Formal Methods for Probabilistic Systems

Annabelle McIver
Carroll Morgan

- Source-level program logic
- Meta-theorems for loops
- Examples
- Relational operational model
  - Standard, deterministic, terminating ................. functions
  - Standard, deterministic, non-terminating ............. functions with ⊥
  - Standard, demonic, non-terminating .................. relations with ⊥
  - Standard powerdomains ................................ closure
  - Probabilistic powerdomains .............................. sub-distributions
  - Demonic, probabilistic powerdomains .................. sets of...
  - Examples ......................................................... program geometry
Standard, deterministic, terminating relational semantics
**Standard, deterministic, terminating relational semantics**

No probabilistic choice.

Output predictable from input.

No infinite loops or “run-time errors”.

A program $f$ is a function of type state-to-state.

Function $f$ applied to initial state $s$ gives final state $s'$.

$f : S \rightarrow S$

$f(s) = s'$

"Relates" initial states to final states, and so gives an "operational" view.

This is function application, that is $f(s)$. 
Standard, deterministic, terminating relational semantics

\[ s := (s - 1) \mod 4 \]

Function \( f \), where \( f.s = (s - 1) \mod 4 \).
A program $f$ is now a function of type state to state-or-bottom. $f : S \rightarrow S_{\perp}$

Function $f$ applied to initial state $s$ gives final state $s'$ ... or the special nontermination state $\perp$.

\[
\begin{align*}
  f.s & = s' \quad \text{if } f \text{ terminates, from } s, \text{ at } s' \\
  & = \perp \quad \text{otherwise}
\end{align*}
\]
Standard, deterministic relational semantics

We suppose it is a “run-time error” to attempt to set $s$ to -1.
Standard relational semantics
possibly nonterminating
possibly demonically nondeterministic

A program $r$ is now a relation of type state to state-or-bottom.

Usually $r$ is total
image-finite
and up-closed.  

“Miracles” are excluded.
Continuity is required.
If $r$ can fail to terminate, then all (other) behaviours are deemed possible as well.

$r: S \leftrightarrow S_\perp$

[r.s.s'] holds just when $r$ can reach $s'$ from $s$.

Boolean valued — true iff $(s,s') \in r$. 
Standard relational semantics

$s := s \pm 1$
Standard relational semantics

$s := s \pm 1$
Standard relational semantics

Initial states

0
1
2
3

Final states

0
1
2
3

$\bot$

$s := s \pm 1$

Remember that it is a “run-time error” to attempt to set $s$ outside its type $\{0..3\}$. 
Standard relational semantics

\[ s := s \pm 1 \]

...so we take an alternative view...

Gets complicated...
Standard relational semantics

Initial states

Sets of final states

A program \( r \) is a relation of type state to state-or-bottom... or equivalently a set-valued function.

\[ r: S \leftrightarrow S_\perp \]
\[ r: S \rightarrow \mathbb{P}S_\perp \]
\[ r: S \rightarrow \mathbb{F}^+S_\perp \]
The significance of up-closure

Informally, we regard 3 as a “better” outcome than ⊥. And we regard a program \( f_2 \) that delivers consistently better results than some other program \( f_1 \) as a “better” program overall:

\[
\text{If } (\forall s \cdot f_1.s \sqsubseteq f_2.s) \text{ then we say } f_1 \sqsubseteq f_2
\]

This in effect “promotes” the order \( \sqsubseteq \) from an order on individual values to an order on functions resulting in those values.

For nondeterminism we seek a similar promotion, but this time to the sets of values that represent the demonic choice.

A flat domain, based on the integers; for example \( \bot \sqsubseteq 3 \).

Program \( f_1 \) is refined by \( f_2 \) if some of \( f_1 \)’s nontermination is replaced by proper outcomes in \( f_2 \).

A proper outcome

nontermination

A flat domain, based on the integers; for example \( \bot \sqsubseteq 3 \).
The significance of up-closure: powerdomains

Given two relational programs $r_1$ and $r_2$, we say that $r_1 \sqsubseteq r_2$ iff, for all initial states $s$, any outcome in the set $r_2.s$ can be justified by some outcome in the set $r_1.s$, that is if every behaviour of the implementation $r_2$ is justified by the specification $r_1$:

For all $s$, and $s_2 \in r_2.s$, there is an $s_1 \in r_1.s$ such that $s_1 \sqsubseteq s_2$

That is, if $r_2.s.s_2$ holds, or equivalently $(s,s_2) \in r_2$.

This is known as the Smyth order.

For subsets $S_1, S_2$ of the state space $S$, we say that $S_1 \sqsubseteq S_2$ iff

$$(\forall s_2 \mid s_2 \in S_2 \cdot (\exists s_1 \mid s_1 \in S_1 \cdot s_1 \sqsubseteq s_2))$$ .

The refinement order between relations is just the Smyth order on result-sets, lifted functionally as we saw before.

The significance of up-closure: equivalence classes

For subsets \( S_1, S_2 \) of the state space \( S \), we say that \( S_1 \sqsubseteq S_2 \) iff

\[
(\forall s_2 | s_2 \in S_2 \cdot (\exists s_1 | s_1 \in S_1 \cdot s_1 \sqsubseteq s_2)) .
\]

Notice that both \( \{\bot, 2\} \sqsubseteq \{\bot, 3\} \) and \( \{\bot, 3\} \sqsubseteq \{\bot, 2\} \). This means that \( \sqsubseteq \) is not a partial order — rather it is a pre-order, satisfying reflexivity and transitivity but not antisymmetry. We say that \( \{\bot, 2\} \cong \{\bot, 3\} \), that they are equivalent.

This is a nuisance, but a well known one with a well known solution: we form equivalence classes, and take a distinguished representative from each class. That representative happens to be the up-closure — that is, for subset \( S_1 \) of \( S \), the set

\[
S_1 \uparrow \text{ defined } \{ s | s \in S \cdot (\exists s_1 | s_1 \in S_1 \cdot s_1 \sqsubseteq s) \}
\]

Not only does this have the property \( S_1 \cong S_2 \text{ iff } S_1 \uparrow = S_2 \uparrow \), as we would expect from the equivalence-class-representative construction, but we have also that

\[
S_1 \subseteq S_2 \text{ iff } S_1 \uparrow \supseteq S_2 \uparrow
\]
Up-closure for a flat domain

In the flat domain $S_\bot$ the definition of up-closure is particularly simple; it is

$$S_1^\uparrow = \begin{cases} S_1 & \text{if } \bot \notin S_1 \\ S_\bot & \text{otherwise.} \end{cases}$$

Although we have gone a long way to justify this easy construction, it is reassuring to know that it fits in with the general theory — and that will make things work much more smoothly later on.

Morgan’s Rule: *If you’re going to re-invent the wheel... at least make sure it’s round.*
A probabilistic powerdomain

The powerdomain construction we have just seen took an underlying set of values, with a partial order representing “refinement”, and from it constructed — in a very general way — a partial order over sets of those values, one which can be used to describe demonically nondeterministic programs.

A similar construction — though more complex — takes the underlying set of values, with its refinement order, to a partial order over distributions on those values.

That is what we shall use.


A probabilistic powerdomain over a flat structure

- Take our underlying space $S \perp$, with its “flat” information order, and generate the Scott topology on it.

- Carry on by generating the space of probabilistic evaluations over that topology.

- Then notice that the result is isomorphic to

$$\{ \Delta : [0,1] \rightarrow \sum_{s \in S} \Delta .s \leq 1 \}$$

with the order

$$\Delta_1 \subseteq \Delta_2 \text{ iff } \Delta_1 .s \leq \Delta_2 .s \text{ for all } s \in S.$$  

- These are called discrete sub-probability measures.

Discrete sub-probability measures

A discrete probability distribution assigns probabilities to individual points, e.g. the function \( \{ H \mapsto 1/2, T \mapsto 1/2 \} \) that describes flipping an unbiased coin.

It gains the prefix “sub-” if it is not required to sum to one, as in the distribution \( \{ H \mapsto 1/3, T \mapsto 1/3 \} \) for a coin that “might not terminate”— this implicitly includes a probability \( 1 - 1/3 - 1/3 = 1/3 \) of nontermination \( \bot \).

Such a coin is refined by another that terminates at least as often; and any extra termination can be assigned to either proper outcome; for example, we have

\[
\{ H \mapsto 1/3, T \mapsto 1/3 \} \sqsubseteq \{ H \mapsto 2/5, T \mapsto 1/2 \}
\]

in which the right-hand coin refines the left-hand coin, but still has probability \( 1/10 \) of failing to terminate.

Again we have used theoretical tools (information orders, Scott topology, Jones/Plotkin evaluations...) that in the end (via isomorphism) have produced something quite simple.

We have thus ensured that the wheel is “round” — and so it rolls very nicely!
A demonic powerdomain over discrete sub-probability measures

To have both demonic and probabilistic choice available to us, we take the probabilistic powerdomain we have just constructed — discrete sub-probability measures — and apply our earlier “up-closure of sets” construction; the latter will add demonic choice, as it did before, but this time to elements that already model probability.

The flat domain over state space $S$.

The probabilistic powerdomain over $S^\bot$.

Sets of discrete sub-probability measures, for demonic choice.

Closed sets of discrete sub-probability measures, for refinement.

The relational model of demonic, probabilistic programs.

\[ S^\bot \]
\[ \bar{S} \]
\[ \mathbb{P}\bar{S} \]
\[ \mathbb{C}_S \]
\[ S \rightarrow \mathbb{C}_S \]

Discrete sub-probability measures.

Then up closure, convex closure, Cauchy closure?

\[ \mathbb{C}_S \subseteq \mathbb{P}\bar{S} \]
A brief tour of $\mathcal{CS}$
when $S$ is the two-element space $\{H, T\}$
of coin-flip results

An unbiased coin.

A brief tour of $\mathbb{CS}$ when $S$ is the two-element space $\{H, T\}$ of coin-flip results
A brief tour of $\mathbb{C}S$
when $S$ is the two-element space $\{H, T\}$
of coin-flip results

A tails-biased coin.
A brief tour of $\mathcal{CS}$

when $S$ is the two-element space $\{H, T\}$ of coin-flip results

... one refinement of which is an unbiased coin.
A brief tour of $\mathbb{C}S$
when $S$ is the two-element space $\{H, T\}$ of coin-flip results

A possibly nonterminating coin... whose refinements include all three coins before.
A brief tour of $\mathbb{C} S$

when $S$ is the two-element space $\{ H, T \}$ of coin-flip results

Demonically, either of two possibly nonterminating coins.
A brief tour of \( \mathcal{C} S \)
when \( S \) is the two-element space \( \{ H, T \} \)
of coin-flip results

Demonically, either of two possibly nonterminating coins.
A brief tour of $\mathcal{C}S$
when $S$ is the two-element space \{H, T\} of coin-flip results


$\mathcal{H}S$ for Jifeng He

Demonically, either of two possibly nonterminating coins.
A brief tour of $\mathcal{C}S$ concluded ... but what’s the connection with the programming logic?


Demonically, either of two possibly nonterminating coins.

Convex closure
Up closure
Cauchy closure
A brief tour of CS concluded ... but what’s the connection with the programming logic?

Demonically, either of two possibly nonterminating coins.

What is the greatest guaranteed expected value of this program with respect to the post-expectation \([c=H] + 2[c=T]\)?

It’s 5/6.

\[
\begin{align*}
x + 2y &= 0 \\
x + 2y &= \frac{1}{3} + 2(\frac{1}{4}) \\
&= 5/6
\end{align*}
\]
A brief tour of $\mathbb{S}$ concluded... but what's the connection with the programming logic?

Demonically, either of two possibly nonterminating coins.

What is the greatest guaranteed expected value of this program with respect to the post-expectation $2[c=H] + [c=T]$?
A brief tour of CSS concluded... but what’s the connection with the programming logic?

Demonically, either of two possibly nonterminating coins.

What is the greatest guaranteed expected value of this program with respect to the post-expectation $2[c=H] + [c=T]$?

It’s not $11/12$. 

$$2x + y = 2/3 + 1/4 = 11/12$$
A brief tour of CS concluded... but what's the connection with the programming logic?

What is the greatest guaranteed expected value of this program with respect to the post-expectation $2[c=H] + [c=T]$?

It's $5/6$ again, because this time the demon goes to the other extreme.

$$2x + y = 0$$

$$2x + y = 2/4 + 1/3 = 5/6$$

$$2x + y = (1/4, 1/3); (2,1); (3,1/4)$$

$H$

$T$
The two semantics are congruent

\[ \text{preE} \Rightarrow \text{wp.prog.postE} \]

**means**

\[ (\forall s:S; \sigma:\text{"prog" } s \cdot \text{"preE" } s \leq \exp_{\sigma'} \text{"postE"}) \]
The two semantics are congruent

\[ \text{wp}.prog.postE.s \]

**means**

\[ (\sigma:\text{"prog' s • "preE' s} \leq \exp_\sigma\text{"postE'}) \]

**transformer model:**

\[ \text{fun}.S \rightarrow \text{fun}.S \]

(sublinear)

**relational model:**

\[ S \rightarrow P(\text{dist}.S) \]

**Combined logic of weakest pre-expectations:**

\[ \text{preE} \Rightarrow \text{wp}(\text{prog,postE}) \]
Exercises

Ex. 1: Experiment with the geometric presentation of the transformer semantics: what happens to the demonic coin with post-expectation

just \([c=H]\)?
just \([c=T]\)?
just \([true]\)?

(The direction numbers for \([true]\) are \((1,1)\), i.e. the grazing-line approaches at \(45^\circ\). Which distribution-point does it touch first?)

Ex. 2: Why isn’t the answer to the third item above just 1 again?