Symbolic reductions of probabilistic models using linear process equations

Mark Timmer
March 8, 2010

Joint work with Joost-Pieter Katoen, Jaco van de Pol, and Mariëlle Stoelinga
Contents

1 Introduction

2 A process algebra with data and probability: prCRL

3 Linear probabilistic process equations

4 Case study: leader election protocol

5 Confluence reduction

6 Conclusions and Future Work
Probabilistic Model Checking

Probabilistic model checking:
- Verifying quantitative properties,
- Using a probabilistic model (e.g., a probabilistic automaton)
Probabilistic model checking:

- Verifying quantitative properties,
- Using a probabilistic model (e.g., a probabilistic automaton)

Non-deterministically choose one of the three transitions

Probabilistically choose the next state
Probabilistic model checking:

- Verifying quantitative properties,
- Using a probabilistic model (e.g., a probabilistic automaton)

Non-deterministically choose one of the three transitions
Probabilistically choose the next state

Limitations of previous approaches:

- Susceptible to the state space explosion problem
- Restricted treatment of data
Overview of our approach

Probabilistic specification (prCRL)

Linearisation

Linear Probabilistic Process Equation (LPPE)

Instantiation

State space (PA)

Visualisation

Model checking

Optimisation
- Dead variables
- Confluence
Contents

1 Introduction

2 A process algebra with data and probability: prCRL

3 Linear probabilistic process equations

4 Case study: leader election protocol

5 Confluence reduction

6 Conclusions and Future Work
A process algebra with data and probability: prCRL

Specification language prCRL:

- Based on $\mu$CRL (so data), with additional probabilistic choice
- Semantics defined in terms of probabilistic automata
- Minimal set of operators to facilitate formal manipulation
- Syntactic sugar easily definable
A process algebra with data and probability: prCRL

Specification language prCRL:
- Based on $\mu$CRL (so data), with additional probabilistic choice
- Semantics defined in terms of probabilistic automata
- Minimal set of operators to facilitate formal manipulation
- Syntactic sugar easily definable

The grammar of prCRL process terms

Process terms in prCRL are obtained by the following grammar:

$$p ::= Y(t) \mid c \Rightarrow p \mid p + p \mid \sum_{x:D} p \mid a(t)\sum_{x:D} f : p$$

Process equations and processes

A process equation is something of the form $X(\vec{g} : \vec{G}) = p$. 
An example specification

Sending an arbitrary natural number

\[ X(\text{active} : \text{Bool}) = \]

not(\text{active}) \Rightarrow \text{ping} \cdot \sum_{b : \text{Bool}} X(b)

\[ \begin{array}{c}
\text{+ active} \Rightarrow \tau \sum_{n : \mathbb{N} > 0} \frac{1}{2^n} : \left( \text{send}(n) \cdot X(\text{false}) \right)
\end{array} \]
An example specification

Sending an arbitrary natural number

\[
X(\text{active} : \text{Bool}) =
\]

\[
\text{not(}\text{active}\text{)} \Rightarrow \text{ping} \cdot \sum_{b:\text{Bool}} X(b)
\]

\[
+ \text{active} \Rightarrow \tau \sum_{n:\mathbb{N} > 0} \frac{1}{2^n} : \left( \text{send}(n) \cdot X(\text{false}) \right)
\]

Diagram:

- \(X(\text{false})\)
- \(\sum_{b:\text{Bool}} X(b)\)
- \(\text{ping}\)
- \(\tau\)
- \(\text{send}(1)\)
- \(\text{send}(2)\)
- Probability edges:
  - 0.5
  - 0.25
  - ...
Compositionality using extended prCRL

For compositionality we introduce extended prCRL. It extends prCRL by parallel composition, encapsulation, hiding and renaming.
Compositionality using extended prCRL

For compositionality we introduce extended prCRL. It extends prCRL by parallel composition, encapsulation, hiding and renaming.

\[
X(n : \{1, 2\}) = \text{write}_X(n) \cdot X(n) + \text{choose} \sum_{n' : \{1, 2\}} \frac{1}{2} : X(n')
\]

\[
Y(m : \{1, 2\}) = \text{write}_Y(m^2) \cdot Y(m) + \text{choose}' \sum_{m' : \{1, 2\}} \frac{1}{2} : Y(m')
\]
Compositionality using extended prCRL

For compositionality we introduce extended prCRL. It extends prCRL by parallel composition, encapsulation, hiding and renaming.

\[
X(n : \{1, 2\}) = \text{write}_X(n) \cdot X(n) + \text{choose} \sum_{n' : \{1, 2\}} \frac{1}{2} : X(n')
\]

\[
Y(m : \{1, 2\}) = \text{write}_Y(m^2) \cdot Y(m) + \text{choose}' \sum_{m' : \{1, 2\}} \frac{1}{2} : Y(m')
\]

\[
Z = (X(1) \parallel Y(2))
\]
Compositionality using extended prCRL

For compositionality we introduce extended prCRL. It extends prCRL by parallel composition, encapsulation, hiding and renaming.

\[
X(n : \{1, 2\}) = \text{write}_X(n) \cdot X(n) + \text{choose} \sum_{n':\{1,2\}} \frac{1}{2} : X(n') \\
Y(m : \{1, 2\}) = \text{write}_Y(m^2) \cdot Y(m) + \text{choose}' \sum_{m':\{1,2\}} \frac{1}{2} : Y(m')
\]

\[
Z = (X(1) \parallel Y(2)) \\
\gamma(\text{choose, choose'}) = \text{chooseTogether}
\]
Compositionality using extended prCRL

For compositionality we introduce extended prCRL. It extends prCRL by parallel composition, encapsulation, hiding and renaming.

\[
X(n : \{1, 2\}) = \text{write}_{X(n)} \cdot X(n) + \text{choose} \sum_{n' : \{1, 2\}} \frac{1}{2} : X(n')
\]

\[
Y(m : \{1, 2\}) = \text{write}_{Y(m^2)} \cdot Y(m) + \text{choose'} \sum_{m' : \{1, 2\}} \frac{1}{2} : Y(m')
\]

\[
Z = \partial_{\{\text{choose, choose'}\}}(X(1) \parallel Y(2))
\]

\[
\gamma(\text{choose, choose'}) = \text{chooseTogether}
\]
Compositionality using extended prCRL

For compositionality we introduce extended prCRL. It extends prCRL by parallel composition, encapsulation, hiding and renaming.

\[ X(n : \{1, 2\}) = \text{write}_X(n) \cdot X(n) + \text{choose} \sum_{n' : \{1, 2\}} \frac{1}{2} : X(n') \]

\[ Y(m : \{1, 2\}) = \text{write}_Y(m^2) \cdot Y(m) + \text{choose}' \sum_{m' : \{1, 2\}} \frac{1}{2} : Y(m') \]

\[ Z = \partial_{\{\text{choose}, \text{choose}'\}} (X(1) \parallel Y(2)) \]

\[ \gamma(\text{choose, choose}') = \text{chooseTogether} \]
Contents

1 Introduction

2 A process algebra with data and probability: prCRL

3 Linear probabilistic process equations

4 Case study: leader election protocol

5 Confluence reduction

6 Conclusions and Future Work
A linear format for prCRL: the LPPE

LPPEs are a subset of prCRL specifications:

\[
X(\vec{g} : \vec{G}) = \sum_{\vec{d}_1 : \vec{D}_1} c_1 \Rightarrow a_1(b_1) \sum_{\vec{e}_1 : \vec{E}_1} f_1 : X(\vec{n}_1) \\
\ldots \\
+ \sum_{\vec{d}_k : \vec{D}_k} c_k \Rightarrow a_k(b_k) \sum_{\vec{e}_k : \vec{E}_k} f_k : X(\vec{n}_k)
\]
A linear format for prCRL: the LPPE

LPPEs are a subset of prCRL specifications:

\[
X(\vec{g} : \vec{G}) = \sum_{\vec{d}_1 : \vec{D}_1} c_1 \Rightarrow a_1(b_1) \sum_{\vec{e}_1 : \vec{E}_1} f_1 : X(\vec{n}_1)
\]

\[
\ldots
\]

\[
+ \sum_{\vec{d}_k : \vec{D}_k} c_k \Rightarrow a_k(b_k) \sum_{\vec{e}_k : \vec{E}_k} f_k : X(\vec{n}_k)
\]

Advantages of using LPPEs instead of prCRL specifications:

- Easy state space generation
- Straight-forward parallel composition
- **Symbolic optimisations** enabled at the language level
A linear format for prCRL: the LPPE

LPPEs are a subset of prCRL specifications:

\[
X(\vec{g} : \vec{G}) = \sum_{\vec{d}_1 : \vec{D}_1} c_1 \Rightarrow a_1(b_1) \sum_{\vec{e}_1 : \vec{E}_1} f_1 : X(\vec{n}_1) \\
\ldots \\
+ \sum_{\vec{d}_k : \vec{D}_k} c_k \Rightarrow a_k(b_k) \sum_{\vec{e}_k : \vec{E}_k} f_k : X(\vec{n}_k)
\]

Advantages of using LPPEs instead of prCRL specifications:
- Easy state space generation
- Straight-forward parallel composition
- **Symbolic optimisations** enabled at the language level

**Theorem**

*Every specification (without unguarded recursion) can be linearised to an LPPE, preserving strong probabilistic bisimulation.*
Linear probabilistic process equations – An example

Specification in prCRL

\[ X(\text{active} : \text{Bool}) = \]
\[ \text{not(}\text{active}\text{)} \Rightarrow \text{ping} \cdot \sum_{b: \text{Bool}} X(b) \]
\[ + \text{active} \Rightarrow \tau \sum_{n: \mathbb{N} \geq 0} \frac{1}{2^n} : \text{send}(n) \cdot X(\text{false}) \]
Linear probabilistic process equations – An example

**Specification in prCRL**

\[ X(\text{active} : \text{Bool}) = \]
\[ \text{not(\text{active}) } \Rightarrow \text{ping} \cdot \sum_{b: \text{Bool}} X(b) \]
\[ + \text{active } \Rightarrow \tau \sum_{n: \mathbb{N} \geq 0} \frac{1}{2^n} : \text{send}(n) \cdot X(\text{false}) \]

**Specification in LPPE**

\[ X(pc : \{1..3\}, n : \mathbb{N} \geq 0) = \]
\[ + pc = 1 \Rightarrow \text{ping} \cdot X(2, 1) \]
\[ + pc = 2 \Rightarrow \text{ping} \cdot X(2, 1) \]
\[ + pc = 2 \Rightarrow \tau \sum_{n: \mathbb{N} \geq 0} \frac{1}{2^n} : X(3, n) \]
\[ + pc = 3 \Rightarrow \text{send}(n) \cdot X(1, 1) \]
Contents

1. Introduction

2. A process algebra with data and probability: prCRL

3. Linear probabilistic process equations

4. Case study: leader election protocol

5. Confluence reduction

6. Conclusions and Future Work
Case study: a leader election protocol

- **Implementation** in Haskell:
  - Linearisation: from prCRL to LPPE
  - Parallel composition of LPPEs, hiding, renaming, encapsulation
  - Generation of the state space of an LPPE
  - Automatic constant elimination and summand simplification

- Manual **dead variable reduction**
Case study: a leader election protocol

- Implementation in Haskell:
  - Linearisation: from prCRL to LPPE
  - Parallel composition of LPPEs, hiding, renaming, encapsulation
  - Generation of the state space of an LPPE
  - Automatic constant elimination and summand simplification
- Manual dead variable reduction

Case study

Leader election protocol à la Itai-Rodeh

- Two processes throw a die
  - One of them throws a 6 → this will be the leader
  - Both throw 6 or neither throws 6 → throw again
Case study: a leader election protocol

- **Implementation** in Haskell:
  - Linearisation: from prCRL to LPPE
  - Parallel composition of LPPEs, hiding, renaming, encapsulation
  - Generation of the state space of an LPPE
  - Automatic constant elimination and summand simplification

- **Manual dead variable reduction**

---

**Case study**

Leader election protocol à la Itai-Rodeh

- Two processes throw a **die**
  - *One of them throws a 6* → *this will be the leader*
  - *Both throw 6 or neither throws 6* → *throw again*

- More precise:
  - **Passive thread**: receive value of opponent
  - **Active thread**: roll, send, compare (or block)
A prCRL model of the leader election protocol

\[ P(id : \{1, 2\}, val : Die, set : Bool) = \]
A prCRL model of the leader election protocol

\[
P(id : \{1, 2\}, val : Die, set : Bool) = \\
set = false \Rightarrow \sum_{d : Die} \text{rec}(id, \text{other}(id), d) \cdot P(id, d, true)
\]
A prCRL model of the leader election protocol

\[ P(id: \{1, 2\}, val: Die, set: Bool) = \]

\[ set = false \Rightarrow \sum_{d:Die} rec(id, other(id), d) \cdot P(id, d, true) \]

\[ + set = true \Rightarrow getVal(val) \cdot P(id, val, false) \]
A prCRL model of the leader election protocol

\[ P(id : \{1, 2\}, val : Die, set : Bool) = \]
\[ set = false \Rightarrow \sum_{d : Die} rec(id, other(id), d) \cdot P(id, d, true) \]
\[ + set = true \Rightarrow getVal(val) \cdot P(id, val, false) \]
\[ A(id : \{1, 2\}) = \]
A prCRL model of the leader election protocol

\[
P(id : \{1, 2\}, val : Die, set : Bool) =
\]
\[
  \begin{align*}
  \text{set} = \text{false} & \Rightarrow \sum_{d : \text{Die}} \text{rec}(id, \text{other}(id), d) \cdot P(id, d, \text{true}) \\
  + \quad \text{set} = \text{true} & \Rightarrow \text{getVal}(val) \cdot P(id, val, \text{false})
\end{align*}
\]

\[
A(id : \{1, 2\}) =
\]
\[
  \text{roll}(id) \sum_{d : \text{Die}} \frac{1}{6} : \text{send}(\text{other}(id), id, d) \cdot \sum_{e : \text{Die}} \text{readVal}(e) \cdot 
\]
A prCRL model of the leader election protocol

\[ P(id : \{1, 2\}, val : Die, set : Bool) = \]
\[ \text{set} = \text{false} \Rightarrow \sum_{d:Die} \text{rec}(id, \text{other}(id), d) \cdot P(id, d, true) \]
\[ + \text{set} = \text{true} \Rightarrow \text{getVal}(val) \cdot P(id, val, false) \]

\[ A(id : \{1, 2\}) = \]
\[ \text{roll}(id) \sum_{d:Die} \frac{1}{6} : \text{send}(\text{other}(id), id, d) \cdot \sum_{e:Die} \text{readVal}(e) \cdot \]

UNIVERSITY OF TWENTE.

Symbolic reductions of probabilistic models

March 8, 2010 15 / 30
A prCRL model of the leader election protocol

\[
P(id : \{1, 2\}, val : \text{Die}, set : \text{Bool}) =
\]

\[
set = \text{false} \Rightarrow \sum_{d:\text{Die}} \text{rec}(id, \text{other}(id), d) \cdot P(id, d, \text{true})
\]

\[
+ set = \text{true} \Rightarrow \text{getVal}(val) \cdot P(id, val, \text{false})
\]

\[
A(id : \{1, 2\}) =
\]

\[
\text{roll}(id) \cdot \sum_{d:\text{Die}} \frac{1}{6} : \text{send}(\text{other}(id), id, d) \cdot \sum_{e:\text{Die}} \text{readVal}(e) \cdot
\]

\[
( (d = e \lor (d \neq 6 \land e \neq 6) \Rightarrow A(id))
\]

\[
+ (d = 6 \land e \neq 6 \Rightarrow \text{leader}(id) \cdot A(id))
\]

\[
+ (e = 6 \land d \neq 6 \Rightarrow \text{follower}(id) \cdot A(id))
\]
A prCRL model of the leader election protocol

\[
P(id : \{1, 2\}, val : Die, set : Bool) =
\]
\[
\begin{align*}
set = false & \Rightarrow \sum_{d : Die} rec(id, other(id), d) \cdot P(id, d, true) \\
+ set = true & \Rightarrow getVal(val) \cdot P(id, val, false)
\end{align*}
\]

\[
A(id : \{1, 2\}) =
\]
\[
\begin{align*}
roll(id) \sum_{d : Die} \frac{1}{6} : send(other(id), id, d) \cdot \sum_{e : Die} readVal(e) \cdot \\
( d = e \lor (d \neq 6 \land e \neq 6) \Rightarrow A(id)) \\
+ (d = 6 \land e \neq 6 \Rightarrow leader(id) \cdot A(id)) \\
+ (e = 6 \land d \neq 6 \Rightarrow follower(id) \cdot A(id))
\end{align*}
\]

\[
C(id : \{1, 2\}) =
\]
\[
P(id, heads, false) || A(id)
\]
A prCRL model of the leader election protocol

\[
P(id : \{1, 2\}, \ val : \text{Die}, \ set : \text{Bool}) =
\]
\[
\begin{align*}
set = \text{false} \Rightarrow & \sum_{d : \text{Die}} \text{rec}(id, \text{other}(id), d) \cdot P(id, d, \text{true}) \\
+ \ set = \text{true} \Rightarrow & \text{getVal}(\val) \cdot P(id, \val, \text{false})
\end{align*}
\]

\[
A(id : \{1, 2\}) =
\]
\[
\text{roll}(id) \sum_{d : \text{Die}} \frac{1}{6} : \text{send}(\text{other}(id), id, d) \cdot \sum_{e : \text{Die}} \text{readVal}(e) \cdot \\
( (d = e \lor (d \neq 6 \land e \neq 6) \Rightarrow A(id)) \\
+ (d = 6 \land e \neq 6 \Rightarrow \text{leader}(id) \cdot A(id)) \\
+ (e = 6 \land d \neq 6 \Rightarrow \text{follower}(id) \cdot A(id)))
\]

\[
C(id : \{1, 2\}) = \ P(id, \text{heads}, \text{false}) \ || \ A(id)
\]

\[
\gamma(\text{getVal}, \text{readVal}) = \text{checkVal}
\]
A prCRL model of the leader election protocol

\[ P(id : \{1, 2\}, val : \text{Die}, set : \text{Bool}) = \]
\[ \text{set} = \text{false} \Rightarrow \sum_{d : \text{Die}} \text{rec}(id, \text{other}(id), d) \cdot P(id, d, \text{true}) \]
\[ + \text{set} = \text{true} \Rightarrow \text{getVal}(val) \cdot P(id, val, \text{false}) \]

\[ A(id : \{1, 2\}) = \]
\[ \text{roll}(id) \sum_{d : \text{Die}} \frac{1}{6} : \text{send}(\text{other}(id), id, d) \cdot \sum_{e : \text{Die}} \text{readVal}(e) \cdot \]
\[ (d = e \lor (d \neq 6 \land e \neq 6) \Rightarrow A(id)) \]
\[ + (d = 6 \land e \neq 6 \Rightarrow \text{leader}(id) \cdot A(id)) \]
\[ + (e = 6 \land d \neq 6 \Rightarrow \text{follower}(id) \cdot A(id)) \]

\[ C(id : \{1, 2\}) = \partial_{\text{getVal, readVal}}(P(id, \text{heads}, \text{false}) || A(id)) \]

\[ \gamma(\text{getVal, readVal}) = \text{checkVal} \]
A prCRL model of the leader election protocol

\[ P(id : \{1, 2\}, val : Die, set : Bool) = \]
\[ \text{set} = \text{false} \Rightarrow \sum_{d:Die} \text{rec}(id, \text{other}(id), d) \cdot P(id, d, \text{true}) \]
\[ + \text{set} = \text{true} \Rightarrow \text{getVal}(val) \cdot P(id, val, false) \]

\[ A(id : \{1, 2\}) = \]
\[ \text{roll}(id) \sum_{d:Die} \frac{1}{6} : \text{send}(\text{other}(id), id, d) \cdot \sum_{e:Die} \text{readVal}(e) \cdot \]
\[ (d = e \lor (d \neq 6 \land e \neq 6) \Rightarrow A(id)) \]
\[ + (d = 6 \land e \neq 6 \Rightarrow \text{leader}(id) \cdot A(id)) \]
\[ + (e = 6 \land d \neq 6 \Rightarrow \text{follower}(id) \cdot A(id)) \]

\[ C(id : \{1, 2\}) = \partial_{\text{getVal}, \text{readVal}}(P(id, heads, false) || A(id)) \]
\[ S = C(1) || C(2) \]

\[ \gamma(\text{getVal, readVal}) = \text{checkVal} \]
A prCRL model of the leader election protocol

\[ P(id: \{1, 2\}, \text{val: } \text{Die}, \text{set: } \text{Bool}) = \]
\[ \text{set} = \text{false} \Rightarrow \sum_{d: \text{Die}} \text{rec}(id, \text{other}(id), d) \cdot P(id, d, \text{true}) \]
\[ + \text{set} = \text{true} \Rightarrow \text{getVal}(\text{val}) \cdot P(id, \text{val}, \text{false}) \]
\[ A(id: \{1, 2\}) = \]
\[ \text{roll}(id) \sum_{d: \text{Die}} \frac{1}{6} : \text{send}(\text{other}(id), id, d) \cdot \sum_{e: \text{Die}} \text{readVal}(e) \cdot \]
\[ ( (d = e \lor (d \neq 6 \land e \neq 6) \Rightarrow A(id)) \]
\[ + (d = 6 \land e \neq 6 \Rightarrow \text{leader}(id) \cdot A(id)) \]
\[ + (e = 6 \land d \neq 6 \Rightarrow \text{follower}(id) \cdot A(id)) ) \]
\[ C(id: \{1, 2\}) = \partial_{\text{getVal, readVal}}(P(id, \text{heads, false}) \parallel A(id)) \]
\[ S = \quad C(1) \parallel C(2) \]
\[ \gamma(\text{rec, send}) = \text{comm} \quad \gamma(\text{getVal, readVal}) = \text{checkVal} \]
A prCRL model of the leader election protocol

\[ P(id : \{1, 2\}, val : \text{Die}, set : \text{Bool}) = \]
\[ \text{set} = \text{false} \Rightarrow \sum_{d:\text{Die}} \text{rec}(id, \text{other}(id), d) \cdot P(id, d, \text{true}) \]
\[ + \text{set} = \text{true} \Rightarrow \text{getVal}(val) \cdot P(id, val, \text{false}) \]

\[ A(id : \{1, 2\}) = \]
\[ \text{roll}(id) \sum_{d:\text{Die}} \frac{1}{6} : \text{send}(\text{other}(id), id, d) \cdot \sum_{e:\text{Die}} \text{readVal}(e) \cdot \]
\[ (d = e \lor (d \neq 6 \land e \neq 6) \Rightarrow A(id)) \]
\[ + (d = 6 \land e \neq 6 \Rightarrow \text{leader}(id) \cdot A(id)) \]
\[ + (e = 6 \land d \neq 6 \Rightarrow \text{follower}(id) \cdot A(id)) \]

\[ C(id : \{1, 2\}) = \partial_{\text{getVal}, \text{readVal}}(P(id, \text{heads}, \text{false}) \mid\mid A(id)) \]

\[ S = \partial_{\text{send}, \text{rec}}(C(1) \mid\mid C(2)) \]

\[ \gamma(\text{rec}, \text{send}) = \text{comm} \quad \gamma(\text{getVal}, \text{readVal}) = \text{checkVal} \]
Reductions on the leader election protocol model

In order to obtain reductions first linearise
Reductions on the leader election protocol model

In order to obtain reductions first linearise:

\[
\sum_{e21:D} pc21 = 3 \land pc11 = 1 \land set11 \land val11 = e21 \Rightarrow
\]

\[
\text{checkVal}(val11) \quad \sum_{(k1,k2):\{\ast\} \times \{\ast\}} \text{multiply}(1.0, 1.0):
\]

\[
Z(1, id11, val11, false, 1, 4, id21, d21, e21, pc12, id12, val12, set12, d12, pc22, id22, d22, e22)
\]
Reductions on the leader election protocol model

In order to obtain reductions first linearise:

\[
\sum_{e21:D} pc21 = 3 \land pc11 = 1 \land set11 \land val11 = e21 \Rightarrow \\
\text{checkVal}(val11) \sum multiply(1.0, 1.0): \\
(k1,k2):\{*\} \times \{*\} \\
Z(1, id11, val11, false, 1, 4, id21, d21, e21, \\
pc12, id12, val12, set12, d12, pc22, id22, d22, e22)
\]

Before reductions:

- 18 parameters
- 14 summands
- 3423 states
- 5478 transitions

After reductions:

- 10 parameters
- 12 summands
- 1613 states (-53%)
- 2278 transitions (-58%)
Reductions on the leader election protocol model

In order to obtain reductions first linearise:

\[
\begin{align*}
pc21 &= 3 \land \quad set11 \\
\sum (k1,k2):\{\ast}\times\{\ast}\quad &1.0: \\
checkVal(val11) &\Rightarrow \\
Z(val11, false, 4, d21, val11, \\
val12, set12, pc22, d22, e22)
\end{align*}
\]

Before reductions:
- 18 parameters
- 14 summands
- 3423 states
- 5478 transitions

After reductions:
- 10 parameters
- 12 summands
Reductions on the leader election protocol model

In order to obtain reductions first linearise:

\[ pc21 = 3 \land \quad set11 \quad \Rightarrow \quad checkVal(val11) \sum_{(k1,k2) : \{\ast\} \times \{\ast\}} 1.0: \]

\[ Z(1, \text{false}, 4, d21, val11, \]
\[ val12, set12, pc22, d22, e22) \]

Before reductions:
- 18 parameters
- 14 summands
- 3423 states
- 5478 transitions

After reductions:
- 10 parameters
- 12 summands
- 1613 states (-53%)
- 2278 transitions (-58%)
Contents

1 Introduction

2 A process algebra with data and probability: prCRL

3 Linear probabilistic process equations

4 Case study: leader election protocol

5 Confluence reduction

6 Conclusions and Future Work
Overview of confluence reduction

Strong probabilistic bisimulation is sometimes too restrictive.
Overview of confluence reduction

Strong probabilistic bisimulation is sometimes too restrictive.

Confluence reduction: efficiently reducing specifications while preserving branching probabilistic bisimulation.
Overview of confluence reduction

Strong probabilistic bisimulation is sometimes too restrictive.

**Confluence reduction**: efficiently reducing specifications while preserving branching probabilistic bisimulation.

Intuition:
Overview of confluence reduction

Strong probabilistic bisimulation is sometimes too restrictive.

**Confluence reduction**: efficiently reducing specifications while preserving branching probabilistic bisimulation.

Intuition:

![Diagram](image-url)
Overview of confluence reduction

Strong probabilistic bisimulation is sometimes too restrictive.

**Confluence reduction**: efficiently reducing specifications while preserving branching probabilistic bisimulation.

Intuition:

![Diagram](image_url)
Overview of confluence reduction

Strong probabilistic bisimulation is sometimes too restrictive.

**Confluence reduction**: efficiently reducing specifications while preserving branching probabilistic bisimulation.

Intuition:

\[
\begin{array}{ccc}
\bullet & \xrightarrow{\tau_c} & \bullet \\
\downarrow & & \downarrow \\
\bullet & \xrightarrow{a} & \bullet \\
\end{array}
\quad \begin{array}{ccc}
\bullet & \xrightarrow{\tau} & \bullet \\
\downarrow & & \downarrow \\
\bullet & \xrightarrow{a} & \bullet \\
\end{array}
\]
Overview of confluence reduction

Strong probabilistic bisimulation is sometimes too restrictive.

**Confluence reduction**: efficiently reducing specifications while preserving branching probabilistic bisimulation.

Intuition:

\[
\begin{align*}
\text{a} & \xrightarrow{\tau_{C}} \text{a} \\
\text{a} & \xrightarrow{\tau_{C}} \text{a}
\end{align*}
\]
Variants of confluence

- Weak confluence
- Confluence
- Strong confluence
Examples

Reduction based on strong confluence

Graphical representation of reduction based on strong confluence.
Examples

Reduction based on strong confluence

\[ a \xrightarrow{\tau} c \]

\[ c \xrightarrow{\tau} a \]

\[ a \xrightarrow{\tau} b \]

Giving \( \tau \) steps priority works because of the absence of \( \tau \) loops.
Examples

Reduction based on strong confluence

![Diagram showing reduction based on strong confluence]
Examples

Reduction based on strong confluence

\[
\begin{align*}
    & a \\
    & \tau \\
    & c & \tau_c \\
    & \tau_c & c & \tau_c \\
    & \tau_c & \bar{a} & \tau_c \\
    & \tau_c & \bar{a} & \tau_c \\
    & \tau_c & \bar{a} & \tau_c \\
\end{align*}
\]
Examples

Reduction based on strong confluence

Giving steps priority works because of the absence of loops.
Examples

Reduction based on strong confluence

\[
\begin{align*}
\tau_c &\quad a \\
\tau_c &\quad \tau_c \\
\tau_c &\quad \tau_c \\
\tau_c &\quad \tau_c \\
\end{align*}
\]
Examples

Reduction based on strong confluence

- Giving \( \tau_c \) steps priority works because of the absence of \( \tau_c \) loops.
Examples

Reduction based on strong confluence

![Reduction diagram](image)
Examples

Reduction based on strong confluence
Examples

Reduction based on strong confluence

Giving $\tau_c$ steps priority works because of the absence of $\tau_c$ loops.
Examples

Reduction based on weak confluence

[Diagram showing a graph with nodes and edges labeled with \( \tau \) and \( a, b \).]
Examples

Reduction based on weak confluence

\[
\begin{align*}
\tau_c & \xrightarrow{\tau} \tau_c \\
\tau_c & \xrightarrow{\tau} \tau_c \\
\tau_c & \xrightarrow{\tau} \tau_c
\end{align*}
\]

Here we used the equivalence classes of \( A / \tau_c \xrightarrow{} \) as nodes. (None of the blue nodes could be chosen as representative, as none of them can do both an \( a \) and \( b \) transition.)
Examples

Reduction based on weak confluence

![Diagram showing reduction based on weak confluence](image)
Examples

Reduction based on weak confluence

\[ \tau_c \rightarrow \tau \rightarrow \tau \]

Here we used the equivalence classes of \( A/\tau_c \) as nodes. (None of the blue nodes could be chosen as representative, as none of them can do both an \( a \) and a \( b \) transition.)
Examples

Reduction based on weak confluence

\[
\begin{align*}
\tau_c & \quad \tau \\
\tau_c & \quad \tau \\
a & \quad b
\end{align*}
\]
Examples

Reduction based on weak confluence

Here we used the equivalence classes of $A/\tau_c \xleftrightarrow{}$ as nodes.
(None of the blue nodes could be chosen as representative, as none of them can do both an $a$ and $b$ transition.)
Examples

Reduction based on weak confluence

Reduction based on weak confluence

\[ \tau_c \]

\[ a \]

\[ b \]

\[ \bar{a} \]

\[ \tau_c \]

\[ \tau_c \]

\[ \tau_c \]

\[ \tau_c \]

\[ \tau_c \]

\[ \tau_c \]

\[ \tau_c \]

\[ \tau_c \]
Examples

Reduction based on weak confluence

![Diagram showing reduction based on weak confluence]
Examples

Reduction based on weak confluence

Here we used the equivalence classes of $\mathcal{A}/\ll\overset{\tau_c}{\llra}$ as nodes.
(None of the blue nodes could be chosen as representative, as none of them can do both an $a$ and an $a$ transition.)
Examples

Reduction based on confluence using representatives

\[
\begin{array}{c}
a \
\tau \rightarrow b \\
a \
\tau \rightarrow b \\
\tau \rightarrow a \\
\tau \rightarrow a \\
\end{array}
\]
Examples

Reduction based on confluence using representatives
Examples

Reduction based on confluence using representatives
Examples

Reduction based on confluence using representatives

\[
\begin{array}{c}
\text{a} \\
\tau \\
\text{b} \\
\end{array}
\]
Examples

Reduction based on confluence using representatives

![Diagram showing reduction based on confluence using representatives](image-url)
Examples

Reduction based on confluence using representatives

\[ \begin{array}{c}
 a \\
\tau_c \\
 a \\
\tau_c \\
\tau_c \\
 b \\
\tau_c \\
 b \\
\tau_c \\
\tau_c \\
 a \\
\end{array} \]
Examples

Reduction based on confluence using representatives

![Diagram showing reduction based on confluence using representatives](image-url)
Examples

Reduction based on confluence using representatives

![Diagram showing reduction based on confluence using representatives]
Examples

Reduction based on confluence using representatives
Examples

Reduction based on confluence using representatives
Examples

Reduction based on confluence using representatives

\[ \begin{align*}
\tau_c & \quad \rightarrow \quad \bar{a} \\
\tau_c & \quad \rightarrow \quad \tau_c \\
\tau_c & \quad \rightarrow \quad \tau_c \\
\end{align*} \]
For simplicity we only consider strong confluence from now on.

Non-probabilistic:

\[ \tau_c \]

\[ a \]

\[ \overline{a} \]

\[ \overline{\tau_c} \]
For simplicity we only consider strong confluence from now on.

Non-probabilistic:

\[
\begin{align*}
\text{a} & \xrightarrow{\tau_c} \text{\bar{a}} \\
\text{\bar{a}} & \xrightarrow{\tau_c} \text{a}
\end{align*}
\]

Probabilistic:

\[
\begin{align*}
\text{a} \xrightarrow{1/2} \text{\bar{a}} \\
\text{\bar{a}} \xrightarrow{1/2} \text{a}
\end{align*}
\]
Confluence for probabilistic automata

For simplicity we only consider strong confluence from now on.

Non-probabilistic:

\[ \begin{array}{c}
\tau_c \\
a \\
\overline{\tau_c} \\
\end{array} \quad \begin{array}{c}
\overline{a} \\
\tau_c \\
a \\
\end{array} \]

Probabilistic:

\[ \begin{array}{c}
\frac{1}{2}a \\
\frac{1}{2}a \\
\frac{1}{3}a \\
\frac{1}{6}a \\
\frac{1}{2}a \\
\end{array} \]

\[ \begin{array}{c}
\frac{1}{2}a \\
\frac{1}{2} \\
\frac{1}{2} \\
\frac{1}{3} \\
\frac{1}{6} \\
\frac{1}{2} \\
\end{array} \]
For simplicity we only consider strong confluence from now on.
Why $\tau_c$ steps should have a Dirac distribution
Why $\tau_c$ steps should have a Dirac distribution
Why $\tau_c$ steps should have a Dirac distribution
Why $\tau_c$ steps should have a Dirac distribution
Why $\tau_c$ steps should have a Dirac distribution
Why $\tau_c$ steps should have a Dirac distribution

As all states are (potentially) different, no reduction can be obtained.
Detecting confluence using LPPEs

Given an LPPE, confluence can be detected using theorem proving.

\[
X(\vec{g} : \vec{G}) = \sum_{\vec{d}_1 : \vec{D}_1} c_1 \Rightarrow \tau \sum_{\vec{e}_1 : \vec{E}_1} f_1 : X(\vec{n}_1) \\
\ldots \\
+ \sum_{\vec{d}_k : \vec{D}_k} c_k \Rightarrow a_k(b_k) \sum_{\vec{e}_k : \vec{E}_k} f_k : X(\vec{n}_k)
\]

To check the first \(\tau\)-summand is confluent, we check whether indeed

- \(|E_1| = 1\), or \(f_1 = 1.0\) for one \(e_i \in E_1\).
- the summand is confluent with all other summands.
Detecting confluence using LPPEs

\[ X(\vec{g} : \vec{G}) = \sum_{\vec{d}_1 : \vec{D}_1} c_1 \Rightarrow \tau \cdot X(\vec{n}_1) \]

\[ \ldots \]

\[ + \sum_{\vec{d}_k : \vec{D}_k} c_k \Rightarrow a_k(b_k) \sum_{\vec{e}_k : \vec{E}_k} f_k : X(\vec{n}_k) \]
Detecting confluence using LPPEs

\[ X(\vec{g} : \vec{G}) = \sum_{\vec{d}_1 : \vec{D}_1} c_1 \Rightarrow \tau \cdot X(\vec{n}_1) \]
\[ \ldots \]
\[ + \sum_{\vec{d}_k : \vec{D}_k} c_k \Rightarrow a_k(b_k) \sum_{\vec{e}_k : \vec{E}_k} f_k : X(\vec{n}_k) \]

To prove:
\[ c_1(g, d_1) \land c_k(g, d_k) \rightarrow \]
Detecting confluence using LPPEs

\[
X(\vec{g} : \vec{G}) = \sum_{\vec{d}_1 : \vec{D}_1} c_1 \Rightarrow \tau \cdot X(\vec{n}_1) \\
\hspace{1cm} \ldots \ldots \\
+ \sum_{\vec{d}_k : \vec{D}_k} c_k \Rightarrow a_k(\vec{b}_k) \sum_{\vec{e}_k : \vec{E}_k} f_k : X(\vec{n}_k)
\]

To prove:

\[
c_1(g, d_1) \land c_k(g, d_k) \rightarrow \\
\phantom{c_1(g, d_1) \land c_k(g, d_k) \rightarrow} c_k(n_1(g, d_1), d_k)
\]
Detecting confluence using LPPEs

$$X(\vec{g} : \vec{G}) = \sum_{\vec{d}_1 : \vec{D}_1} c_1 \Rightarrow \tau \cdot X(\vec{n}_1)$$

$$+ \sum_{\vec{d}_k : \vec{D}_k} c_k \Rightarrow a_k(b_k) \sum_{\vec{e}_k : \vec{E}_k} f_k : X(\vec{n}_k)$$

To prove:

$$c_1(g, d_1) \land c_k(g, d_k) \rightarrow$$

$$\left( \begin{array}{l}
    c_k(n_1(g, d_1), d_k) \\
    \land c_1(n_k(g, d_k, e_k), d_1)
\end{array} \right)$$
Detecting confluence using LPPEs

\[ X(\vec{g} : \vec{G}) = \sum_{\vec{d}_1 : \vec{D}_1} c_1 \Rightarrow \tau \cdot X(\vec{n}_1) \]
\[ \ldots \]
\[ + \sum_{\vec{d}_k : \vec{D}_k} c_k \Rightarrow a_k(b_k) \sum_{\vec{f}_k : \vec{E}_k} f_k : X(\vec{n}_k) \]

To prove:

\[ c_1(g, d_1) \land c_k(g, d_k) \rightarrow \]
\[ \left( c_k(n_1(g, d_1), d_k) \right) \land c_1(n_k(g, d_k, e_k), d_1) \land a_k(g, d_k) = a_k(n_1(g, d_1), d_k) \]
Detecting confluence using LPPEs

\[ X(\vec{g} : \vec{G}) = \sum_{\vec{d}_1 : \vec{D}_1} c_1 \Rightarrow \tau \cdot X(\vec{n}_1) \]

\[ + \sum_{\vec{d}_k : \vec{D}_k} c_k \Rightarrow a_k(b_k) \sum_{\vec{e}_k : \vec{E}_k} f_k : X(\vec{n}_k) \]

To prove:

\[ c_1(g, d_1) \land c_k(g, d_k) \rightarrow \]

\[ \left( c_k(n_1(g, d_1), d_k) \land c_1(n_k(g, d_k, e_k), d_1) \land a_k(g, d_k) = a_k(n_1(g, d_1), d_k) \land n_k(n_1(g, d_1), d_k, e_k) = n_1(n_k(g, d_k, e_k), d_1) \right) \]
Reducing LPPEs based on confluent $\tau$ steps

After $\tau_c$ steps have been identified, two types of reductions are possible:

1. **Symbolic prioritisation: change the LPPE**
   - Let $c$ be a confluent summand
   - Find a non-confluent summand $n$ such that $c$ is always enabled after executing $n$
   - Change the next state of $n$, basically merging $n$ and $c$

As we only do this for non-confluent summands, loops are avoided.
Reducing LPPEs based on confluent $\tau$ steps

After $\tau_c$ steps have been identified, two types of reductions are possible:

1. **Symbolic prioritisation: change the LPPE**
   - Let $c$ be a confluent summand
   - Find a non-confluent summand $n$ such that $c$ is always enabled after executing $n$
   - Change the next state of $n$, basically merging $n$ and $c$

   As we only do this for non-confluent summands, loops are avoided.

2. **On-the-fly state space generation using representatives**
   - Generate the state space from the LPPE
   - For each transition that is visited, go to the representative of the target state
   - When no representative is known yet, compute it (using a variation on Tarjan’s SCC algorithm)
Contents

1 Introduction

2 A process algebra with data and probability: prCRL

3 Linear probabilistic process equations

4 Case study: leader election protocol

5 Confluence reduction

6 Conclusions and Future Work
Conclusions and Future Work

Conclusions / Results

- We developed the process algebra prCRL, incorporating both data and probability.
- We defined a normal form for prCRL, the LPPE; starting point for symbolic optimisations and easy state space generation.
- We generalised reduction techniques from LPEs to the probabilistic case; constant elimination, confluence reduction.
Conclusions and Future Work

Conclusions / Results

- We developed the process algebra prCRL, incorporating both data and probability.
- We defined a normal form for prCRL, the LPPE; starting point for symbolic optimisations and easy state space generation.
- We generalised reduction techniques from LPEs to the probabilistic case; constant elimination, confluence reduction

Future work

- Finish work on confluence reduction: proofs, case study, implementation
- Develop additional reduction techniques
- Generalise proof techniques such as cones and foci to the probabilistic case
Questions

Questions?