

Formal Methods for Probabilistic Systems

Annabelle McIver
Carroll Morgan

- Probabilistic temporal logic: qTL
- Probabilistic sequential-programming logic: $pGCL$
- Probabilistic modal mu-calculus: $qM\mu$

British *EPSRC* (Oxford),
then Australian *ARC*
(Macquarie/UNSW),
[1994-continuing](#).

Annabelle McIver
Carroll Morgan
Jeff Sanders
Karen Seidel

`web.comlab.ox.ac.uk/
oucl/
research/
areas/
probs/`

Formal Methods for Probabilistic Systems

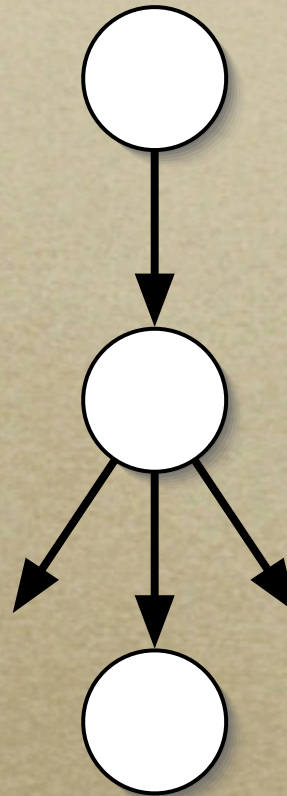
Annabelle McIver
Carroll Morgan

- Probabilistic temporal logic: qTL
 - Standard temporal logic
 - A quantitative logic of expected values
 - Syntax and semantics of qTL
 - “Axioms” and “Rules of Inference”
 - Example proofs (1,2,3)
 - Case study: *The Jumping Bean*

Standard (computation-tree) temporal logic

transitions ↓

○ states



Predicate operators

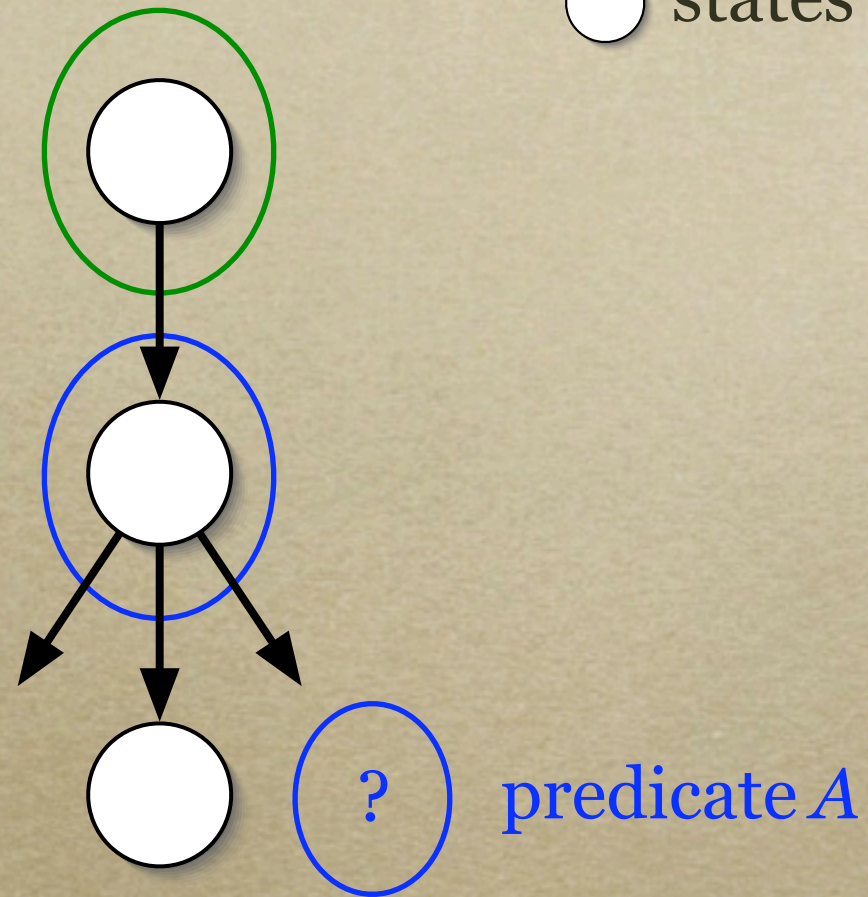
next-time \bigcirc

transitions \downarrow

\bigcirc states

For demonic (universal) nondeterminism, take **conjunction** over all successors

predicate $\bigcirc A$



Predicate operators

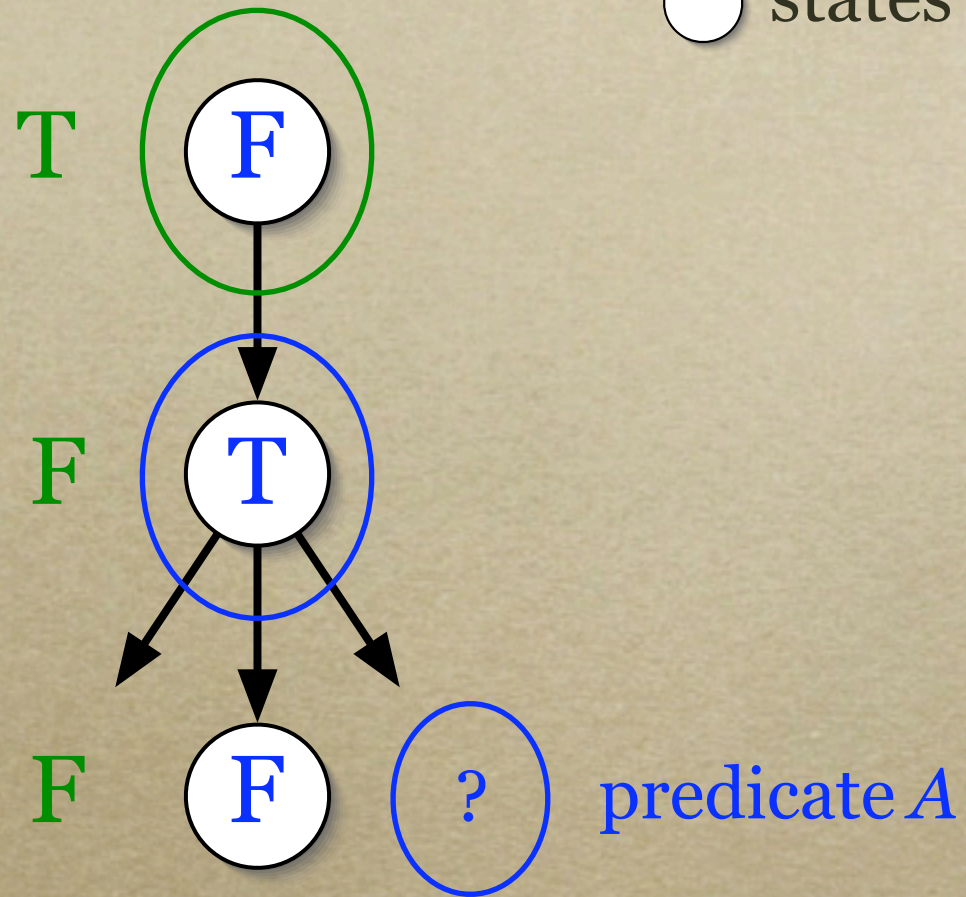
next-time ○

transitions ↓

For demonic (universal) nondeterminism, take conjunction over all successors

○ states

predicate ○A



Predicate operators

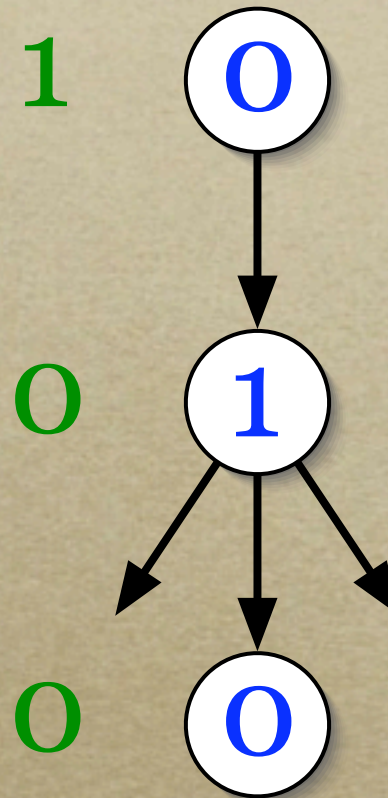
next-time ○

transitions ↓

○ states

For demonic (universal) nondeterminism, take *minumum* over all successors

predicate ○A



predicate A

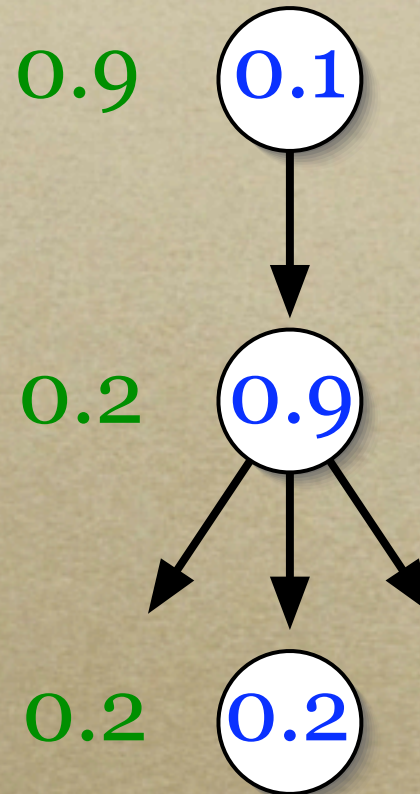
Expectation operators

next-time \circ

standard
transitions \downarrow

\circ states

*For demonic (universal)
nondeterminism,
take minimum over all
successors*



expectation $\circ A$

expectation A

Expectation operators

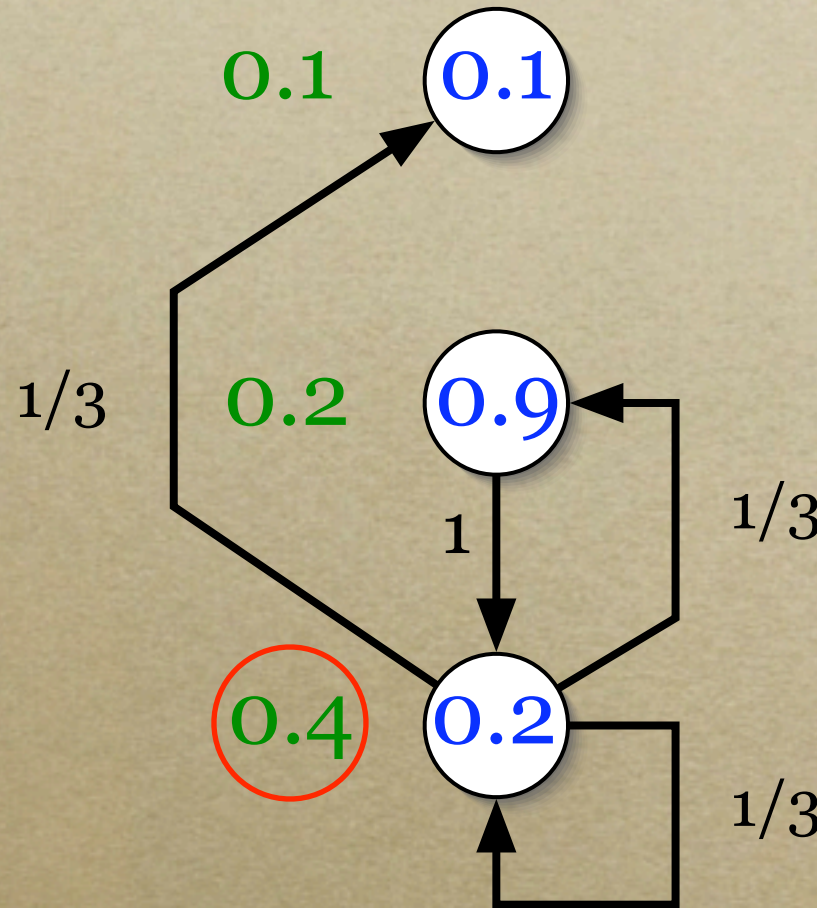
next-time ○

probabilistic
transitions ↓

○ states

For *probabilistic*
nondeterminism,
take *expected value*
over all successors

expectation ○A



expectation A

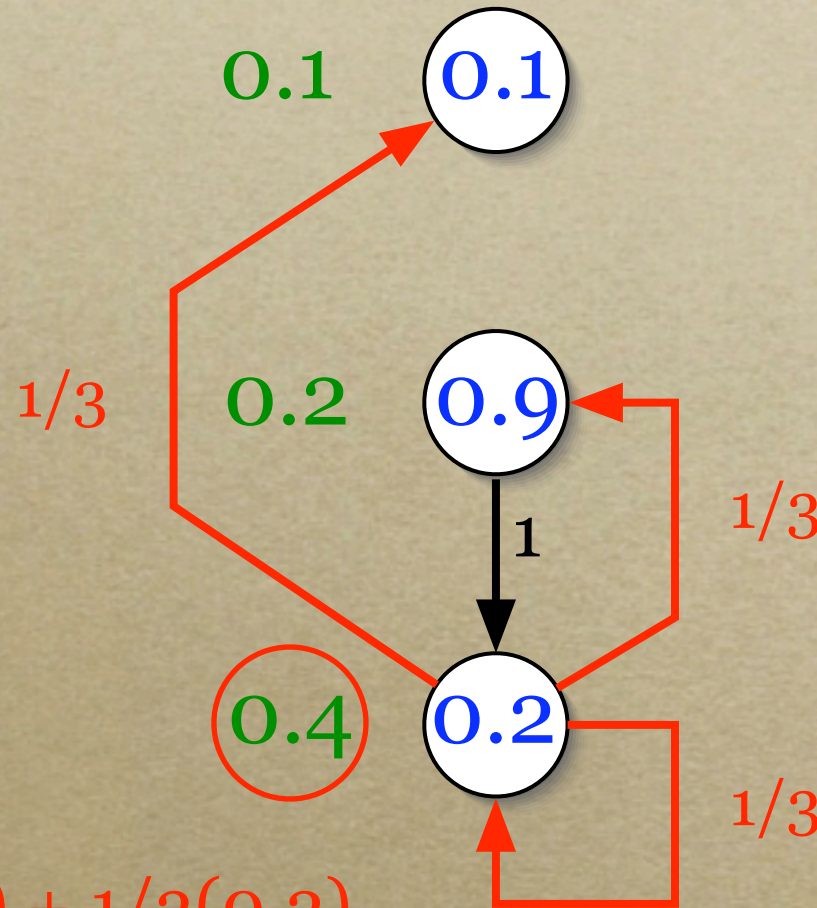
Expectation operators

next-time ○

probabilistic transitions ↓

○ states

For probabilistic nondeterminism, take expected value over all successors



expectation ○A

expectation A

$$\frac{1}{3}(0.1) + \frac{1}{3}(0.9) + \frac{1}{3}(0.2)$$

Predicate operators

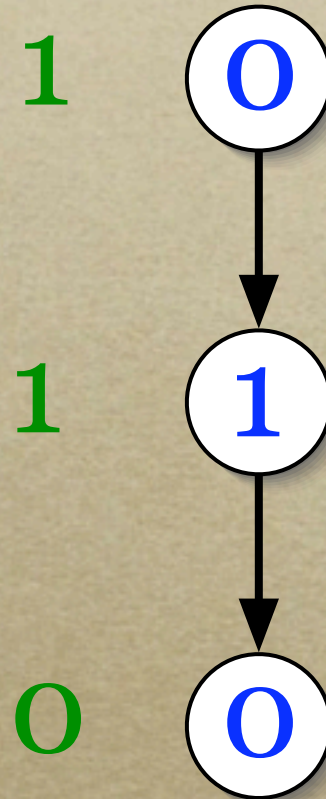
eventually \diamond

standard
transitions \downarrow

 states

*For eventually,
seek the maximum*

expectation $\diamond A$



expectation A

Predicate operators

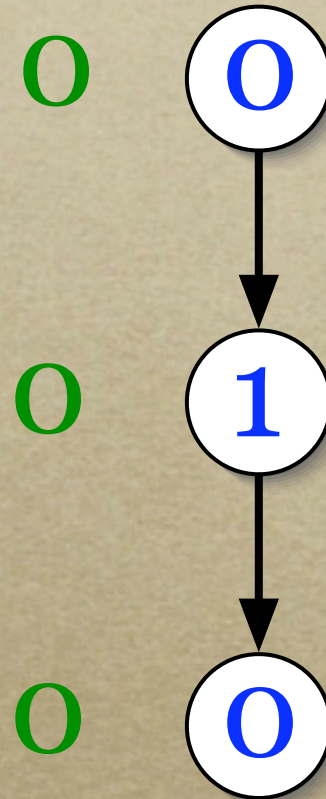
always \square

standard
transitions \downarrow

\circ states

*For always,
seek the *minimum**

expectation $\square A$



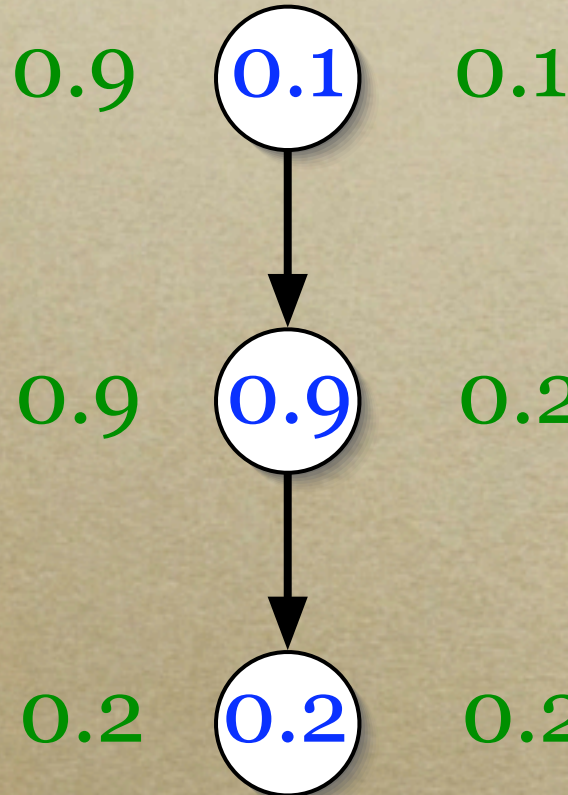
expectation A

Expectation operators

eventually \diamond
always \square

standard
transitions \downarrow

expectation A



*For demonic
(universal)
nondeterminism,
take **minumum**
over all successors*

expectation $\diamond A$

*For eventually,
seek the maximum*

expectation $\square A$

*For always,
seek the minimum*

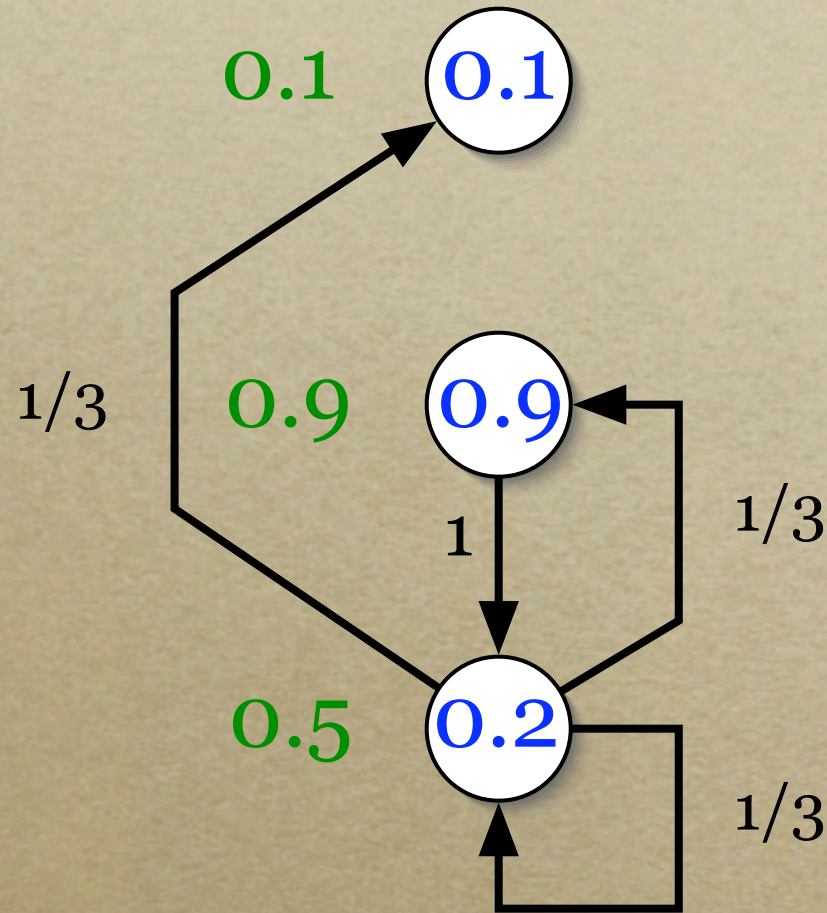
Expectation operators

eventually \diamond

probabilistic
transitions \downarrow

For eventually,
seek the maximum

expectation $\diamond A$



expectation A

Expectation operators

eventually \diamond

probabilistic
transitions \downarrow

if *maximising-strategy*
then *take A now*
else *make one step;*
repeat

fi

For eventually,
seek the maximum

1/3

0.1



0.9



1/3

expectation $\diamond A$

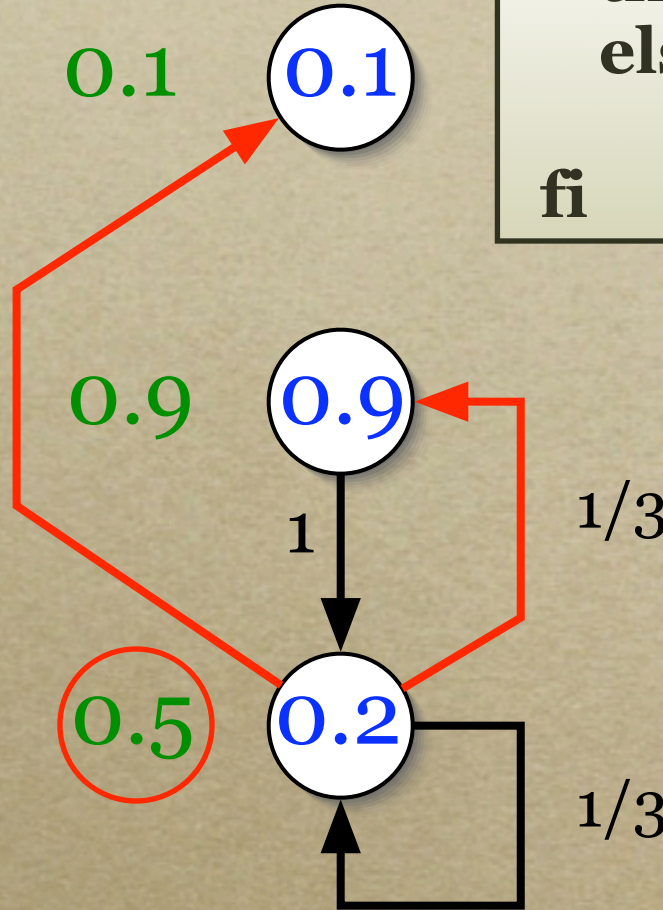
0.5



expectation A

1/3

$$\frac{[1/3(0.1) + 1/3(0.9)]}{[1/3 + 1/3]}$$



Expectation operators

eventually \diamond

Definition: For any assignment A of real values in the interval $[0,1]$ to the states of a probabilistic/demonic transition system, the

expectation $\diamond A$

is the *supremum*, over all *strategies*, of the game

The strategies can be mixed, or non-stationary, or memoried.

```
if strategy
  then take  $A$  now
  else make one step;
fi
```

There can be demonic (minimising) choices made here, “built-in” to the transition system over which the *eventually* is taken.

Expectation operators

always \square

Definition: For any assignment A of real values in the interval $[0,1]$ to the states of a probabilistic/demonic transition system, the

expectation $\square A$

is the *infimum*, over all *strategies*, of the game

The strategies can be mixed, or non-stationary, or memoried.

```
if strategy
  then take  $A$  now
  else make one step;
fi
```

There can be demonic (minimising) choices made here, “built-in” to the transition system over which the *eventually* is taken.

Expectation operators

always \square

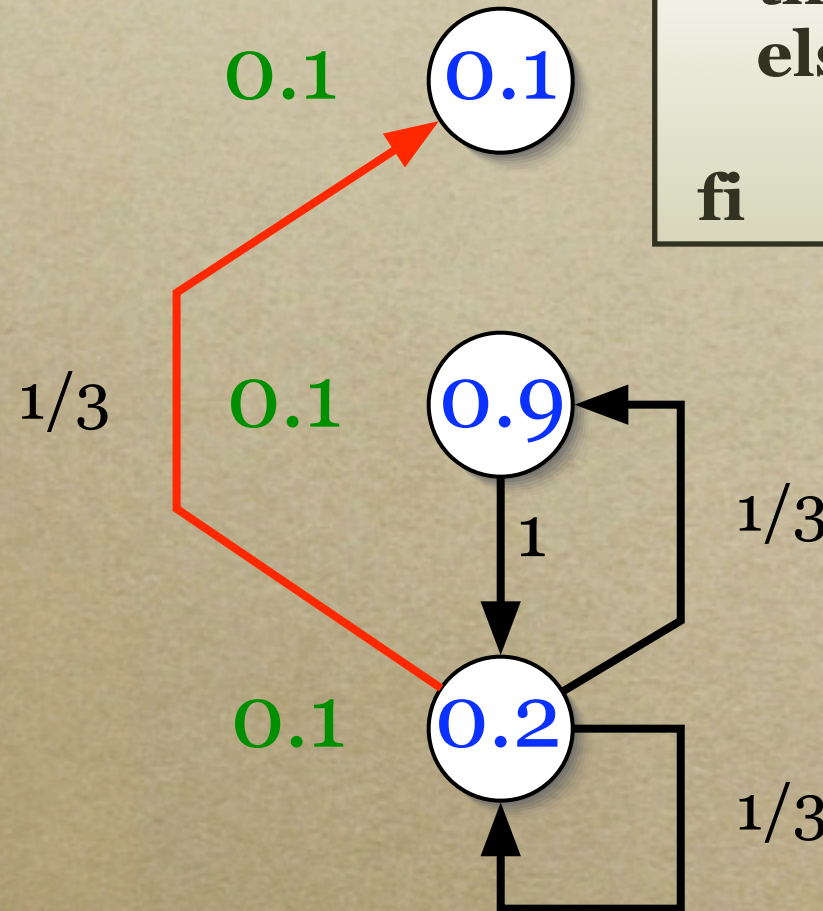
probabilistic transitions \downarrow

For always, seek the *minimum*

if *minimising*-strategy
then take A now
else make one step;
repeat

fi

expectation $\square A$

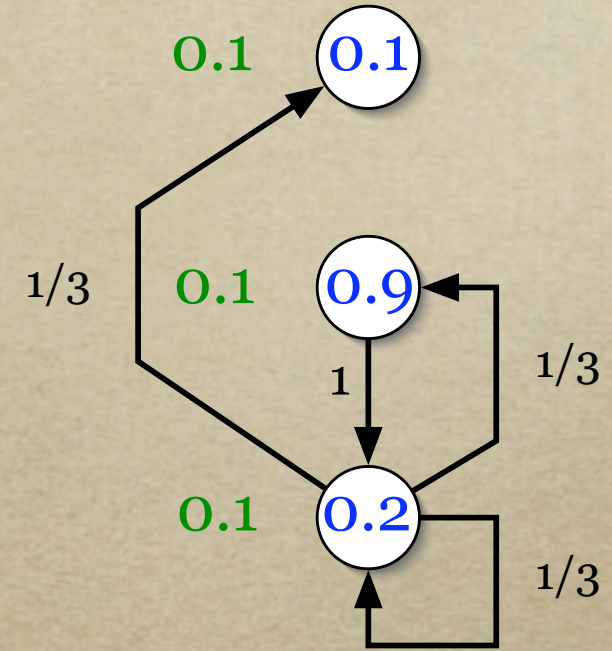
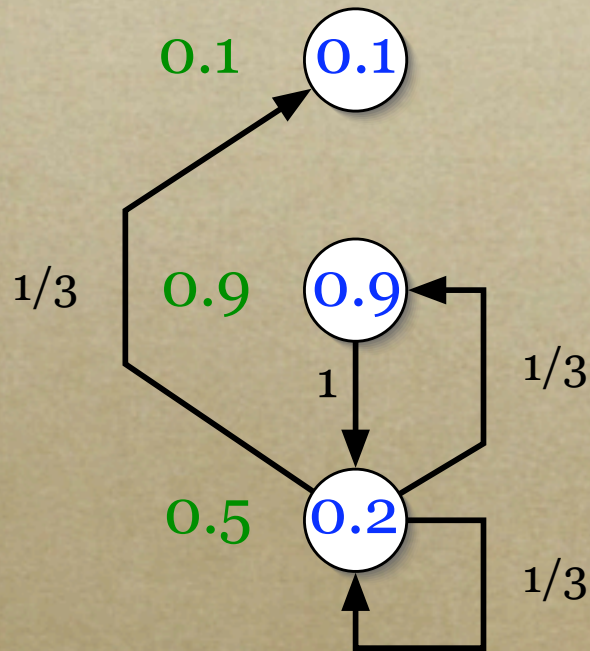


expectation A

Expectation operators

eventually \diamond
always \square

These modalities satisfy fixed-point equations.



expectation $\diamond A$

*For eventually,
seek the maximum*

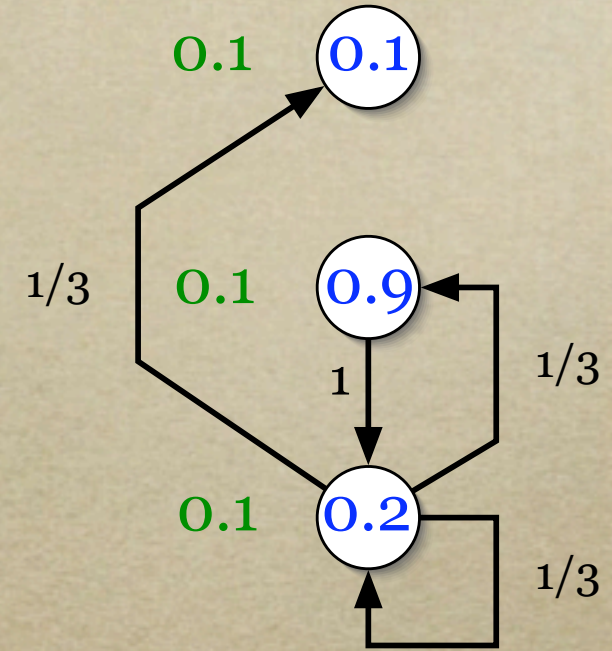
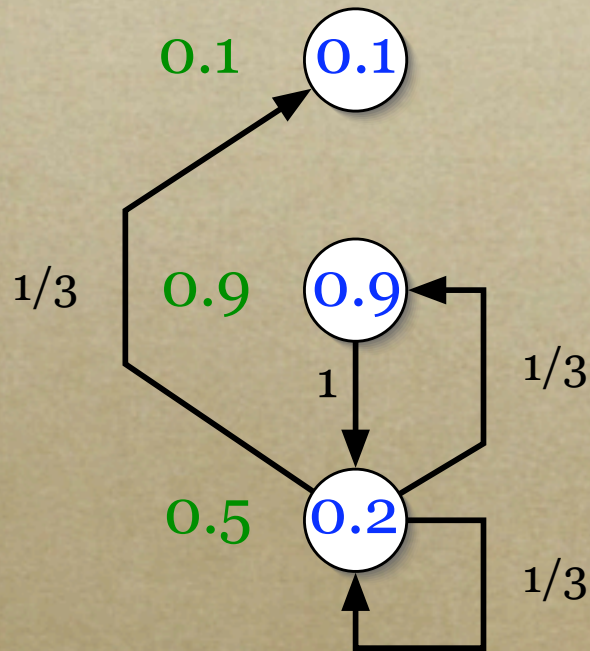
expectation $\square A$

*For always,
seek the minimum*

Expectation operators

eventually \diamond
always \square

These modalities satisfy fixed-point equations.



expectation $\diamond A$

$$\diamond A = A \sqcup \bigcirc \diamond A$$

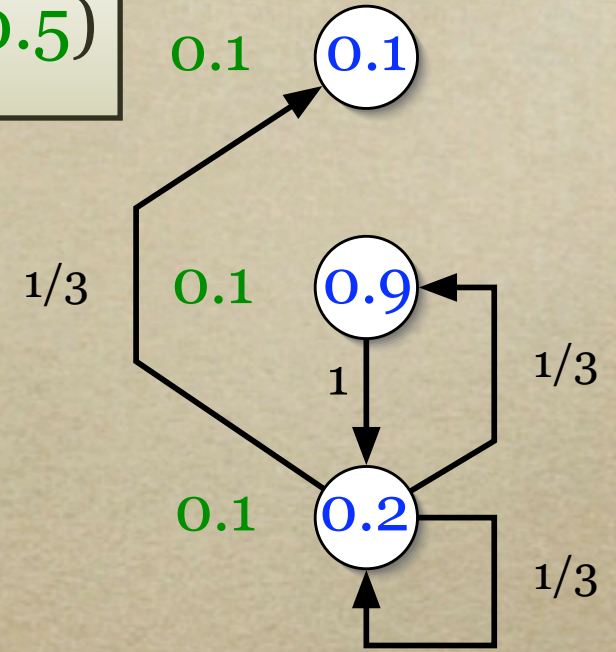
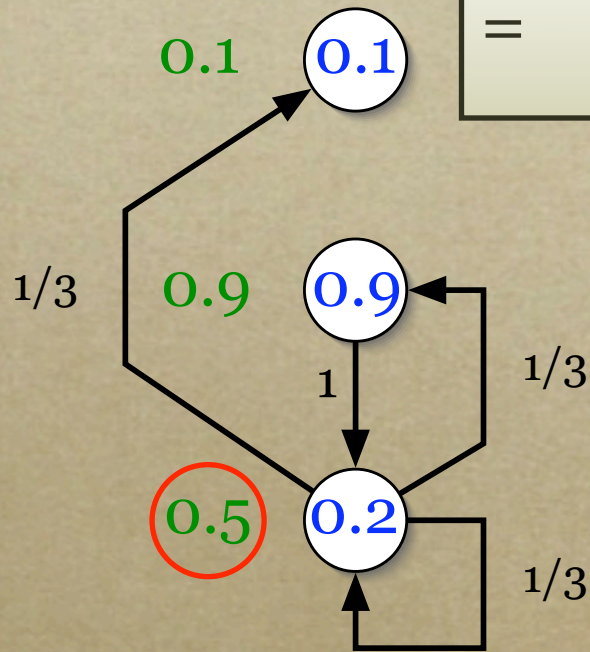
expectation $\square A$

$$\square A = A \sqcap \bigcirc \square A$$

Expectation operators

eventually \diamond
always \square

$$= 0.5 = 0.2 \sqcup (1/3)(0.1+0.9+0.5)$$



expectation $\diamond A$

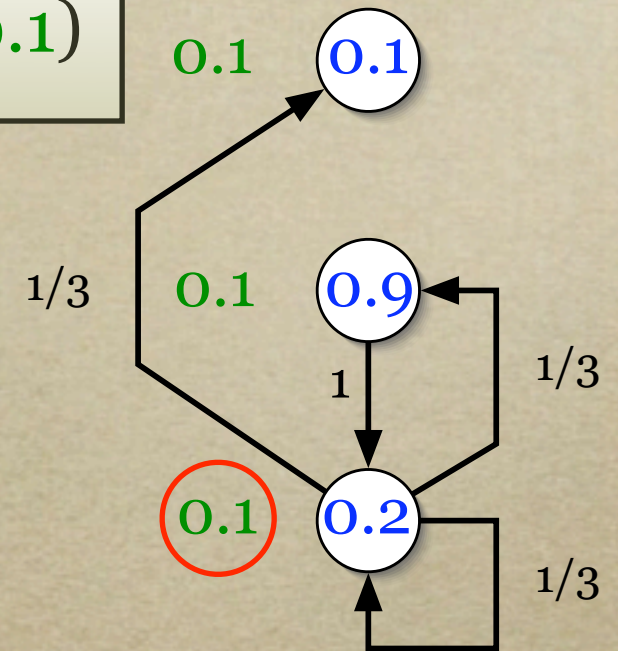
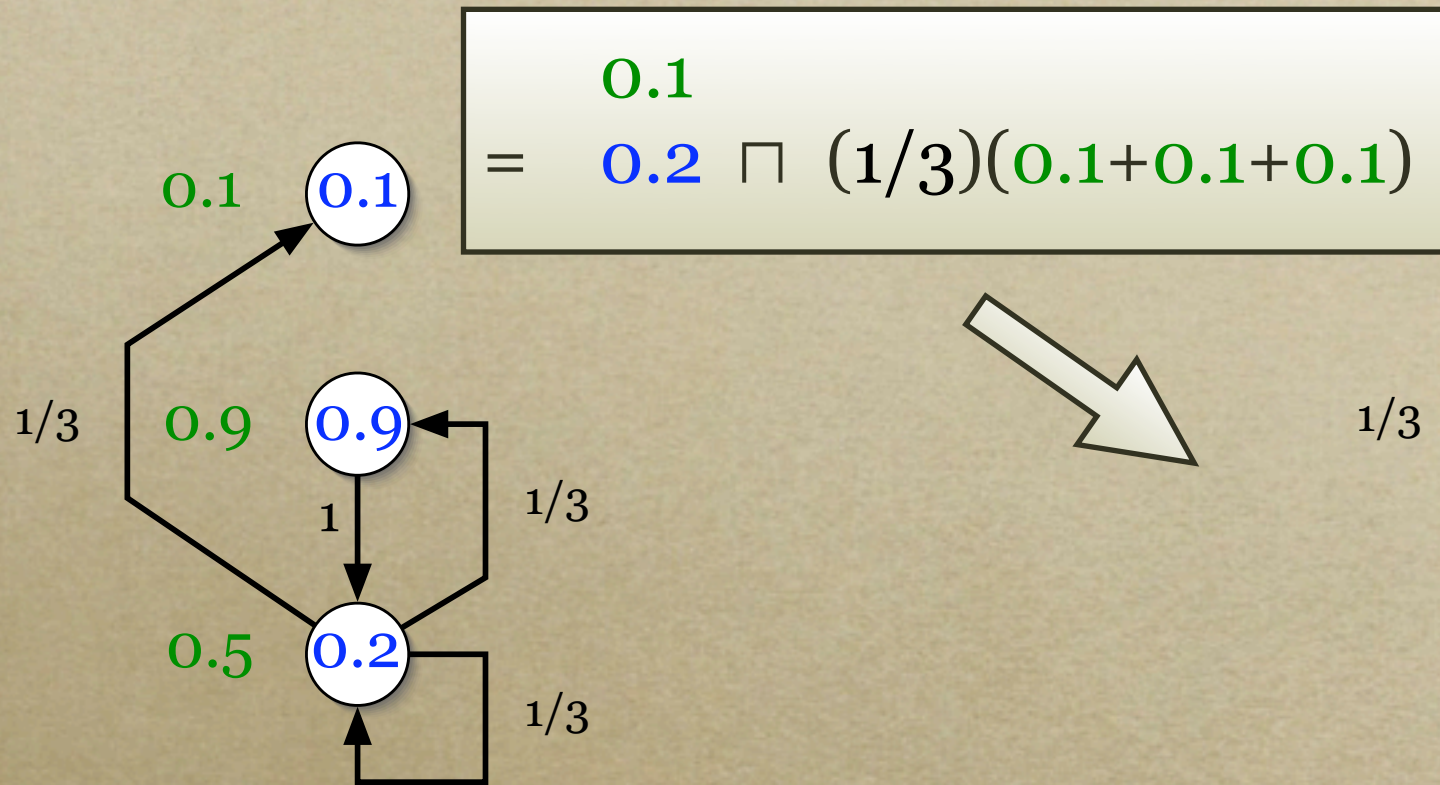
$$\diamond A = A \sqcup \bigcirc \diamond A$$

expectation $\square A$

$$\square A = A \sqcap \bigcirc \square A$$

Expectation operators

eventually \diamond
always \square



expectation $\diamond A$

$$\diamond A = A \square \bigcirc \diamond A$$

expectation $\square A$

$$\square A = A \square \bigcirc \square A$$

The quantitative temporal logic qTL – syntax

$$A \hat{=} \quad \mathbf{E} \mid A_1 \sqcap A_2 \mid A_1 \sqcup A_2 \mid \neg A \\ \mid \circ A \mid \diamond A \mid \square A \mid A_1 \triangleright A_2$$

- Formulae \mathbf{E} are the analogues of the non-modal formulae in standard modal logic; here they stand for fixed functions into $[0, 1]$ of the underlying state space.
- Minimum \sqcap and maximum \sqcup will be the quantitative analogues of conjunction and disjunction.
- Quantitative \neg will be subtraction from 1.
- \circ , \diamond , \square and \triangleright are the modal operators *next-time*, *eventually*, *always* and (weak) *unless* respectively.

The quantitative temporal logic qTL — semantics

We take a state space S (usually countable, often finite), and form a derived space $\mathbb{H}.S$ of probabilistic/demonic transitions over S , defined as follows:

$$\begin{array}{lll} \overline{S} & \hat{=} & S \rightarrow [0, 1] \quad \text{summing to } \leq 1 \\ \mathbb{H}.S & \hat{=} & S \rightarrow \mathbb{P}.\overline{S} \quad \text{with some closure conditions} \end{array}$$

The quantitative temporal logic qTL — interpretation

We write $\llbracket A \rrbracket_{\mathcal{X}.s}$ for the value of A at state s relative to a demonic/probabilistic transition system \mathcal{X} of type $S \rightarrow \mathbb{P}.\overline{S}$ over a state space S .

- $\llbracket E \rrbracket.s$ is (informally) the value in $[0, 1]$ taken by E at s . Typically the state space will be a Cartesian product of program variables' types, and thus E will be some expression in those variables. Standard (Boolean) predicates are represented by expressions taking values zero (false) or one (true).

- $\llbracket A_1 \sqcap A_2 \rrbracket$ and $\llbracket A_1 \sqcup A_2 \rrbracket$ are the pointwise minimum and maximum respectively of $\llbracket A_1 \rrbracket$ and $\llbracket A_2 \rrbracket$.

- $\llbracket \neg A \rrbracket.s$ is $1 - \llbracket A \rrbracket.s$.

The quantitative temporal logic qTL — interpretation

We write $\llbracket A \rrbracket_{\mathbb{P}, s}$ for the value of A at state s relative to

a de
over

Confusingly, when the individual worlds of a modal (temporal) logic are the possible machine states of an executing program, the *variables* of the program are *constant symbols* from a purely logical point of view.

\mathbb{P}, \bar{S}

•

This is because they represent values that are *fixed* within any particular state, and one does not quantify over them.

$s.$

of

es-

are

ne

On the other hand, the *variables* of the logic (over which we can quantify) are often called *logical constants* in the Computing-Science literature.

nd

maximum respectively of $\llbracket A_1 \rrbracket$ and $\llbracket A_2 \rrbracket$.

• $\llbracket \neg A \rrbracket_{\mathbb{P}, s}$ is $1 - \llbracket A \rrbracket_{\mathbb{P}, s}$.

The quantitative temporal logic qTL — interpretation

- Given “current state” s , we define $\llbracket \circ A \rrbracket.s$ to be the (universal, or “demonic”) minimum over all the “next-state” sub-distributions Δ in $\mathcal{X}.s$ of the expected value of $\llbracket A \rrbracket$ over Δ .

For fixed \mathcal{X} we regard $\llbracket \circ A \rrbracket.s$ as a function $\llbracket \circ \rrbracket$ of “post-expectation” $\llbracket A \rrbracket$ and current state s , so that we can write $\llbracket \circ A \rrbracket.s = \llbracket \circ \rrbracket.\llbracket A \rrbracket.s$ or, more simply,

$$\llbracket \circ A \rrbracket = \llbracket \circ \rrbracket.\llbracket A \rrbracket .$$

- $\llbracket \diamond A \rrbracket$ is the *least fixed-point* of the function \mathcal{F} defined

$$\mathcal{F}.X \hat{=} \llbracket A \rrbracket \sqcup \llbracket \circ \rrbracket.X ,$$

where X is of type $S \rightarrow [0, 1]$.

The quantitative temporal logic qTL — interpretation

- $\llbracket \Box A \rrbracket$ is the *greatest fixed-point* of the function \mathcal{G} defined

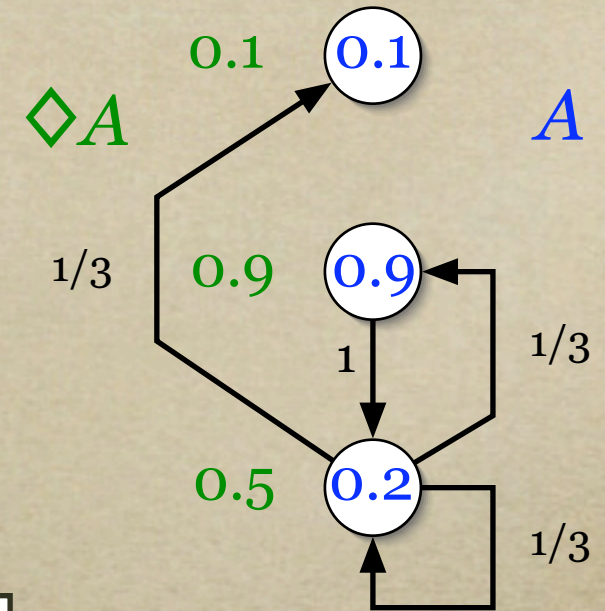
$$\mathcal{G}.X \hat{=} \llbracket A \rrbracket \sqcap \llbracket \circ \rrbracket.X .$$

- $\llbracket A_1 \triangleright A_2 \rrbracket$ is the *greatest fixed-point* of the function \mathcal{U} defined

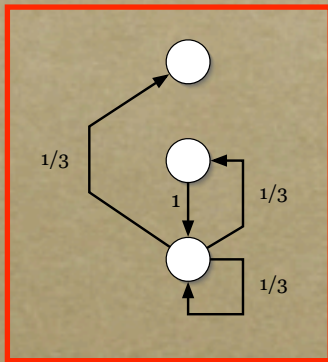
$$\mathcal{U}.X \hat{=} \llbracket A_2 \rrbracket \sqcup (\llbracket A_1 \rrbracket \sqcap \llbracket \circ \rrbracket.X) .$$

The quantitative temporal logic qTL —

*the congruence
of the operational
and the denotational
interpretations*



Operational:



if *maximising-strategy*
then *take A now*
else *make one step;*
repeat

fi

Denotational:

$$[[\diamond A]] = (\mu X \cdot [[A]] \sqcup [[\circ]].X)$$

The quantitative temporal logic qTL —

*the congruence
of the operational
and the denotational
interpretations*

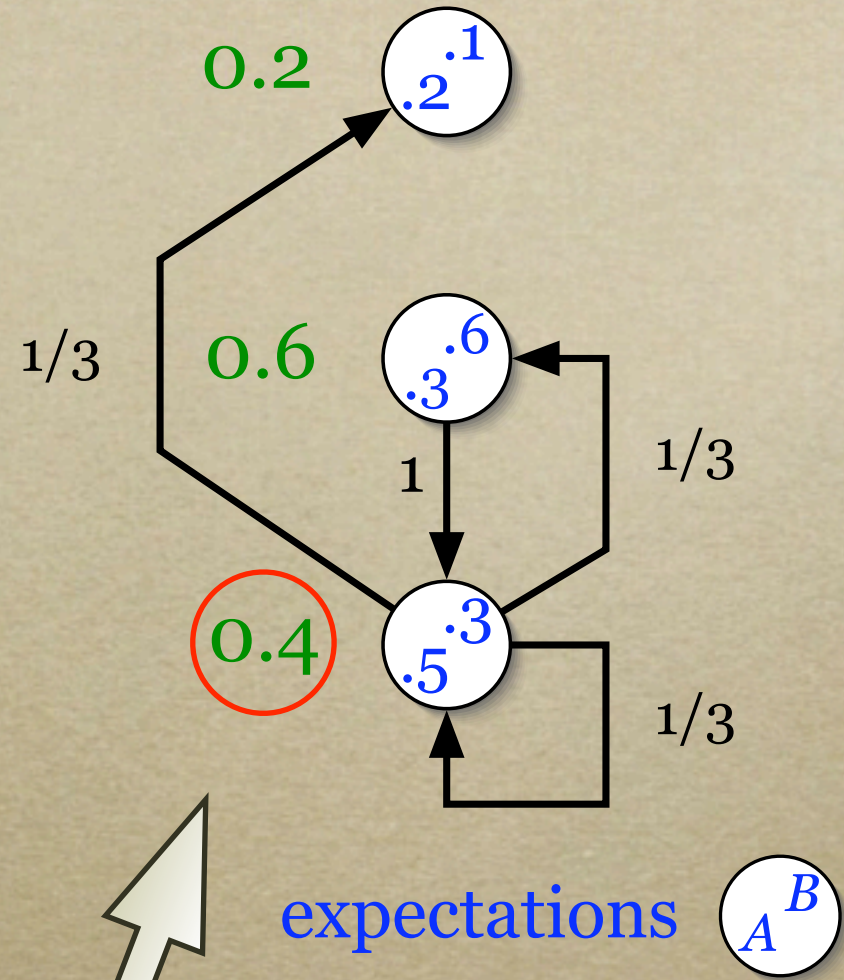
if *maximising-strategy*
then *take A now*
else *make one step;*
repeat
fi

Theorem: The game-and-strategy *operational* definitions for the temporal operators agree with the *denotational* interpretations given above in terms of least- and greatest fixed points.

Expectation operators

unless \triangleright

```
if maximising-strategy
  then take B now
elsif minimising-strategy
  then take A now
else make one step;
     repeat
fi
```



expectation $A \triangleright B$

$$A \triangleright B = B \sqcup (A \sqcap \bigcirc(A \triangleright B))$$

$$0.4 = 0.3 \sqcup (0.5 \sqcap (1/3)(0.2 + 0.6 + 0.4))$$

Properties of \circ

- **scaling** $\circ(pA) \equiv p(\circ A)$ for $0 \leq p \leq 1$.
 - **choice** $\circ(A \oplus_p B) \Leftarrow (\circ A) \oplus_p (\circ B)$ for $0 \leq p \leq 1$.
 - **conjunction** $\circ(A \& B) \Leftarrow (\circ A) \& (\circ B)$.
-
- **probabilistic choice** $A \oplus_p B \equiv pA + (1-p)B$.
 - **probabilistic conjunction** $A \& B \equiv (A + B - 1) \sqcup 0$.
 - **probabilistic implication** *etc.*
 - $A \Leftarrow B$ iff $A \geq B$ everywhere.
 - $A \Rightarrow B$ iff $A \leq B$ everywhere.
 - $A \equiv B$ iff $A \Leftarrow B$ and $A \Rightarrow B$.

“Axioms” and “rules of inference” eventually \diamond

Fixed-point properties

If x is the least fixed-point of some function F , then

- $x = F.x$, and
- for all y we have $y \sqsupseteq x$ if $y \sqsupseteq F.y$.

Properties of \diamond

- \diamond fixed point $\diamond A \equiv A \sqcup (\circ \diamond A)$.
- \diamond least $B \Leftarrow \diamond A$ if $B \Leftarrow A \sqcup (\circ B)$.

“Axioms” and “rules of inference”

always \square
unless \triangleright

Properties of \square

- \square fixed point $\square A \equiv A \sqcap (\circ \square A)$.
- \square greatest $B \Rightarrow \square A$ if $B \Rightarrow A \sqcap (\circ B)$.

Properties of \triangleright

- \triangleright fixed point $A \triangleright B \equiv B \sqcup (A \sqcap \circ (A \triangleright B))$.
- \triangleright greatest $C \Rightarrow A \triangleright B$ if $C \Rightarrow B \sqcup (A \sqcap \circ C)$.

Example proofs (1)

double-eventually $\diamond \diamond$

Lemma: For all A we have $\diamond \diamond A \equiv \diamond A$.

Proof: For $\diamond \diamond A \Leftarrow \diamond A$ we reason

$$\begin{aligned} & \diamond \diamond A \\ \equiv & \diamond(A \sqcup (\circ \diamond A)) \\ \Leftarrow & \diamond A \end{aligned}$$

\diamond fixed point
 \diamond monotonic

For the other direction we reason

$$\begin{aligned} & \diamond A \sqcup (\circ \diamond A) \\ \Rightarrow & \diamond A \sqcup A \sqcup (\circ \diamond A) \\ \equiv & \diamond A \sqcup \diamond A \\ \equiv & \diamond A, \end{aligned}$$

\diamond fixed point

hence by \diamond least we have $\diamond \diamond A \Rightarrow \diamond A$.

$$\diamond B \Leftarrow \diamond A \quad \text{if} \quad \diamond B \Leftarrow A \sqcup \circ B$$

Example proofs (2) eventually-and-always \diamond & \square

Lemma: For all A, B we have $\diamond A \ \& \ \square B \Rightarrow \diamond(A \ \& \ B)$.

Proof: We reason

$$\begin{aligned} & \diamond A \ \& \ \square B \Rightarrow \diamond(A \ \& \ B) \\ \text{iff } & \diamond A \Rightarrow \square B \rightarrow \diamond(A \ \& \ B) \end{aligned}$$

$\&, \rightarrow$ are \Rightarrow -adjoints



$\&, \rightarrow$ are \Rightarrow -adjoints...?

For scalars $0 \leq a, b, c \leq 1$ we have

$$\begin{aligned} & \rightarrow a \ \& \ b \leq c \\ \text{iff } & (a + b - 1) \sqcup 0 \leq c \\ \text{iff } & a + b - 1 \leq c & 0 \leq c \\ \text{iff } & a \leq 1 - b + c \\ \text{iff } & a \leq (1 - b + c) \sqcap 1 & a \leq 1 \\ & \rightarrow \text{iff } a \leq b \rightarrow c, \end{aligned}$$

provided we make the definition $b \rightarrow c \hat{=} (1 - b + c) \sqcap 1$.

adjoint property

Example proofs (2) eventually-and-always $\diamond \wedge \square$

Lemma: For all A, B we have $\diamond A \wedge \square B \models \diamond(A \wedge B)$.

Proof: We reason

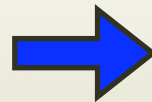
$$\begin{aligned} & \diamond A \wedge \square B \models \diamond(A \wedge B) \\ \text{iff } & \diamond A \models (\square B \Rightarrow \diamond(A \wedge B)) \end{aligned}$$

\wedge, \Rightarrow are \models -adjoints



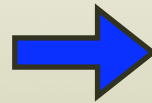
\wedge, \Rightarrow are \models -adjoints

adjoint property



$$a \wedge b \models c$$

\vdots



$$\text{iff } a \models b \Rightarrow c .$$

Example proofs (2) eventually-and-always \diamond & \square

Lemma: For all A, B we have $\diamond A \ \& \ \square B \ \Rightarrow \ \diamond(A \ \& \ B)$.

Proof: We reason

$$\begin{array}{l} \diamond A \ \& \ \square B \ \Rightarrow \ \diamond(A \ \& \ B) \\ \text{iff } \diamond A \ \Rightarrow \ \square B \ \multimap \ \diamond(A \ \& \ B) \end{array}$$

$\&, \multimap$ are \Rightarrow -adjoints



Example proofs (2) eventually-and-always \diamond & \square

Lemma: For all A, B we have $\diamond A \ \& \ \square B \Rightarrow \diamond(A \ \& \ B)$.

Proof: We reason

$$\begin{aligned} & \diamond A \ \& \ \square B \Rightarrow \diamond(A \ \& \ B) \\ \text{iff } & \diamond A \Rightarrow \square B \multimap \diamond(A \ \& \ B) \\ \\ \text{if } & A \sqcup \circ(\square B \multimap \diamond(A \ \& \ B)) \\ & \Rightarrow \square B \multimap \diamond(A \ \& \ B) \\ \\ \text{iff } & (A \sqcup \circ(\square B \multimap \diamond(A \ \& \ B))) \ \& \ \square B \\ & \Rightarrow \diamond(A \ \& \ B) \end{aligned}$$

$\&, \multimap$ are \Rightarrow -adjoints

\diamond least

$B \Leftarrow \diamond A$ if $B \Leftarrow A \sqcup \circ B$

$\&, \multimap$ are \Rightarrow -adjoints



Example proofs (2) eventually-and-always \diamond & \square

Lemma: For all A, B we have $\diamond A \ \& \ \square B \Rightarrow \diamond(A \ \& \ B)$.

Proof: We reason



$$\begin{aligned} \text{iff} \quad & (A \sqcup \circ(\square B \multimap \diamond(A \ \& \ B))) \ \& \ \square B \\ \Rightarrow \quad & \diamond(A \ \& \ B) \end{aligned}$$

$\&, \multimap$ are \Rightarrow -adjoints

$$\begin{aligned} \text{iff} \quad & A \ \& \ \square B \\ & \sqcup \ \circ(\square B \multimap \diamond(A \ \& \ B)) \ \& \ \square B \\ \Rightarrow \quad & A \ \& \ B \sqcup \ \circ \diamond(A \ \& \ B) \end{aligned}$$

\sqcup distribution
 \diamond **fixed point**

$$\begin{aligned} \text{if} \quad & \circ(\square B \multimap \diamond(A \ \& \ B)) \ \& \ \circ \square B \\ \Rightarrow \quad & \circ \diamond(A \ \& \ B) \end{aligned}$$

$\square B \Rightarrow B, \circ \square B$



Example proofs (2) eventually-and-always \diamond & \square

Lemma: For all A, B we have $\diamond A \ \& \ \square B \ \Rightarrow \ \diamond(A \ \& \ B)$.

Proof: We reason



if $\circ(\square B \rightarrow \diamond(A \ \& \ B)) \ \& \ \circ \square B$ $\square B \Rightarrow B, \circ \square B$
 $\Rightarrow \circ \diamond(A \ \& \ B)$

if $\circ((\square B \rightarrow \diamond(A \ \& \ B)) \ \& \ \square B)$ \circ conjunction
 $\Rightarrow \circ \diamond(A \ \& \ B)$

if $\square B \ \& \ (\square B \rightarrow \diamond(A \ \& \ B))$ \circ monotonic
 $\Rightarrow \diamond(A \ \& \ B) ,$

which is a trivial consequence of $\&, \rightarrow$ adjointness.

Theorem: If the probability of eventually establishing a predicate is everywhere bounded away from zero, then in fact it is one.

Theorem: For standard expectation P and real $0 < c \leq 1$,

if $\underline{c} \Rightarrow \diamond P$, then in fact $\underline{1} \Rightarrow \diamond P$,

where by \underline{c} and similar we mean the everywhere- c expectation, and we say that an expectation is *standard* if it is everywhere either zero or one (thus is the characteristic function of some predicate).

Example proofs (3)

The “zero-one” Law

Proof: We assume a number of algebraic properties of our temporal formulae, and prove the law for the special case in which the transition system is *purely probabilistic*, that is contains no demonic nondeterminism or divergence.

We reason

$$\begin{aligned} & c(\diamond P) \\ \equiv & \diamond(cP) \\ \equiv & \diamond(P \& (\underline{c} + \underline{1} - \diamond P)) \\ \Leftarrow & \diamond P \& \square(\underline{c} + \underline{1} - \diamond P) \\ \Leftarrow & \diamond P \& (\square \underline{c} + \square(\underline{1} - \diamond P)) \\ \equiv & \diamond P \& (\underline{c} + \underline{1} - \diamond P) \\ \equiv & \underline{c} , \end{aligned}$$

But where did we use
the assumption $\underline{c} \Rightarrow \diamond P$?

\diamond scaling

P standard

\diamond - \square lemma

\square sub-distributes +
purely probabilistic system

whence the result $\underline{1} \Rightarrow \diamond P$ follows from division by c .

Example proofs (3)

Algebraic properties used

- **\diamond scaling** $\diamond(cA) \equiv c(\diamond A)$.
- **\square scaling** $\square(cA) \equiv c(\square A)$.
- **\square subdistributes** $p \oplus \square(A \ p \oplus B) \Leftarrow \square A \ p \oplus \square B$.
- **purely probabilistic system** In a purely probabilistic system we have
 - **non-divergence** $\circ \underline{1} \equiv \underline{1}$.
 - **unreachability invariance** $\underline{1} - \diamond A \Rightarrow \square(\underline{1} - \diamond A)$.

A “purely probabilistic system” corresponds to a Markov process; allowing demonic nondeterminism makes it a *Markov Decision Process* (for which the theorem is still true).

Example proofs (3)

Unreachability invariance

A system is *purely probabilistic* when every transition is a one-summing probabilistic choice among possible successors: in qTL that is just the two conditions

- **non-divergence** $\circ \underline{1} \equiv \underline{1}$, and
- **linearity** $\circ(A \oplus_p B) \equiv \circ A \oplus_p \circ B$ for all A, B .

Unreachability invariance is, informally, that if the probability of eventually establishing A is zero now, then it remains zero; that it holds in purely probabilistic systems is proved as follows. We reason

$$\begin{array}{ll} \underline{1} - \diamond A \Rightarrow \square(\underline{1} - \diamond A) & \\ \text{if } \underline{1} - \diamond A \Rightarrow \circ(\underline{1} - \diamond A) & \text{property of } \square \\ \text{iff } \underline{1} - \diamond A \Rightarrow \circ \underline{1} - \circ \diamond A & \text{linearity} \\ \text{iff } \diamond A \Leftarrow \circ \diamond A & \text{non-divergence} \\ \text{iff } A \sqcup \circ \diamond A \Leftarrow \circ \diamond A, & \diamond \text{ fixed point} \end{array}$$

which is trivial.

Example proofs (3)

Unreachability invariance

A system is a one-summing pTL that is just

- non-divergence
- linearity

$$\begin{aligned}
 & \circ B + \circ(\underline{1} - B) \\
 \equiv & 2(\circ B \oplus_{1/2} \circ(\underline{1} - B)) \\
 \equiv & 2(\circ(B \oplus_{1/2} (\underline{1} - B))) \quad \text{linearity} \\
 \equiv & 2(\circ(\underline{1/2})) \\
 \equiv & 2(1/2)(\circ\underline{1}) \quad \text{scaling} \\
 \equiv & \circ\underline{1} .
 \end{aligned}$$

is a
s: in

Unreachability invariance is, informally, that if the probability of eventually establishing A is zero now, then it remains zero; that it holds in purely probabilistic systems is proved as follows. We reason

$$\begin{aligned}
 & \underline{1} - \diamond A \Rightarrow \square(\underline{1} - \diamond A) \\
 \text{if } & \underline{1} - \diamond A \Rightarrow \circ(\underline{1} - \diamond A) \\
 \text{iff } & \underline{1} - \diamond A \Rightarrow \circ\underline{1} - \circ\diamond A \\
 \text{iff } & \diamond A \Leftarrow \circ\diamond A \\
 \text{iff } & A \sqcup \circ\diamond A \Leftarrow \circ\diamond A ,
 \end{aligned}$$

property of \square
linearity
 non-divergence
 \diamond fixed point

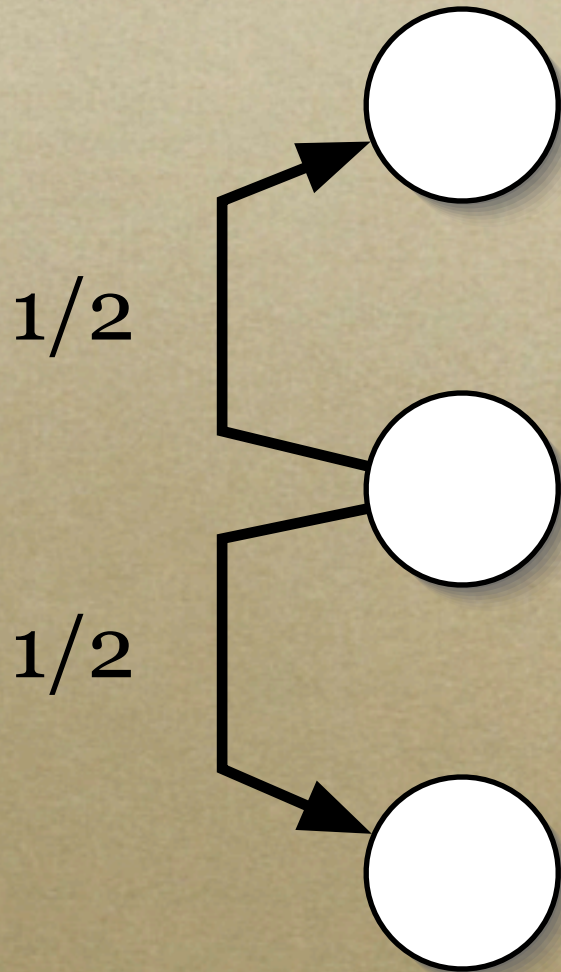
which is trivial.

The *Jumping Bean* sits on the number line and randomly hops an integer distance, either up or down, according to the following rules:

- With some nonzero probability, however small, it *must move* at least one unit up or down.
- There is a *uniform maximum distance*, arbitrarily large but fixed, that it can travel in one jump.
- Its *expected movement is never down*: on average, it either moves up or stays where it is.

Example application

The Jumping Bean

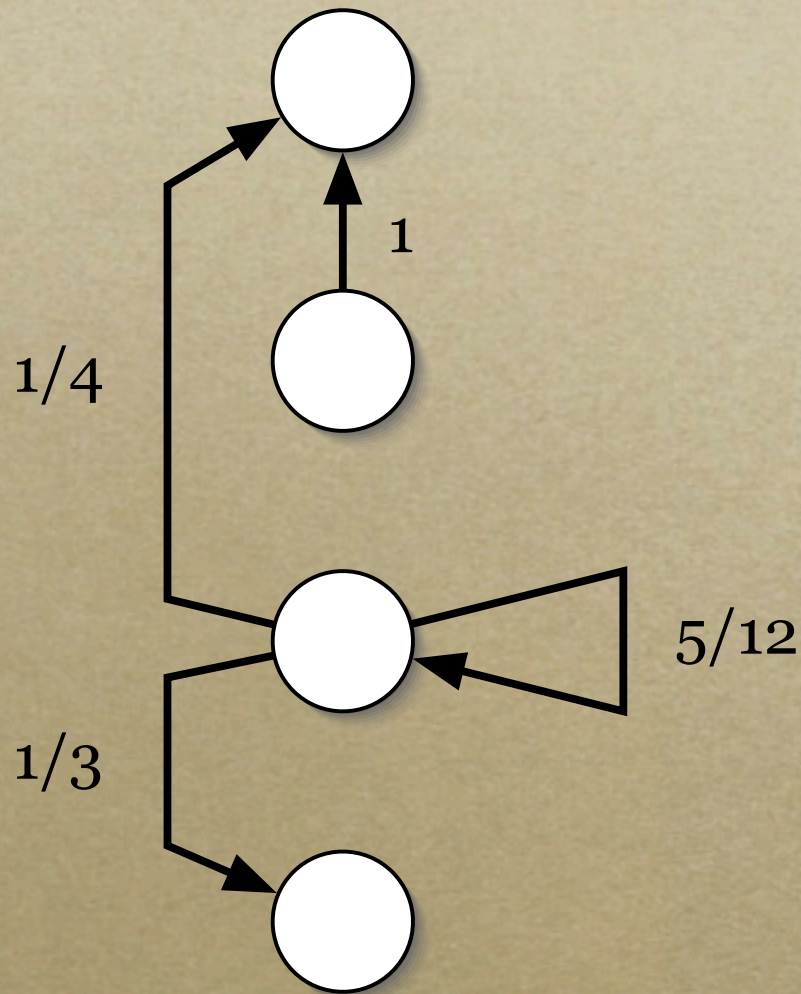


- With some nonzero probability, however small, it *must move* at least one unit up or down.
- There is a *uniform maximum distance*, arbitrarily large but fixed, that it can travel in one jump.
- Its *expected movement is never down*: on average, it either moves up or stays where it is.

The symmetric random walk...

Example application

The Jumping Bean

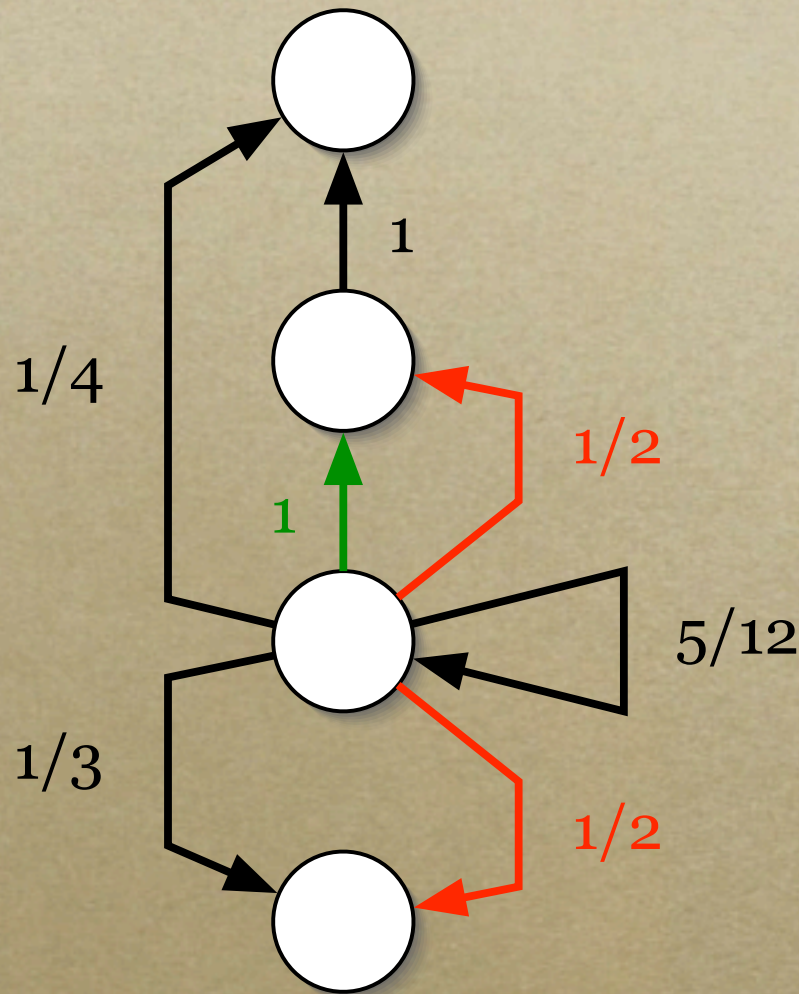


- With some nonzero probability, however small, it *must move* at least one unit up or down.
- There is a *uniform maximum distance*, arbitrarily large but fixed, that it can travel in one jump.
- Its *expected movement is never down*: on average, it either moves up or stays where it is.

...or something more exotic,

Example application

The Jumping Bean



or even unpredictably demonic!

- With some nonzero probability, however small, it *must move* at least one unit up or down.
- There is a *uniform maximum distance*, arbitrarily large but fixed, that it can travel in one jump.
- Its *expected movement is never down*: on average, it either moves up or stays where it is.

The *Jumping Bean* is guaranteed with probability one to climb arbitrarily high — given any point on the line, eventually the bean will be above it.

- If the bean is *symmetric* —so that its average move is everywhere *exactly zero*— then it *visits the whole line* in the sense that eventually it will jump over any given point.
- The bean carries out a *non-homogeneous random walk*: the jumping behaviour can vary from point to point, and can even vary *at the same point* on different visits.

Example application

The Jumping Bean

For all N ,

$$[n = N] \Rightarrow \lceil \circ[n \neq N] \rceil$$

- With some nonzero probability, however small, it *must move* at least one unit up or down.

Integer variable n (lower-case) is interpreted within the current state; integer variable N (upper-case) is interpreted generally.

Square brackets $[\cdot]$ form the *characteristic function* of their (Boolean) argument.

Ceiling brackets $\lceil \cdot \rceil$ take the least integer no less than their (real-valued) argument.

Example application

For all N ,

$$[n = N] \Rightarrow [\circ[n \neq N]]$$

There exists K such that,
for all N ,

$$\Rightarrow \begin{array}{l} [n = N] \\ \circ[N - K \leq n \leq N + K] \end{array}$$

The Jumping Bean

- With some nonzero probability, however small, it *must move* at least one unit up or down.
- There is a *uniform maximum distance*, arbitrarily large but fixed, that it can travel in one jump.

Example application

For all N ,

$$[n = N] \Rightarrow [\circ[n \neq N]]$$

There exists K such that,
for all N ,

$$\Rightarrow \begin{array}{l} [n = N] \\ \circ[N - K \leq n \leq N + K] \end{array}$$

$$n \Rightarrow \circ n$$

The Jumping Bean

- With some nonzero probability, however small, it *must move* at least one unit up or down.
- There is a *uniform maximum distance*, arbitrarily large but fixed, that it can travel in one jump.
- Its *expected movement is never down*: on average, it either moves up or stays where it is.

Example application

The Jumping Bean

There exists $K \geq 0$ such that, for all L, H ,

$$\frac{\langle L : n : H \rangle}{H + K - L} \equiv \circ \left(\frac{\langle L : n : H + K \rangle}{H + K - L} \right),$$

where in general $\langle a : x : b \rangle$ is defined

$$\begin{array}{ll} 0 & \text{if } x < a \\ x - a & \text{if } a \leq x \leq b \\ b - a & \text{if } b < x. \end{array}$$

- Its *expected movement is never down*: on average, it either moves up or stays where it is.

$$n \equiv \circ n$$

Example application

The Jumping Bean

For all N ,

$$[n = N] \Rightarrow [\circ[n \neq N]]$$

Property *JB1*

Property *JB2*

There exists $K \geq 0$ such that, for all L, H ,

$$\frac{\langle L : n : H \rangle}{H + K - L} \Rightarrow \circ \left(\frac{\langle L : n : H + K \rangle}{H + K - L} \right)$$

- With some nonzero probability, however small, it must move at least one unit up or down.
- Its expected movement is *uniformly up-bounded* and never down.

Example application

The Jumping Bean Proof of claim

We fix an arbitrary H for the bean to reach. Then

- Step 1 — We show for arbitrary L that if the bean ever leaves the interval $[L,H]$ the probability it does so at the H end is at least $(N-L)/(H+K-L)$, where N is its initial position.
- Step 2 — We argue that L can be chosen low enough to make that probability at least $1/2$.
- Step 3 — We argue that the bean *will* eventually leave the interval $[L,H]$, with probability one.
- Step 4 — We combine Steps 2,3 and then appeal to the Zero-One Law.

Example application

The Jumping Bean

Step 1

Lemma: For all L

$\langle L$

We show for arbitrary L that if the bean ever leaves the interval $[L, H]$ the probability it does so at the H end is at least $(N-L)/(H+K-L)$, where N is its initial position.

$\leq n]$.

Proof: We

$\langle L : n$

$\leq n]$

if

$\langle L$

$\Rightarrow [H \leq$

$/(H+K-L))$

if

$\langle L : n : H$

$\Rightarrow \circ(\langle L : n : H \rightarrow))$

if Property *JB2*.

Example application

The Jumping Bean Step 1

Lemma: For all L, H and $K \geq 0$ we have

$$\frac{\langle L : n : H+K \rangle}{H + K - L} \Rightarrow [L \leq n] \triangleright [H \leq n] .$$

Proof: We reason

$$\langle L : n : H+K \rangle / (H+K-L) \Rightarrow [L \leq n] \triangleright [H \leq n]$$

$$\begin{array}{l} \text{if} \quad \langle L : n : H+K \rangle / (H+K-L) \\ \Rightarrow [H \leq n] \sqcup ([L \leq n] \sqcap \circ(\langle L : n : H+K \rangle / (H+K-L))) \end{array}$$

$$\begin{array}{l} \text{if} \quad \langle L : n : H \rangle / (H+K-L) \\ \Rightarrow \circ(\langle L : n : H+K \rangle / (H+K-L)) \end{array}$$

if Property *JB2*.

Example application

The Jumping Bean

Step 2

We have just proved

$$\frac{\langle L : n \rangle}{H - K} \geq \frac{1}{2} [H \leq n] .$$

We argue that L can be chosen low enough to make that probability at least $1/2$.

$$[H \leq n] .$$

Thus, given initial conditions

choose L satisfying

$$(N - L) / (H - K) = 1/2 ,$$

for which $L \hat{=} 2N - (H + K)$ suffices.

Example application

The Jumping Bean Step 2

We have just proved

$$\frac{\langle L : n : H+K \rangle}{H + K - L} \Rightarrow [L \leq n] \triangleright [H \leq n] .$$

Thus, given initial position N , we must choose L satisfying

$$(N - L)/(H + K - L) = 1/2 ,$$

for which $L \hat{=} 2N - (H+K)$ suffices.

Example application

The Jumping Bean **Step 3**, informally

If the bean must move with some nonzero probability, and its expected movement is never down,

then on every jump with some nonzero probability, it must move up...

and so by the Zero-One Law it must leave $[L, H]$ eventually.

We argue that the bean *will* eventually leave the interval $[L, H]$, with probability one.

With some nonzero probability, however small, it will move at least one unit

uniform maximum arbitrarily large but it can travel in one

expected movement is never down: on average, it either moves up or stays where it is.

Example application

If the bean must move with some nonzero probability, and its expected movement is never down,

then on every jump, with some nonzero probability, it must move up...

and so by the Zero-One Law it must leave $[L,H]$ eventually.

The Jumping Bean Step 3, informally

- With some nonzero probability, however small, it *must move* at least one unit up or down.
- There is a *uniform maximum distance*, arbitrarily large but fixed, that it can travel in one jump.
- Its *expected movement is never down*: on average, it either moves up or stays where it is.

Example application

The Jumping Bean Step 3, formally

The 1-boundedness restriction on formulae is relaxed for convenience of calculation, replacing it (in this case) with a bound of $K + 1$. Soundness is guaranteed by scaling.

Assuming we are in a state where $n = N$, we calculate

$$\begin{aligned} & K(\circ[N < n]) \\ \geq & \circ\langle N : n : N+K \rangle \\ = & \circ(\langle N-1 : n : N \rangle + \langle N : n : N+K \rangle - [n = N]) \\ = & \circ(\langle N-1 : n : N+K \rangle + [n \neq N] - \underline{1}) \\ = & \circ\langle N-1 : n : N+K \rangle + \circ[n \neq N] - 1 \\ = & \langle N-1 : n : N \rangle + \circ[n \neq N] - 1 \\ = & \circ[n \neq N] \\ > & 0 . \end{aligned}$$

◦ sub-linearity
Property *JB2*
state satisfies $n = N$,
and Property *JB1*

Example application

The Jumping Bean

Step 4

We reason

$$\begin{aligned} & \diamond[H \leq n] \\ \Leftarrow & [L \leq n] \triangleright [H \leq n] \Leftarrow [H \leq n] \\ \equiv & [L \leq n] \triangleright [L \leq n] \\ \Leftarrow & \frac{1}{2} \ \& \ \underline{1} \\ \equiv & \underline{\frac{1}{2}}. \end{aligned}$$

We combine Steps 2,3 and then appeal to the Zero-One Law.

The second step uses the Zero-One law whose proof is similar to the proof of the *always-eventually* law.

We note finally that if the probability of eventually exceeding H is everywhere at least $1/2$ then, by the Zero-One Law, it must be one — and we are done.

Example application

The Jumping Bean Step 4

We reason

$$\begin{aligned} & \diamond[H \leq n] \\ \Leftrightarrow & [L \leq n] \triangleright [H \leq n] \ \& \ \diamond([L \leq n] \rightarrow [H \leq n]) \\ \equiv & [L \leq n] \triangleright [H \leq n] \ \& \ \diamond([n < L \vee H \leq n]) \\ \Leftrightarrow & \frac{1}{2} \ \& \ \underline{1} \\ \equiv & \underline{\frac{1}{2}} . \end{aligned}$$

The second step uses an *unless-eventually* law whose proof is similar to the proof given earlier for the *always-eventually* law.

We note finally that if the probability of eventually exceeding H is everywhere at least $1/2$ then, by the Zero-One Law, it must be one — and we are done.

Exercises

Ex. 1: A jumping bean that doesn't make it

Consider a jumping bean with the following code:

$$n < 0 \quad \longrightarrow \quad n := n^2 \quad \frac{1}{n^2} \oplus \quad n := n - 1$$

$$n \geq 0 \quad \longrightarrow \quad n := n + 1$$

Show that if started at (negative) position $-N$, its probability of reaching zero is only $1/N$, and hence that it does not have the “eventually exceeds” property we have just proved.

Exercises

Ex. 2: Necessity of bean properties

We showed that a bean having the three properties at right will eventually reach or exceed any position on the line.

Which property fails for the bean of Ex. 1?

Find examples that show each of the other two properties are necessary as well.

- With some nonzero probability, however small, it *must move* at least one unit up or down.
- There is a *uniform maximum distance*, arbitrarily large but fixed, that it can travel in one jump.
- Its *expected movement is never down*: on average, it either moves up or stays where it is.

Exercises

Ex. 3: Formal logic

We have been somewhat informal about the “rules” usually associated with a logic: Which are the axioms of qTL ? What are the rules of inference? How do we “fold in” the use of (standard) predicate logic and arithmetic?

What exactly do we mean when we say this logic is “sound”?

Suggest how these details can be tightened up, by considering which of our claims could be axioms and which could be rules of inference, and deciding what the “quantitative” entailment should be for qTL . What corresponds to *Modus Ponens*? Is there a *Deduction Theorem*?

Check your approach by formalising the claim that it is sound to reason within any non-negative bounded interval $[0, B]$ if it is sound to reason within $[0, 1]$, provided certain changes are made to the “propositional” operators. What changes, exactly?