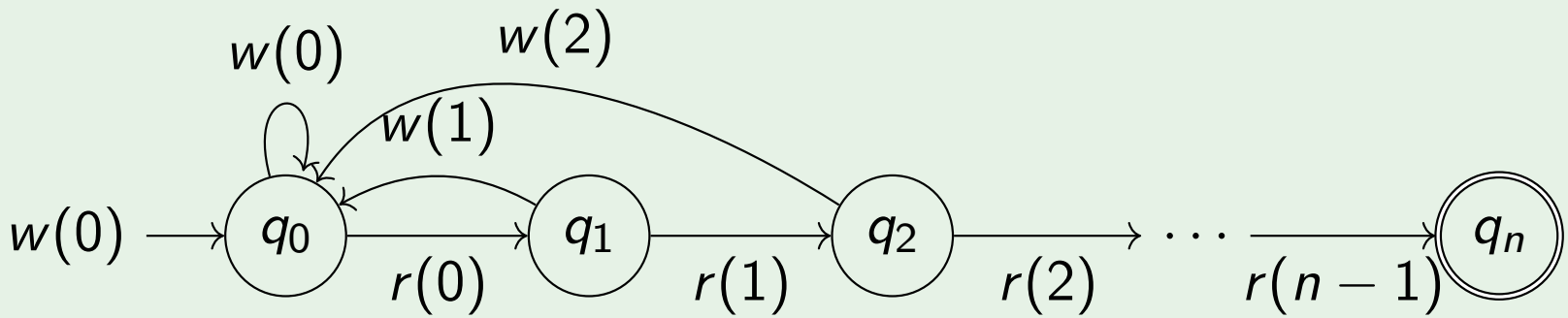
Example



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

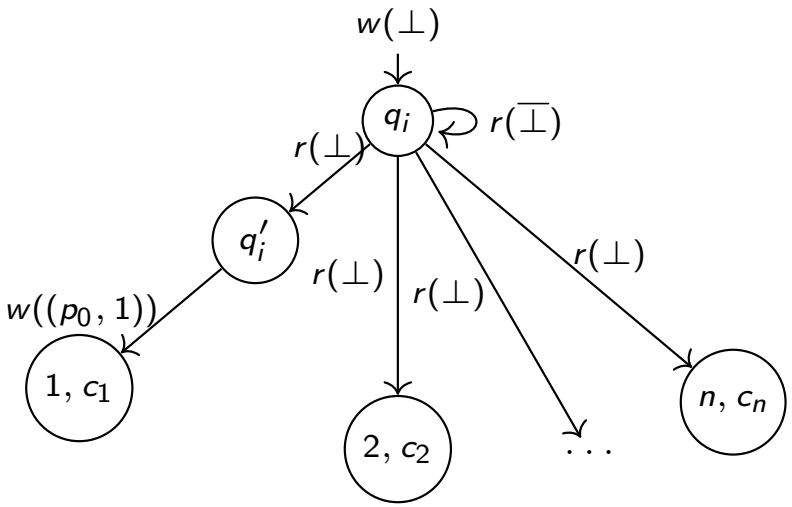
Sketch.

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

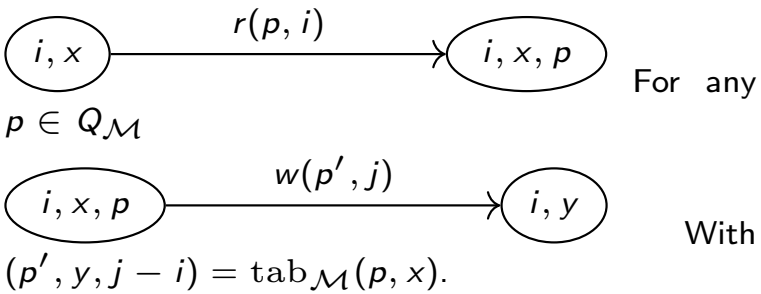
- A given tape position i containing letter x is coded by a fixed state
- The current head position is coded in the register
- If the number of states is too big, we cannot ensure proper encoding
- Key idea: we code improper encoding/non-termination by $\mathbb{P}(\diamond q_f) = 1$
- The previous module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

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

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

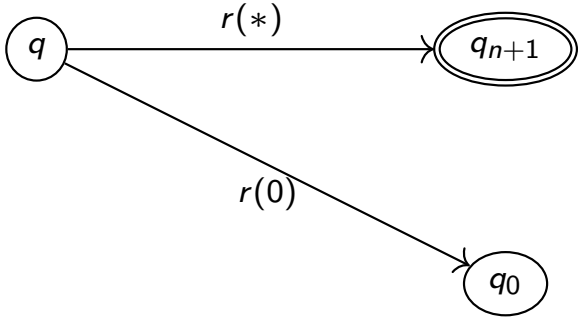


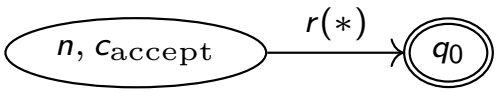
(a) $\{q_i\}$: Initialization: $c_1 \ldots c_n$ is the initial data band



(b) Q_S: Simulation step

For every $q \in Q_S$, we add the two following transitions:





(c) Q_S: Final transition (d) Q_S: two extra transitions that ensure leaving Q_S on the last memory cell almost surely

Figure: Reduction of a linear bounded Turing machine $\mathcal{M}$, the $q_0 \ldots q_{n+1}$ module is the "filter $n+1$ module"

Upper bound ?

- Current investigation: bound the cut-off by bounding the elements of $\mathrm{Pre}^*(\diamond q_f)$ and $\mathrm{Succ}^*((q_0^+, d_0))$.
- Symbolic graph ensures "globally small" elements
- Refine the notion of symbolic graph at will
- For now: exponential tower in $|Q|$

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 $\diamond q_f = \{(q_f^k, d) \mid k, d\}$ an harder property ?)
- Hardness result with atomic operations ?
- (Local ?) Strategies
- Reasonable PSPACE algorithm
- Modelize concrete problems

Thank you for your attention