Proving Probabilistic Properties of the Itai Rodeh leader election protocol for any Number of Processes

Douglas Graham

Department of Computing Science
University of Glasgow
Overview

- Parameterised model checking
  - Classical parameterised model checking problem
  - Proof by induction: Firewire example
  - Extending Firewire & proof probabilistically

- Itai Rodeh leader election protocol
  - Application of induction proof to Itai Rodeh
Parameterised Model Checking

- For system $M(N) = p(1) \parallel p(2) \parallel \ldots \parallel p(N)$ can only model check property $P$ for fixed $N$
- What if we want to verify for any $N$?
- Undecidable in general but techniques apply for subclasses of system
- E.g. proof by induction [Miller & Calder]
  - Firewire leader election protocol
Parameterised Model Checking
Parameterised Model Checking
Parameterised Model Checking

0  
P  
1  
C  
2
Parameterised Model Checking

0 \quad \rightarrow \quad P \quad \rightarrow \quad A \quad \rightarrow \quad 2

0 \quad \rightarrow \quad \rightarrow \quad P \quad \rightarrow \quad A \quad \rightarrow \quad 2

1

0 \quad \rightarrow \quad \rightarrow \quad P \quad \rightarrow \quad A \quad \rightarrow \quad 2

1

0 \quad \rightarrow \quad \rightarrow \quad P \quad \rightarrow \quad A \quad \rightarrow \quad 2

1

0 \quad \rightarrow \quad \rightarrow \quad P \quad \rightarrow \quad A \quad \rightarrow \quad 2

1
Parameterised Model Checking
Parameterised Model Checking

0

1

C
Parameterised Model Checking
Parameterised Model Checking
Parameterised Model Checking

- Notice that once a child node has sent an `ack`, it no longer takes part.
- System is described as *degenerative*.
- Can exploit this behaviour.
- Prove by induction that certain types of property hold for any number of nodes [Miller & Calder]
Parameterised Model Checking

- Show property holds for `base` system – star topology e.g. "leader will always be elected"
- For any configuration and size of system, every execution of model is related (stutter equivalent) to execution in model of smaller system
Probabilistic Parameterised Model Checking

- Can we apply degenerative approach to probabilistic systems?
- Extend Firewire probabilistically
  - Resolve "contention" situations with coin flip
  - Model as MDP in PRISM
- Extend induction proof
  - "Executions" are DTMCs not paths
  - Weak bisimulation instead of stutter equivalence
Probabilistic Parameterised Model Checking

- Can we apply induction approach to any other degenerative probabilistic systems?
- Itai Rodeh leader election protocol for rings?
Probabilistic Parameterised Model Checking

- Unidirectional ring of processes:
Each process flips coin and chooses 0 or 1 with equal probability.
Each process then passes choice to neighbour; if chosen 0 and receive 1 become passive
Counter is then passed around ring by each active process; counter is incremented by any passive process.
Probabilistic Parameterised Model Checking

Counter is then passed around ring by each active process; counter is incremented by any passive process.
Probabilistic Parameterised Model Checking

- If any process receives counter of value N-1 then he becomes leader, else active processes choose again.
Probabilistic Parameterised Model Checking

- Itai Rodeh is partially degenerative
  - When process becomes passive it only passes on messages...
  - ...but it can increment counter, whose max value is dependent on N
- Modelled in PRISM as an MDP [Kwiatkowska et al., Fokkink et al.]
- Our model is variation of these using buffers of size N
Probabilistic Parameterised Model Checking

- Apply same approach as for Firewire:
  - Base system is ring of size 3, say (could be anything that we can model check)
For \( N > 2 \) show that \( M_N \sim M_{N+1} \) where:
- \( \sim \) is some relationship between executions of MDPs
- \( M_N \) is model of system of size \( N \)
Probabilistic Parameterised Model Checking

- Introduce series of “intermediate” models
- Define model $Mc_N$ as for $M_N$ but with buffer length $N+1$
- For system of size $N$, never more than $N$ messages in buffers [Fokkink et al]
- $Mc_N$ is isomorphic to $M_N$

$M_N = Mc_N$
Probabilistic Parameterised Model Checking

- Define model $Mp_N$
- As for $M_{N+1}$ except initial nondeterministic choice over processes with one selected as passive
- Passive process does not increment counter
Probabilistic Parameterised Model Checking
Probabilistic Parameterised Model Checking
Probabilistic Parameterised Model Checking
Probabilistic Parameterised Model Checking
Probabilistic Parameterised Model Checking

- In $Mp_N$ buffers never contain $> N$ messages.
- If $p$ initial passive, number of messages between $p-1$ and $p+1$ never $> N$
  - NB count $p$ as a “buffer”
- Assume process $N+1$ initial passive.
- For $Mp_N$ relate buffers between $N$ and 1 to buffer between $N$ and 1 in $Mc_N$. 
Probabilistic Parameterised Model Checking

$Mc_3$

$\begin{array}{c}
1 \\
2 \\
3
\end{array}$

$\begin{array}{c}
[0,0,2,] \\
[,,] \\
[,,]
\end{array}$

$Mc_3$

$\begin{array}{c}
1 \\
2 \\
3
\end{array}$

$\begin{array}{c}
[0,0,2,] \\
[,,] \\
[,,]
\end{array}$

$Mp_3$

$\begin{array}{c}
1 \\
2 \\
3
\end{array}$

$\begin{array}{c}
[0,0,] \\
[,] \\
[,] \\
[2,] \\
[,,]
\end{array}$
Probabilistic Parameterised Model Checking

For each execution of $Mp_N$ there exists execution of $Mc_N$ that is weakly bisimilar (under relation) and vice versa.

$$M_N = Mc_N \approx Mp_N$$
Probabilistic Parameterised Model Checking

- Define $Mp_N'$ as for $Mp_N$ but initial passive increments counter
- Assume process $p$ initial passive
- If counter has passed through $p$ then relate state in $Mp_N'$ to state in $Mp_N$ with counter -1
Probabilistic Parameterised Model Checking

$Mp_3$

$Mp_3'$

\[ P(2) \xrightarrow{A} P \xrightarrow{A} P(3) \]

\[ P(2) \xrightarrow{A} P(3) \xrightarrow{A} P \]
Probabilistic Parameterised Model Checking

$M_{p_3}$

$M_{p_3'}$

$P$

$A$

$P(1)$
Probabilistic Parameterised Model Checking

- Again relation gives weak bisimulation between executions of models

\[ M_N = M_{cN} \approx M_{pN} \approx M_{pN'} \]
Probabilistic Parameterised Model Checking

- Finally want to show that $Mp_N'$ and $M_{N+1}$ are related.
- But choice of initial passive probabilistic in $M_{N+1}$ and nondeterministic in $Mp_N'$.
- Definition of relation between states is more complex and remains to be resolved.
Probabilistic Parameterised Model Checking

- Hence we have:
  \[ M_N = M_{c_N} \approx M_{p_N} \approx M_{p_N'} \approx? M_{N+1} \]

- So assuming
  \[ M_{p_N'} \approx M_{N+1} \]
  then by induction,
  \[ M_3 | = \Phi \Rightarrow \text{for all } N, \ M_N | = \Phi \]
  where \( \Phi \) is a PCTL property that
  - does not index any process id
  - does not contain next time or time bounded until operators

- \textit{E.g.} “with probability 1, a leader is elected”
Further Work

- Complete proof for Itai Rodeh leader election
- Apply to other degenerative systems
  - Randomised consensus weak shared coin protocol (Aspnes & Herlihy)