Qualitative Reasoning for the Dining Philosophers

Stefan Hallerstede[1] and Thai Son Hoang[2]

[1]Institut für Informatik
Heinrich-Heine-Universität Düsseldorf

[2]Department of Computer Science
Swiss Federal Institute of Technology Zürich (ETH Zürich)

Dagstuhl Seminar, 13th-18th September, 2009

Outline

Motivation

- Probabilistic solution for the dining philosophers.
- Proof from McIver and Morgan: Fairness + probability
- Here: probability only.
- Requirements:
  - simplicity
  - must yield a method
- Approach:
  - create a proof
  - not yet worry too much about the semantic models.
  - do that when we are sure the proof is good enough.

Motivation

- Probabilistic solution for the dining philosophers.
- Proof from McIver and Morgan: Fairness + probability
- Here: probability only.
- Requirements:
  - simplicity
  - must yield a method
- Approach:
  - create a proof
  - not yet worry too much about the semantic models.
  - do that when we are sure the proof is good enough.

The Dining Philosophers

- A number of philosophers sit at a round table.
- Between each adjacent pair of philosopher is a single fork.
- In order to eat, each philosopher need two forks on both sides.
- When hungry, a philosopher might want to pick up a fork, but this might already be taken by his neighbouring philosopher.
- There is a possibility of deadlock or livelock.
- There are deterministic solutions, e.g. using a waiter to break symmetry.
- We consider a symmetric probabilistic solution.

A Probabilistic Algorithm

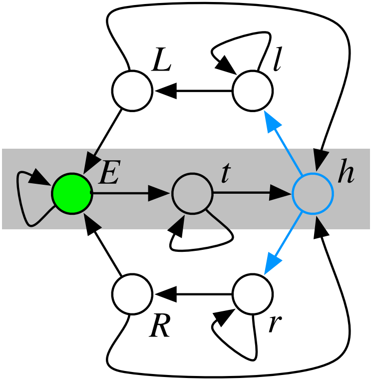


Figure: Actions of a philosophers

Fairness Assumption

Fairness assumption

Every philosopher is scheduled infinitely often with probability one.

Overall system

Some philosophers are hungry;
while "No philosopher is eating" **do**
  Schedule one of the philosopher fairly
end

Standard Event Convergent in Event-B

Intuitively

Event **must** decrease the variant.

More precisely

evt
  any x **where**
    $G(x, v)$
  then
    $v :| S(x, v, v')$
  end

variant: $V(v)$

$$\begin{array}{l} \quad \ldots \\ \quad G(x,v) \\ \vdash \\ \quad \forall v' \cdot S(y,v,v') \Rightarrow V(v') \subset V(v) \end{array}$$

Probabilistic Event Convergent in Event-B

Intuitively

Event might decrease the variant.

More precisely

evt
  any x **where**
    $G(x, v)$
  then
    $v \oplus| \ S(x, v, v')$
  end

variant: $V(v)$

$$\begin{array}{l} \quad \ldots \\ \quad G(x,v) \\ \vdash \\ \quad \exists v' \cdot S(y, v, v') \wedge V(v') \subset V(v) \end{array}$$

The State

Overall system

Some philosophers are hungry;
while "No philosopher is eating" **do**
  Schedule one of the philosopher probabilistically
end

Variables and invariants

variables: h, t, e

invariants:
  $partition(P, h, t, e)$

init
  begin
    $h, t :| \; partition(P, h', t') \wedge h' \neq \varnothing$
    $e := \varnothing$
  end

Hochschule Zürich
echnology Zurich

The Events

The events

eats
any p **where**
$p \in h$
then
$e := e \cup \{p\}$
$h := h \setminus \{p\}$
end

thinks
any p **where**
$p \in e$
then
$t := t \cup \{p\}$
$e := e \setminus \{p\}$
end

getsHungry
any p **where**
$p \in t$
then
$h := h \cup \{p\}$
$t := t \setminus \{p\}$
end

Refinement strategy (1)

Strategy

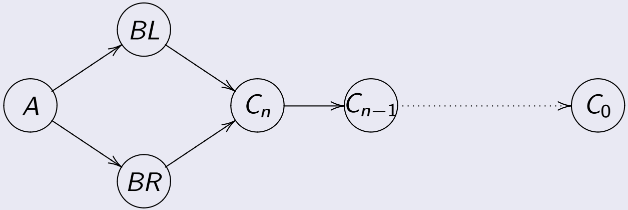
- Gradually introduce the algorithm: new variables/events are added.
- Prove that events other than eats are (probabilistic) convergent.
- System is deadlock-free.

Consequence

Eventually some (hungry) philosopher will eat.

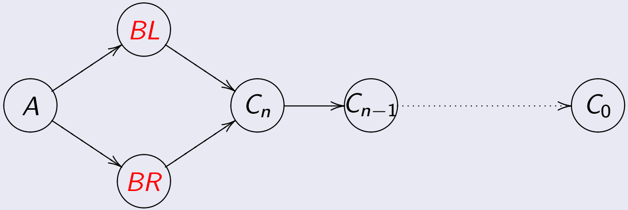
Refinement strategy (2)

The Lexicographic Variant



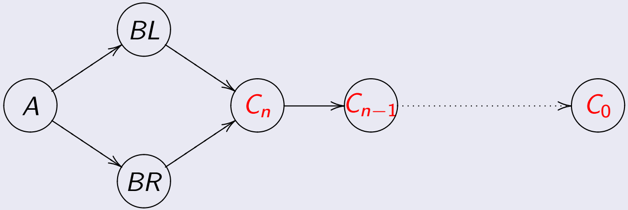
Refinement strategy (2)

The Lexicographic Variant



Refinement strategy (2)

The Lexicographic Variant



Probabilistic Convergent in BR and BL Phase

choose event: Pick-up left or right fork first

choose
any p **where**
$p \notin l$
$p \notin r$
$\ldots$
then
$l, r \oplus| \; (l' = l \cup \{p\} \wedge r' = r) \vee (r' = r \cup \{p\} \wedge l' = l)$
end

variant: $P \setminus r$

$$
\begin{array}{l}
p \notin l \\
p \notin r \\
\ldots \\
\vdash \\
\exists l', r' \cdot \\
\quad ((l' = l \cup \{p\} \wedge r' = r) \vee \\
\quad (r' = r \cup \{p\} \wedge l' = l)) \;\wedge \\
\quad P \setminus r' \subset P \setminus r
\end{array}
$$

Probabilistic Convergent in BR and BL Phase

choose event: Pick-up left or right fork first

choose
any p **where**
$p \notin l$
$p \notin r$
$\dots$
then
$l, r \oplus| \ (l' = l \cup \{p\} \wedge r' = r) \vee$
$(r' = r \cup \{p\} \wedge l' = l)$
end

variant: $P \setminus r$

$$p \notin l$$
$$p \notin r$$
$$\dots$$
$$\vdash$$
$$\exists l', r' \cdot$$
$$((l' = l \cup \{p\} \wedge r' = r) \vee (r' = r \cup \{p\} \wedge l' = l)) \ \wedge$$
$$P \setminus r' \subset P \setminus r$$

Hochschule Zürich
echnology Zurich

Probabilistic Convergent in C_n Phases

Pick up a (left) fork

chooseLeft **any** p **where** $p \in l$ ... **then** ... **end**	dropLeft **any** p **where** $p \in L$ ... **then** ... **end**	...

Difficulties

- The probabilistic choice is associated with the parameter p.
- The reasoning must taken into account all the actions that a particular philosopher can do.
- Need to prove: There exists a philosopher such that he can always act, and any action that he made decreases the variant.

A Possible Solution

evt$_i$
any t **where**
$G_i(t, v)$
then
$v :| Q_i(t, v, v')$
end

variant: V

witness: $W(t, v)$

- Sketch of probabilistic termination witness for t, say $W(t, v)$.
- Sketch of the proof obligations.
  1. Existent of witness: $I(v) \Rightarrow (\exists t \cdot W(t, v))$.
  2. Given the witness, at least one probabilistic event is enable.
     $I(v) \wedge W(t, v) \Rightarrow G_1(t, v) \vee \ldots \vee G_n(t, v)$
  3. For any probabilistic event evt_i, it decreases the variant V:
     $I(v) \wedge W(t, v) \wedge G_i(t, v) \wedge Q_i(t, v, v') \Rightarrow V(v') \subset V(v)$

What About Refinement

- Refinement can reduce non-determinism.
- Qualitative termination is not preserved through this type of refinement.
- We need to have additional proof obligation(s) for preserving qualitative termination.
- But this should be simple and usable.

For Further Reading I

S. Hallerstede and T.S. Hoang
Qualitative Probabilistic Modelling in Event-B,.
IFM 2007.

A. McIver and C. Morgan.
Abstraction, Refinement and Proof for Probabilistic Systems,
Chapter 3 — Case studies on probabilistic termination.
2005.