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
Reachability in Register Protocols
  Definitions
  Example
  (Non-)Deterministic Reachability

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 $p, q \in Q$, $d \in D$. 

Example

$\begin{array}{cccc}
q_0 & q_1 & q_2 & q_{fr}(1) \\
r(0) & r(1) & r(2) & r(0) \\
rw(1) & rw(2) & rw(1) & rw(2) \\
\end{array}$
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

![Diagram of a distributed protocol example](image)
Semantics

\[ q_0 \xrightarrow{r(0)} q_1 \xrightarrow{w(1)} q_2 \xrightarrow{w(2)} q_f \]

Initial states:

\[ 0 \]

Transition labels:

\[ r(1), r(2), w(1), w(2) \]
Semantics

$\mathcal{M} = (Q, \Sigma, \delta, q_0, F)$

where

- $Q = \{q_0, q_1, q_2, q_f\}$
- $\Sigma = \{0, 1\}$
- $\delta$ is the transition function
  
  - $\delta(q_0, 0) = q_0$
  - $\delta(q_0, 1) = q_1$
  - $\delta(q_1, 0) = q_1$
  - $\delta(q_1, 1) = q_2$
  - $\delta(q_2, 0) = q_1$
  - $\delta(q_2, 1) = q_2$
  - $\delta(q_2, 2) = q_f$

- $F = \{q_f\}$

The automaton recognizes the language $L = \{0^r1^s0^r1^s : r, s \geq 0\}$.

- $r(1), r(2)$
- $w(1)$
- $w(2)$

In the diagram:

- $q_0$ is the initial state.
- $q_f$ is the accepting state.
- Transitions are labeled with symbols from $\Sigma$.
- Loops indicate self-loops for each state.

The automaton transitions are:

- From $q_0$ to $q_1$ on $1$
- From $q_1$ to $q_2$ on $1$
- From $q_2$ to $q_f$ on $2$
Semantics

\[
q_0 \xrightarrow{r(0)} q_1 \xrightarrow{w(1)} q_2 \xrightarrow{w(2)} q_f
\]

\[
q_0 \xrightarrow{r(0)} q_1 \xrightarrow{r(1)} q_2 \xrightarrow{r(2)} q_f
\]

0

0

0

0
Semantics

\[ r(1), r(2) \]

\[ q_0 \xrightarrow{r(0)} q_1 \xrightarrow{r(1)} q_2 \xrightarrow{r(2)} q_f \]

\[ w(1), w(2) \]

\[
\begin{align*}
0 & \quad q_0 & q_0 & q_0 \\
\quad & r(0) & & \\
0 & \quad q_1 & q_0 & q_0 \\
\quad & r(0) & & \\
0 & \quad q_1 & q_0 & q_1 \\
\quad & w(1) & & \\
1 & \quad q_1 & q_0 & q_1 \\
\quad & r(1) & & \\
\end{align*}
\]
Semantics

Graphical representation of a finite state machine with states $q_0$, $q_1$, $q_2$, and $q_f$. The transitions are labeled with symbols $r(0)$, $r(1)$, $r(2)$, $w(1)$, and $w(2)$. The diagram illustrates the transitions between states based on input symbols.
Semantics

\[
q_0 \xrightarrow{r(0)} q_1 \xrightarrow{w(1)} q_2 \xrightarrow{r(2)} q_f
\]

\[
r(1), r(2) \quad w(1) \quad w(2)
\]
Semantics

\[ r(1), r(2) \rightarrow w(1) \rightarrow w(2) \rightarrow w(1) \]

\[ q_0 \rightarrow q_1 \rightarrow q_2 \rightarrow q_f \]

\[ r(0) \rightarrow r(1) \rightarrow r(2) \]

\[ w(1) \rightarrow w(2) \]

\[ r(1) \rightarrow r(1) \rightarrow r(1) \]

\[ q_0 \rightarrow q_1 \rightarrow q_2 \rightarrow q_f \]

\[ r(0) \rightarrow r(1) \rightarrow r(2) \]

\[ w(1) \rightarrow w(2) \]

\[ r(1) \rightarrow r(1) \rightarrow r(1) \]

\[ q_0 \rightarrow q_1 \rightarrow q_2 \rightarrow q_f \]

\[ r(0) \rightarrow r(1) \rightarrow r(2) \]

\[ w(1) \rightarrow w(2) \]

\[ r(1) \rightarrow r(1) \rightarrow r(1) \]

\[ q_0 \rightarrow q_1 \rightarrow q_2 \rightarrow q_f \]

\[ r(0) \rightarrow r(1) \rightarrow r(2) \]

\[ w(1) \rightarrow w(2) \]

\[ r(1) \rightarrow r(1) \rightarrow r(1) \]
Semantics

\[ r(1), r(2) \]

\[ w(1) \]

\[ w(2) \]

\[ q_0 \rightarrow q_1 \rightarrow q_2 \rightarrow q_f \]

\[ r(0) \]

\[ r(1) \]

\[ r(2) \]

\[ w(1) \]

\[ w(2) \]

\[ r(1) \]

\[ r(2) \]

\[ \ldots \]
Definition (Configuration of the protocol)

\[ \gamma = \langle f, d \rangle \]

with \( f : Q \rightarrow \mathbb{N} \) (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:

- \( \Gamma \) is the set of configurations
- \( |\gamma| = \sum_q \gamma(q) \) (size)
- \( \text{Pre}(X), \text{Post}(X) \)
- \( +, - \) 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:
- \( \Gamma \) is the set of configurations
- \( |\gamma| = \sum_q \gamma(q) \) (size)
- \( \text{Pre}(X), \text{Post}(X) \)
- \( +, - \) operations on multisets are extended to configurations.

Definition (Semantics)

\( \gamma \rightarrow \gamma' \) if \( \gamma' = \gamma - q + q' \) with either
- \( q \xrightarrow{\text{w}(v(\gamma))} q' \) (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 \(\gamma\) 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 $G_{\text{symb}}$ from the initial transition system by abstraction on the number of copies in each state.

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

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

\(r(1), r(2)\)

\(w(1)\)

\(w(2)\)

\(w(1)\)

\(q_0\) \(\rightarrow\) \(q_1\) \(\rightarrow\) \(q_2\) \(\rightarrow\) \(q_f\)

\(r(0)\)

\(r(1)\)

\(r(2)\)

\(0, \{q_0\}\) \(\rightarrow\) \(0, \{q_1\}\) \(\rightarrow\) \(1, \{q_1\}\) \(\rightarrow\) \(1, \{q_2\}\) \(\rightarrow\) \(2, \{q_1\}\)
Example

\[ r(1), r(2) \quad w(1) \quad w(2) \quad w(1) \]

\[ q_0 \xrightarrow{r(0)} q_1 \xrightarrow{r(1)} q_2 \xrightarrow{r(2)} q_f \]

\[ 0, \{q_0\} \xrightarrow{0} 0, \{q_1\} \xrightarrow{1} 1, \{q_1\} \xrightarrow{1} 1, \{q_2\} \xrightarrow{2} 2, \{q_1\} \]

\[ 1, \{q_1, q_2\} \xrightarrow{2} 2, \{q_1, q_2\} \]
Example
Example

\[ r(1), r(2) \quad w(1) \quad w(2) \quad r(1) \quad r(2) \]

\[ q_0 \quad q_1 \quad q_2 \quad q_f \]

\[ (0, \{q_0\}) \quad (0, \{q_1\}) \quad (1, \{q_1\}) \quad (1, \{q_2\}) \quad (2, \{q_1\}) \]

\[ (1, \{q_1, q_2\}) \quad (2, \{q_1, q_2\}) \quad (2, \{q_1, q_f\}) \]

\[ 0, \{q_0, q_1\} \quad \ldots \]
Example
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 $\gamma \rightarrow^* \gamma'$ there exists $\eta \rightarrow^* \eta'$ 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 $\gamma \rightarrow^* \gamma'$ there exists $\eta \rightarrow^* \eta'$ 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
Definition (Law of motion)
We consider \((\Gamma, \rightarrow)\) as a Markov Chain.

\[
\forall \gamma' \in \text{Post}(\gamma) \quad \Pr(\gamma \to \gamma') = \frac{1}{|\text{Post}(\gamma)|}
\]
Markov Chain

Definition (Law of motion)
We consider \((\Gamma, \rightarrow)\) as a Markov Chain.

\[
\forall \gamma' \in \text{Post}(\gamma) \quad \Pr(\gamma \rightarrow \gamma') = \frac{1}{|\text{Post}(\gamma)|}
\]

Let \((q_0, d_0) \in Q \times D\), a parameter \(n\).
For \(X \subseteq \Gamma\), we denote \(P^n(X)\) 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 $\Gamma$ as a Markov Chain.

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

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 $(q^n_0, d_0)$ (leader-less case).

Qualitative goal

Let $q_f \in Q$.

Estimate $\mathbb{P}^n(\uparrow q_f)$. 
The automaton has states $q_0$, $q_1$, $q_2$, and $q_f$. The transitions are as follows:

- $q_0$ transitions to $q_1$ on input $r(0)$.
- $q_1$ transitions to $q_2$ on input $w(1)$ and $w(2)$.
- $q_2$ transitions to $q_f$ on input $r(2)$.
- $q_0$ to $q_0$ transitions on input $r(1)$.

The initial state is $q_0$, and the final state is $q_f$. The automaton accepts strings that satisfy certain conditions.
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.
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 a priori.
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

\[ P^n(\uparrow q_f) = 0 \iff \text{Post}^*((q^n_0, d_0)) \cap \text{Pre}^*(\uparrow q_f) = \emptyset \]
Discretization

Lemma

\[ \mathbb{P}^n(\uparrow q_f) = 0 \iff \text{Post}^*((q^n_0, d_0)) \cap \text{Pre}^*(\uparrow q_f) = \emptyset \]

\[ \mathbb{P}^n(\uparrow q_f) = 1 \iff \text{Post}^*((q^n_0, d_0)) \subseteq \text{Pre}^*(\uparrow q_f) \]
What we are looking for

Some limit behaviour, if possible

**Definition (Cut-off)**

Let $N$ be a parameter. If $\forall n \geq N \ P^n(\uparrow q_f) = 1$ or $\forall n \geq N \ P^n(\uparrow q_f) < 1$, then $N$ is a cut-off.
Some limit behaviour, if possible

**Definition (Cut-off)**

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

- **positive** $\forall n \geq N \ P^n(\uparrow q_f) = 1$
- **negative** $\forall n \geq N \ P^n(\uparrow q_f) < 1$
- 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 or 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 $\min \text{Post}^* (\uparrow (q_0, d_0))$ and $\min \text{Pre}^* (\uparrow q_f)$
- How to efficiently decide the type of the cut-off?
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 $G_{\text{symb}}$.

The converse is not true
Negative cut-off: the easy case

Remark
Almost-sure reachability in the concrete system implies Almost-sure reachability in $G_{\text{symb}}$.

The converse is not true

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

The converse is not true

Example

\[(q_0^n, 0) \xrightarrow{r(0)} (q_0^{n-1} q_1, 0) \xrightarrow{w(0)} (q_0^{n-1} q_1, 1) \not\xrightarrow{\star \uparrow} q_f\]
Reachability in Register Protocols

Almost sure reachability

**Cut-off constructions**
- Linear filter
- Consequences
- Upper Bound
Linear example

Example

The cut-off is positive and equals $n$.

Invariant (with $m$ initial processes):
\[ \forall j \leq m \sum_{k=0}^{\infty} \gamma(q_k) \geq j + 1 \]

Cut-off value?
Linear example

Example

Cut-off value?

Invariant (with $m$ initial processes):

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

Example

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

Invariant (with $m$ initial processes):

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

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

Decision Problem

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

The cut-off decision problem is PSPACE-hard.
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.
Rackoff’s theorem: \( \min \text{Pre}^*(\uparrow q_f) \) can be bounded by \( M \) doubly-exponential in \(|\mathcal{P}|\).

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

No bound on the \( \min \text{Post}^*(\uparrow (q_0, d_0)) \).

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.*
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.
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?
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?
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