Formal Methods for Probabilistic Systems

Annabelle McIver
Carroll Morgan

- Probabilistic temporal logic: *qTL*
- Probabilistic sequential-programming logic: *pGCL*
- Probabilistic modal mu-calculus: *qM*μ

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/`

`www.cse.unsw.edu.au/~carrollm/canberra04/`

Formal Methods for Probabilistic Systems

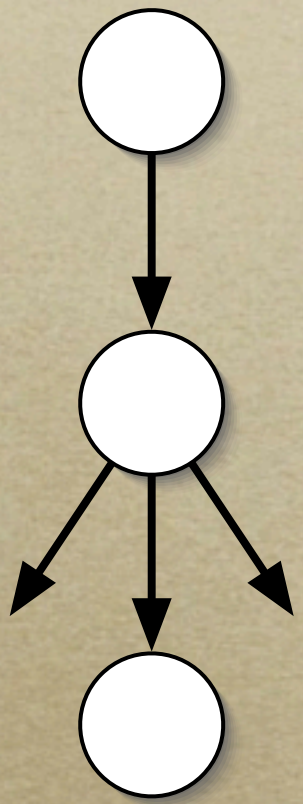
Annabelle McIver
Carroll Morgan

- 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



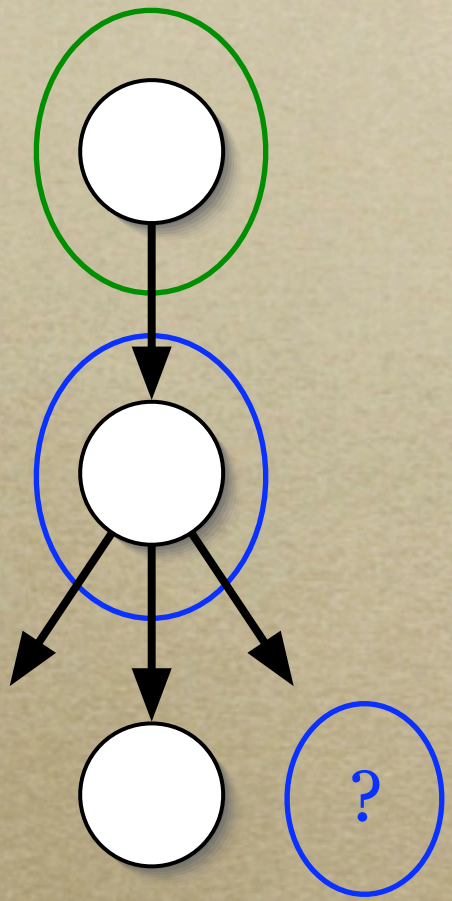
Predicate operators

next-time ○

transitions ↓

○ states

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



predicate ○*A*

predicate *A*

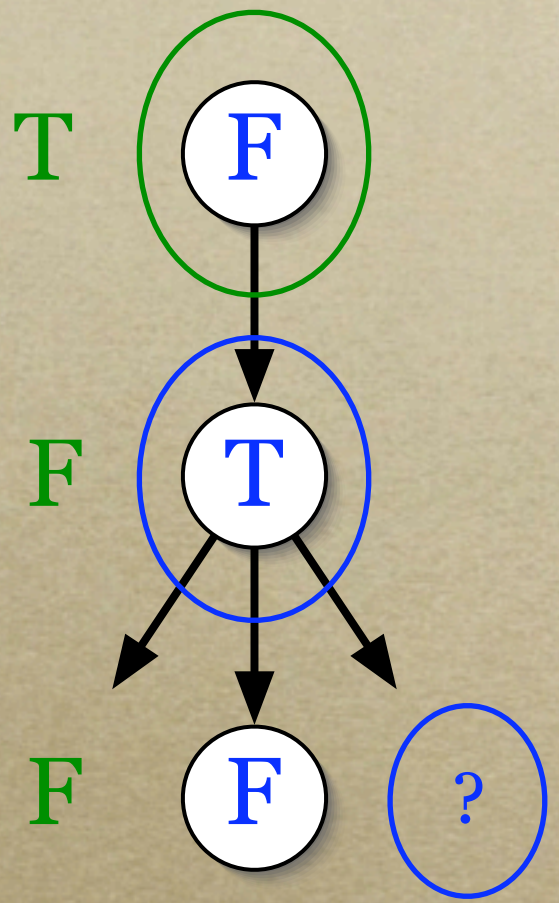
Predicate operators

next-time ○

transitions ↓

○ states

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



predicate ○*A*

predicate *A*

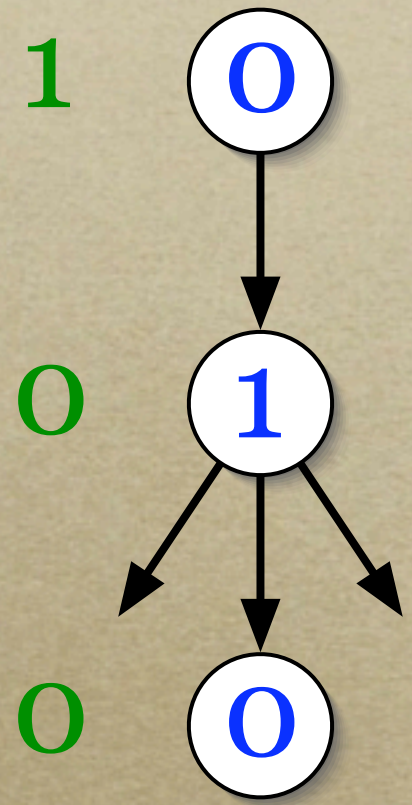
Predicate operators

next-time ○

transitions ↓

○ states

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



predicate ○*A*

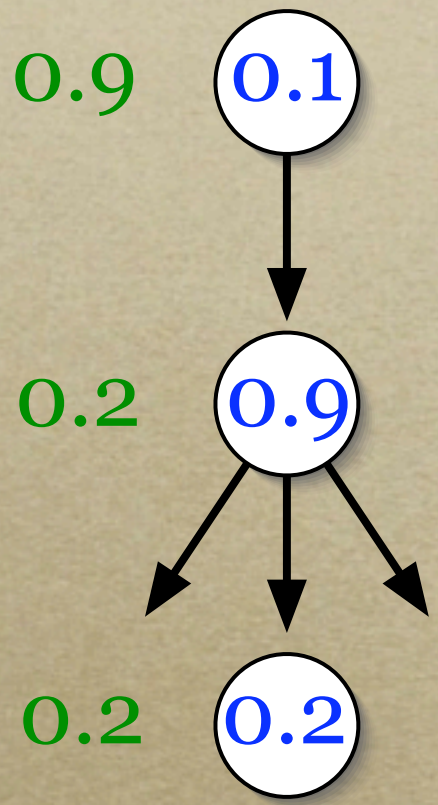
predicate *A*

Expectation operators *next-time* ○

standard
transitions ↓

○ states

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



expectation ○*A*

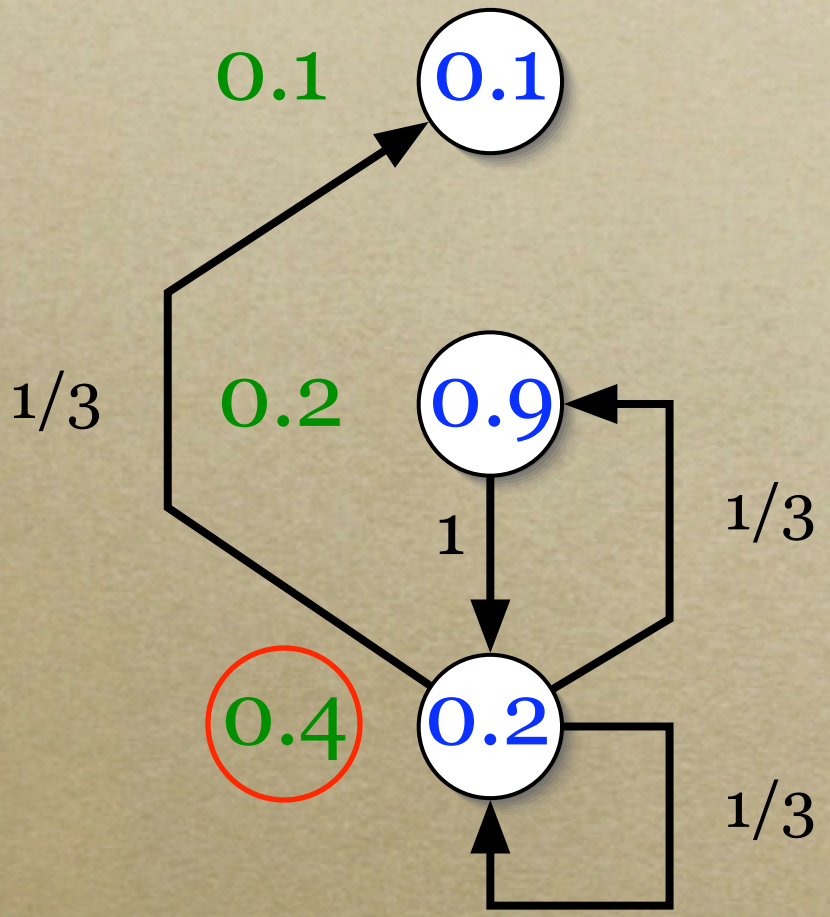
expectation *A*

Expectation operators *next-time* ○

probabilistic transitions ↓

states

For probabilistic nondeterminism, take expected value over all successors



expectation ○*A*

expectation *A*

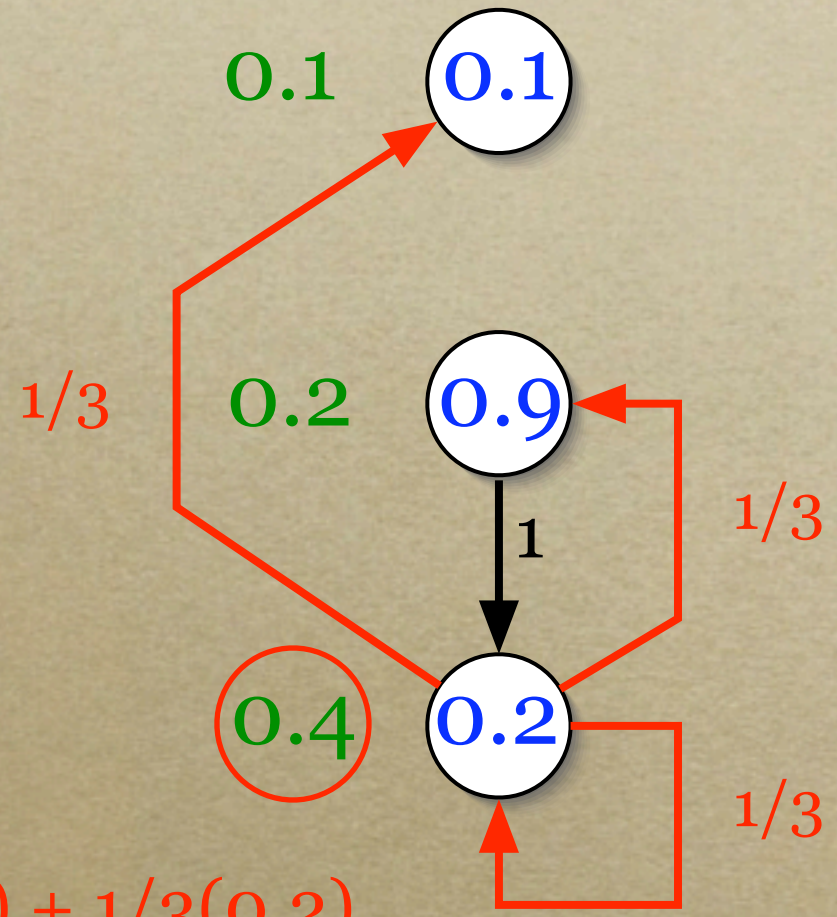
Expectation operators

next-time ○

probabilistic transitions ↓

○ states

For probabilistic nondeterminism, take expected value over all successors



expectation ○*A*

expectation *A*

1/3(0.1) + 1/3(0.9) + 1/3(0.2)

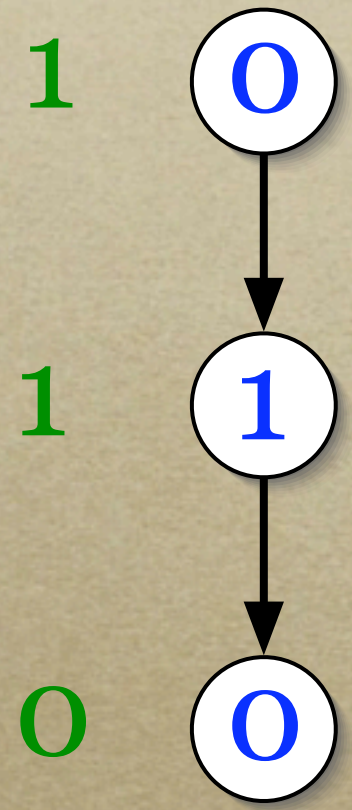
Predicate operators

eventually ◊

standard
transitions

states

For eventually,
seek the maximum



expectation ◊*A*

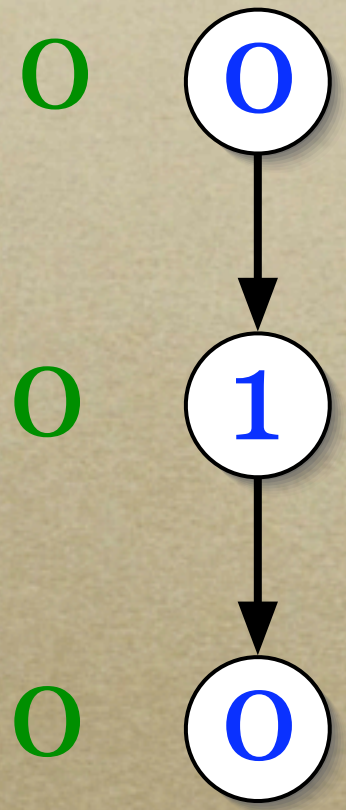
expectation *A*

Predicate operators

always □

standard transitions ↓

○ states



For always, seek the minimum

expectation □*A*

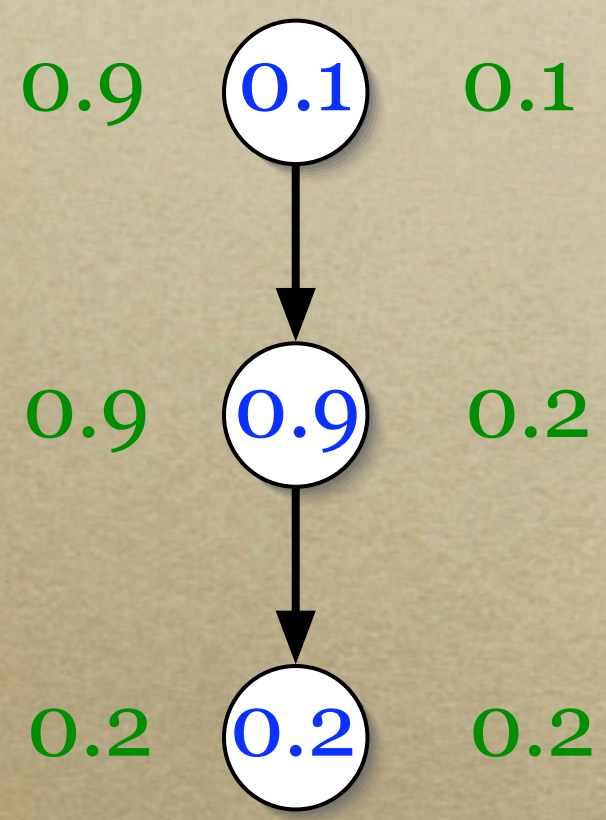
expectation *A*

Expectation operators

eventually ◇
always □

standard transitions ↓

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



expectation ◇*A*

For eventually, seek the maximum

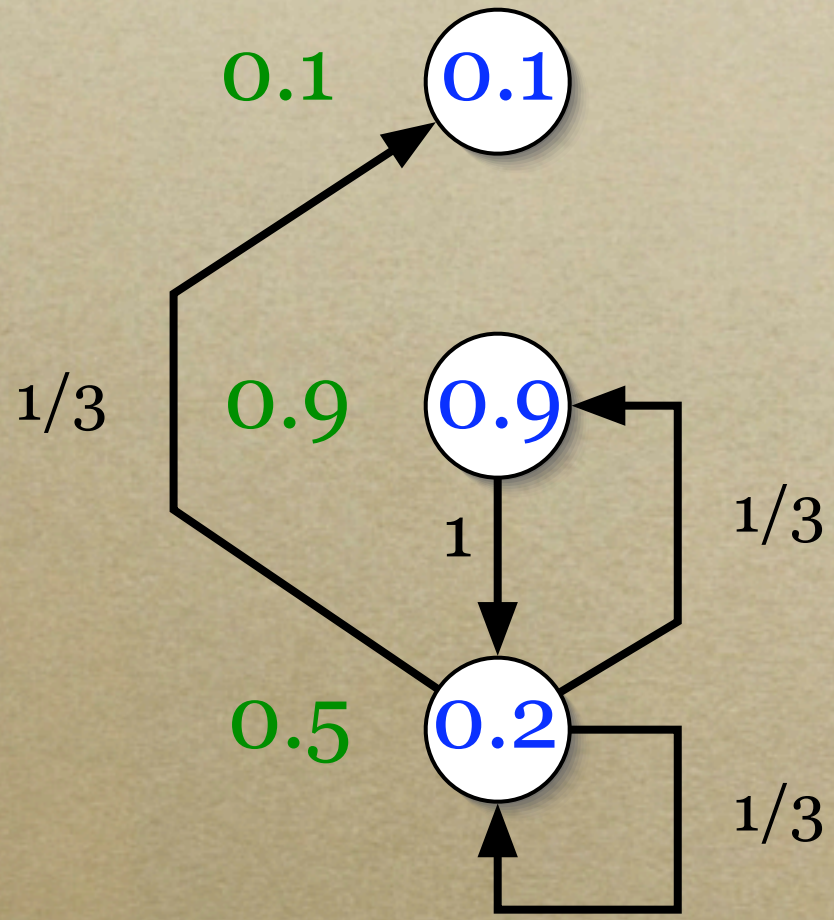
expectation □*A*

For always, seek the minimum

Expectation operators *eventually* ◇

probabilistic
transitions ↓

For eventually,
seek the maximum



expectation ◇*A*

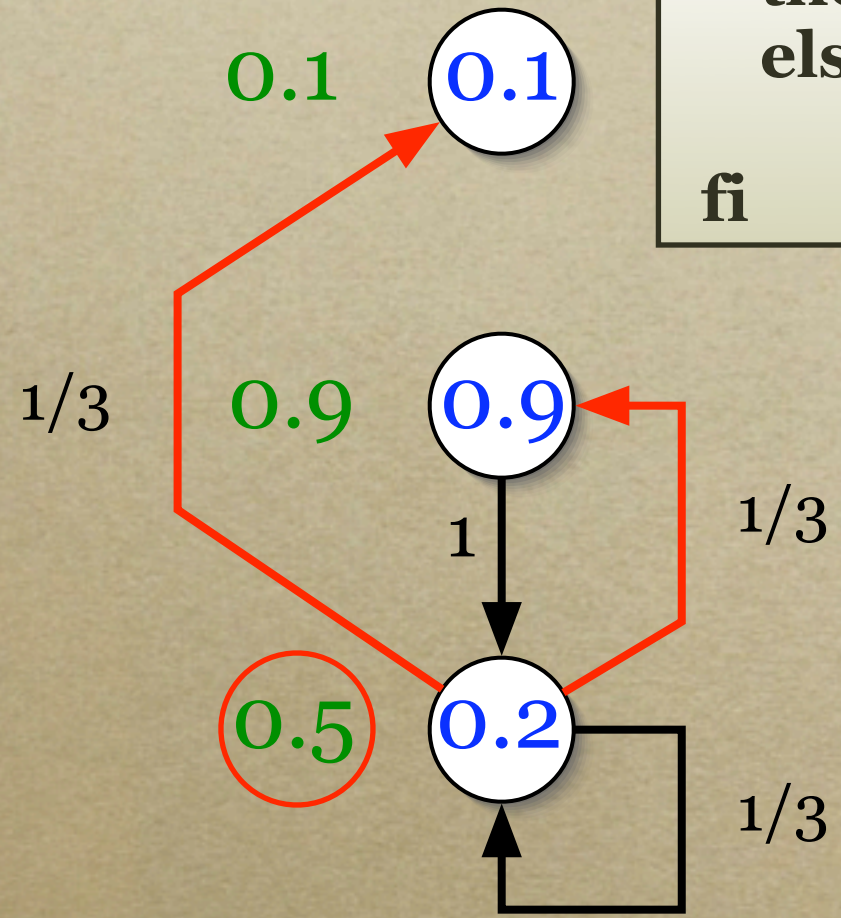
expectation *A*

Expectation operators *eventually* ◇

probabilistic transitions ↓

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

For eventually, seek the maximum



expectation ◇*A*

expectation *A*

[1/3(0.1) + 1/3(0.9)]
/ [1/3 + 1/3]

Expectation operators *eventually* ◊

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*; *repeat*
fi

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

Expectation operators — *always* □

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

expectation $\Box A$

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*; *repeat*
fi

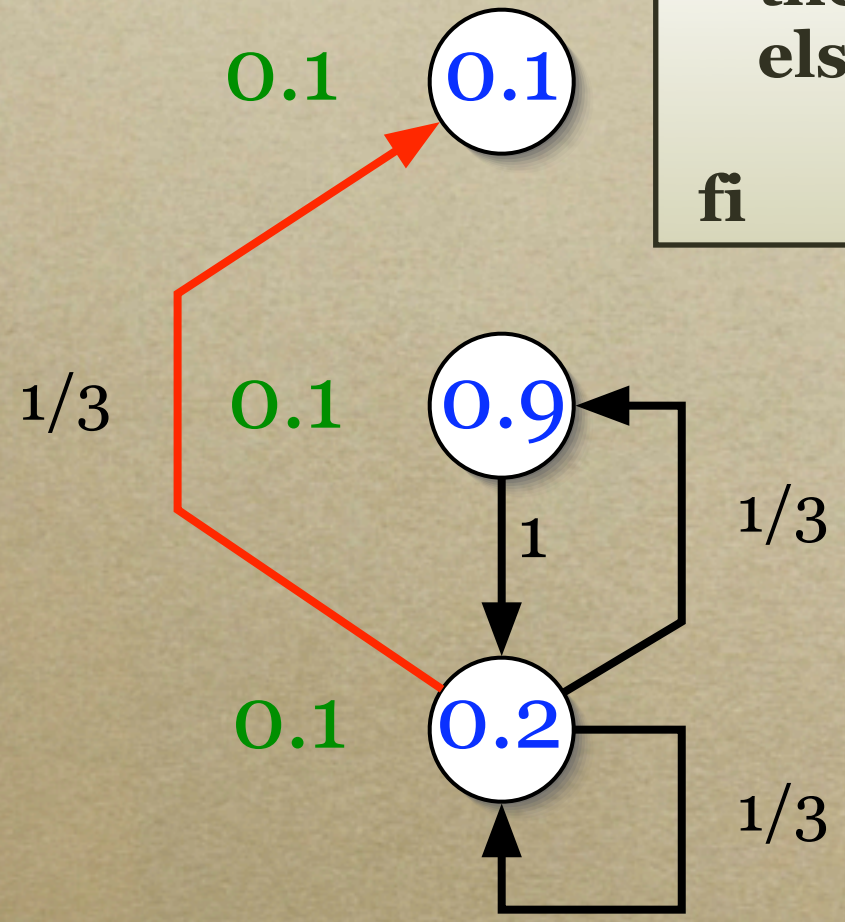
There can be demonic (minimising) choices made here, "built-in" to the transition system over which the *eventually* is taken.

Expectation operators *always* □

probabilistic transitions ↓

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

For always, seek the minimum

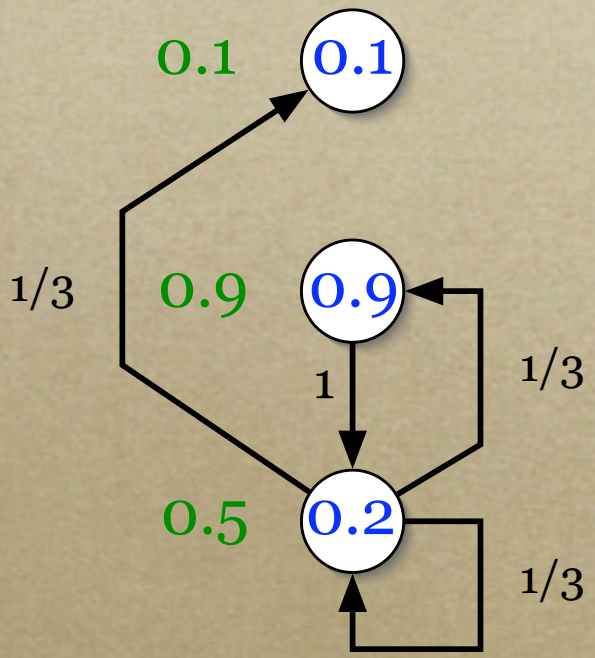


expectation □*A*

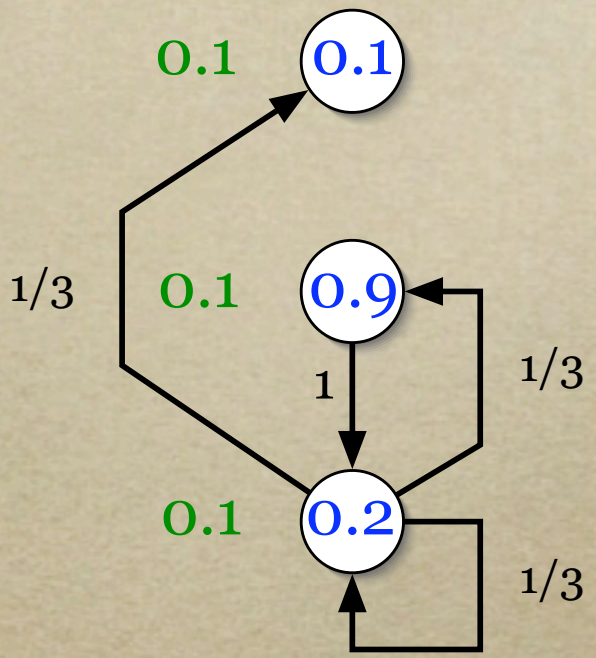
expectation *A*

Expectation operators

eventually ◇
always □



These modalities satisfy fixed-point equations.



expectation ◇*A*

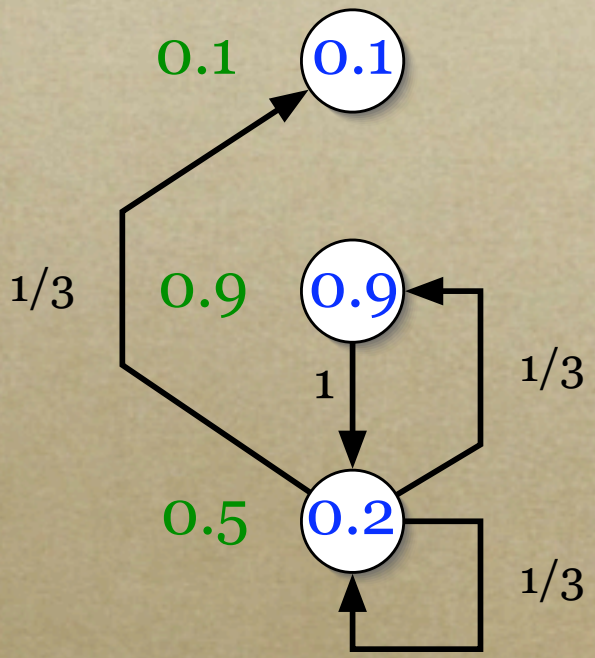
For eventually, seek the maximum

expectation □*A*

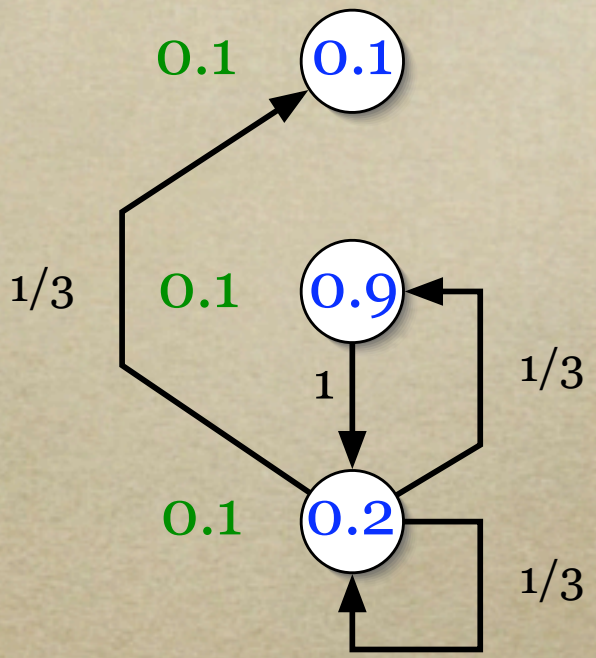
For always, seek the minimum

Expectation operators

eventually ◇
always □



These modalities satisfy fixed-point equations.



expectation ◇*A*

$$\Diamond A = A \sqcup \bigcirc \Diamond A$$

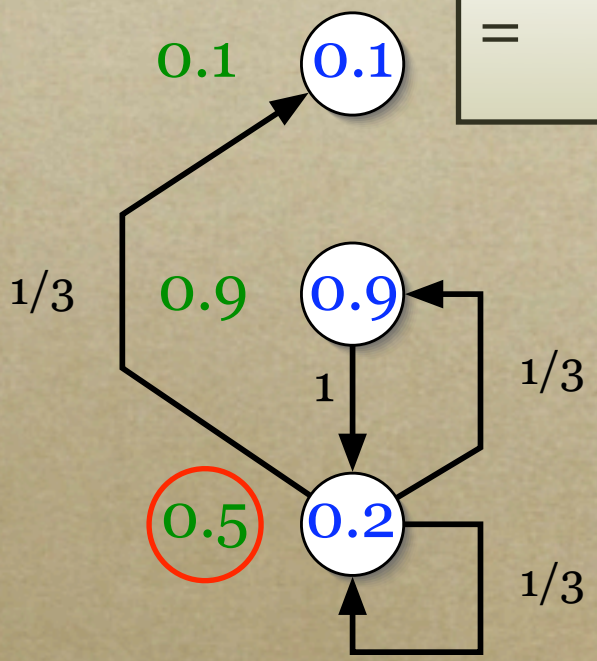
expectation □*A*

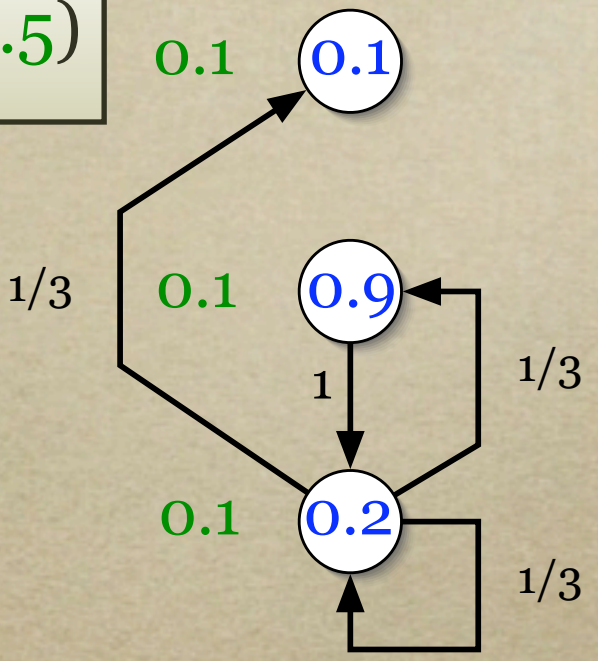
$$\Box A = A \sqcap \bigcirc \Box A$$

Expectation operators

eventually ◇
always □

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





expectation $\Diamond A$

$$\Diamond A = A \sqcup \bigcirc \Diamond A$$

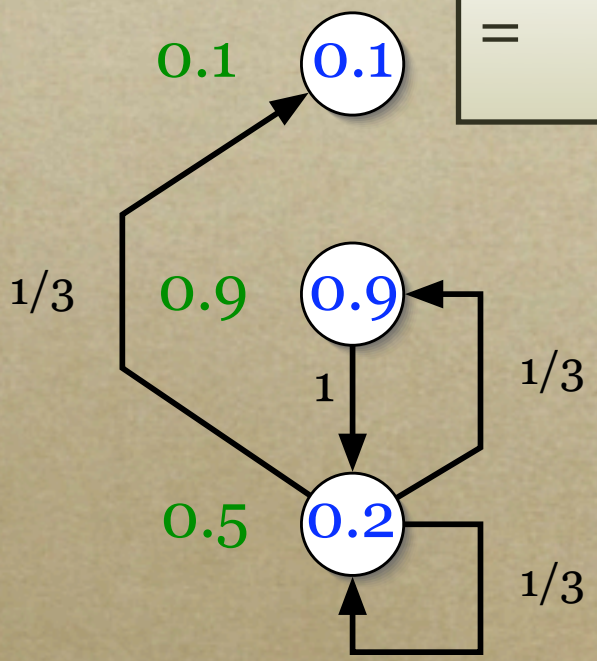
expectation $\Box A$

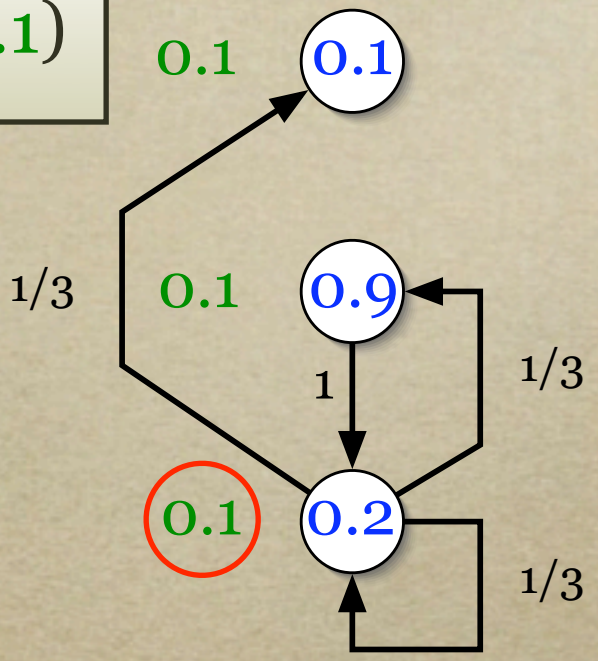
$$\Box A = A \sqcap \bigcirc \Box A$$

Expectation operators

eventually ◇
always □

$$0.1 = 0.2 \sqcap (1/3)(0.1+0.1+0.1)$$





expectation $\Diamond A$

$\Diamond A = A \sqcup \bigcirc \Diamond A$

expectation $\Box A$

$\Box A = A \sqcap \bigcirc \Box A$

The quantitative temporal logic qTL — *syntax*

$$
\begin{aligned}
A \quad \widehat{=} \quad & \mathsf{E} \mid A_1 \sqcap A_2 \mid A_1 \sqcup A_2 \mid \neg A \\
\mid \quad & \circ A \mid \Diamond A \mid \Box A \mid A_1 \rhd A_2
\end{aligned}
$$

- Formulae 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.
- $\circ$, $\Diamond$, $\Box$ and $\rhd$ 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:

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

The quantitative temporal logic qTL — *interpretation*

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

- $[\![\mathsf{E}]\!].s$ 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).

- $[\![A_1 \sqcap A_2]\!]$ and $[\![A_1 \sqcup A_2]\!]$ are the pointwise minimum and maximum respectively of $[\![A_1]\!]$ and $[\![A_2]\!]$.

- $[\![\neg A]\!].s$ is $1 - [\![A]\!].s$.

The quantitative temporal logic qTL — *interpretation*

We write $[\![A]\!]_{\mathcal{X},\mathcal{S}}.s$ for the value of A at state s relative to a de… $\mathbb{P}.\overline{S}$ over…

- $[\![$… s. T… of p… es- s… re r… ne (…

- $[\![$… nd maximum respectively of $[\![A_1]\!]$ and $[\![A_2]\!]$.

- $[\![\neg A]\!].s$ is $1-[\![A]\!].s$.

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.

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

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

The quantitative temporal logic qTL — *interpretation*

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

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

$$[\![\circ A]\!] \quad = \quad [\![\circ]\!].[\![A]\!] \ .$$

- $[\![\diamond A]\!]$ is the *least fixed-point* of the function $\mathcal{F}$ defined

$$\mathcal{F}.\mathsf{X} \quad \widehat{=} \quad [\![A]\!] \ \sqcup \ [\![\circ]\!].\mathsf{X} \ ,$$

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

The quantitative temporal logic qTL — *interpretation*

- $[\![\Box A]\!]$ is the *greatest fixed-point* of the function $\mathcal{G}$ defined

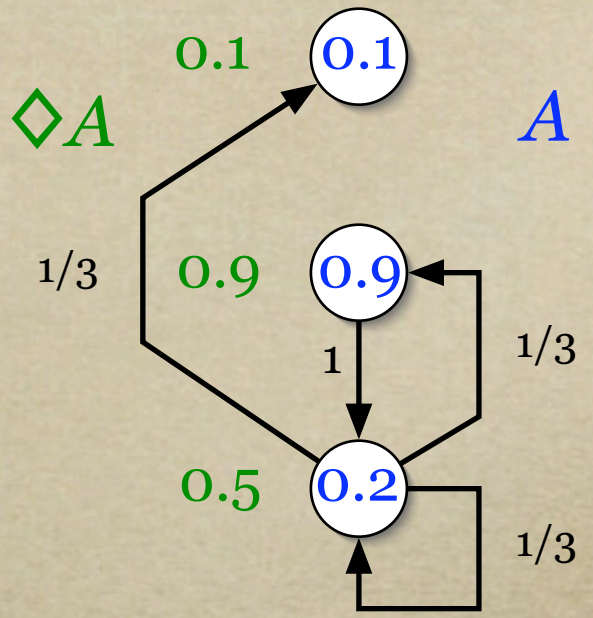
$$\mathcal{G}.\mathsf{X} \;\widehat{=}\; [\![A]\!] \sqcap [\![\circ]\!].\mathsf{X} \; .$$

- $[\![A_1 \rhd A_2]\!]$ is the *greatest fixed-point* of the function $\mathcal{U}$ defined

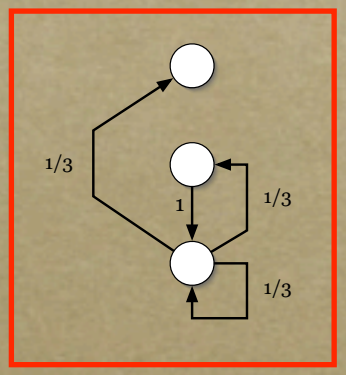
$$\mathcal{U}.\mathsf{X} \;\widehat{=}\; [\![A_2]\!] \sqcup ([\![A_1]\!] \sqcap [\![\circ]\!].\mathsf{X}) \; .$$

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:

$$[\![\Diamond A]\!] \quad = \quad (\mu X \cdot [\![A]\!] \sqcup [\![\circ]\!].X)$$

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

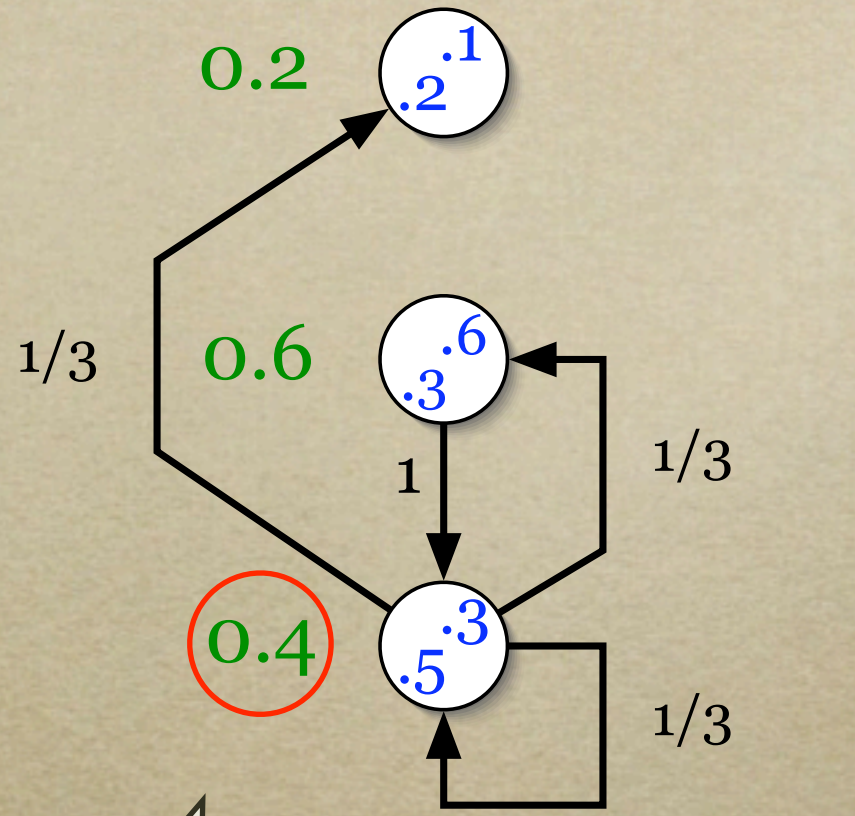
Theorem: The game-and-strategy *operational* definitions for the temporal operators agree with the *denotational* interpretations given above in terms of least- and greatest fixed points.

Annabelle McIver and Carroll Morgan.
Games, probability and the quantitative mu-calculus qMu.
Proc LPAR 2002, *LNAI* 2514, Springer-Verlag, 2002.

Expectation operators

unless ▷

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** $\quad \circ(pA) \;\equiv\; p(\circ A)$ for $0 \leq p \leq 1$.
- **choice** $\quad \circ(A \,{}_p\!\oplus\, B) \;\Leftarrow\; (\circ A) \,{}_p\!\oplus\, (\circ B)$ for $0 \leq p \leq 1$.
- **conjunction** $\quad \circ(A \,\&\, B) \;\Leftarrow\; (\circ A) \,\&\, (\circ B)$.

- **probabilistic choice** $\quad A \,{}_p\!\oplus\, B \;\equiv\; pA + (1{-}p)B$.
- **probabilistic conjunction** $\quad A \,\&\, B \;\equiv\; (A + B - 1) \sqcup 0$.
- **probabilistic implication *etc.***
  $A \Leftarrow B$ iff $A \geq B$ everywhere.
  $A \Rrightarrow B$ iff $A \leq B$ everywhere.
  $A \equiv B$ iff $A \Leftarrow B$ and $A \Rrightarrow B$.

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** $\quad \diamond A \;\equiv\; A \sqcup (\circ \diamond A)$.
- $\diamond$ **least** $\quad B \Leftarrow \diamond A$ if $B \Leftarrow A \sqcup (\circ B)$.

"Axioms" and "rules of inference"

always $\Box$
unless $\triangleright$

Properties of $\Box$

- $\Box$ **fixed point** $\quad \Box A \equiv A \sqcap (\circ \Box A)$.
- $\Box$ **greatest** $\quad B \Rrightarrow \Box A$ if $B \Rrightarrow A \sqcap (\circ B)$.

Properties of $\triangleright$

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

Example proofs (1) *double-eventually* ◇◇

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

Proof: For $\Diamond\Diamond A \Lessdot \Diamond A$ we reason

$$\begin{array}{ll} & \Diamond\Diamond A \\ \equiv & \Diamond(A \sqcup (\circ\Diamond\Diamond A)) \\ \Lessdot & \Diamond A \end{array}$$

◇ **fixed point**

◇ monotonic

For the other direction we reason

$$\begin{array}{ll} & \Diamond A \sqcup (\circ\Diamond A) \\ \Gtrdot & \Diamond A \sqcup A \sqcup (\circ\Diamond A) \\ \equiv & \Diamond A \sqcup \Diamond A \\ \equiv & \Diamond A, \end{array}$$

◇ **fixed point**

hence by ◇ **least** we have $\Diamond\Diamond A \Gtrdot \Diamond A$.

$B \Lessdot \Diamond A$ if $B \Lessdot A \sqcup \circ B$

Example proofs (2) eventually-and-always $\Diamond\&\Box$

Lemma: For all A, B we have $\Diamond A \,\&\, \Box B \Rrightarrow \Diamond(A \,\&\, B)$.

Proof: We reason

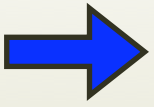
$$\begin{array}{lrcl} & \Diamond A \,\&\, \Box B & \Rrightarrow & \Diamond(A \,\&\, B) \\ \text{iff} & \Diamond A & \Rrightarrow & \Box B \multimap \Diamond(A \,\&\, B) \end{array}$$

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

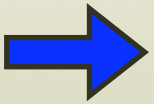
adjoint property

$\&, \multimap$ are $\Rrightarrow$-adjoints. . . ?

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



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



provided we make the definition $b \multimap c \;\widehat{=}\; (1 - b + c) \sqcap 1$.

Example proofs (2) eventually-and-always $\Diamond \wedge \Box$

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

Proof: We reason

$$\begin{array}{lll} & \Diamond A \wedge \Box B & \models \quad \Diamond(A \wedge B) \\ \text{iff} & \Diamond A & \models \quad (\Box B \Rightarrow \Diamond(A \wedge B)) \end{array}$$

$\wedge, \Rightarrow$ are $\models$-adjoints

adjoint property

$\wedge, \Rightarrow$ are $\models$-adjoints

$$a \wedge b \models c$$

$$\vdots$$

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

Example proofs (2) eventually-and-always $\Diamond \& \Box$

Lemma: For all A, B we have $\Diamond A \,\&\, \Box B \Rrightarrow \Diamond(A \,\&\, B)$.

Proof: We reason

$$\begin{array}{rcl} & \Diamond A \,\&\, \Box B & \Rrightarrow \quad \Diamond(A \,\&\, B) \\ \text{iff} & \Diamond A & \Rrightarrow \quad \Box B \multimap \Diamond(A \,\&\, B) \end{array}$$

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

Example proofs (2) eventually-and-always ◇&□

Lemma: For all A, B we have $\boxed{\Diamond A \,\&\, \Box B \Rrightarrow \Diamond(A \,\&\, B).}$

Proof: We reason

$$
\begin{array}{lll}
 & \Diamond A \,\&\, \Box B \;\Rrightarrow\; \Diamond(A \,\&\, B) & \\
\text{iff} & \Diamond A \;\Rrightarrow\; \Box B \multimap \Diamond(A \,\&\, B) & \&, \multimap \text{ are } \Rrightarrow\text{-adjoints} \\
 & & \\
\text{if} & A \sqcup \circ(\Box B \multimap \Diamond(A \,\&\, B)) & \Diamond \textbf{ least} \\
 & \Rrightarrow\; \Box B \multimap \Diamond(A \,\&\, B) & B \Lleftarrow \Diamond A \text{ if } B \Lleftarrow A \sqcup \circ B \\
 & & \\
\text{iff} & (A \sqcup \circ(\Box B \multimap \Diamond(A \,\&\, B))) \,\&\, \Box B & \&, \multimap \text{ are } \Rrightarrow\text{-adjoints} \\
 & \Rrightarrow\; \Diamond(A \,\&\, B) &
\end{array}
$$

Example proofs (2) eventually-and-always ◇&□

Lemma: For all A, B we have $\Diamond A \,\&\, \Box B \Rrightarrow \Diamond(A \,\&\, B)$.

Proof: We reason

iff $\quad (A \sqcup \circ(\Box B \mathrel{-\!\!\triangleright} \Diamond(A \,\&\, B))) \,\&\, \Box B$ $\qquad$ $\&, \mathrel{-\!\!\triangleright}$ are $\Rrightarrow$-adjoints

$\Rrightarrow \quad \Diamond(A \,\&\, B)$

iff $\quad A \,\&\, \Box B$ $\qquad$ $\sqcup$ distribution

$\sqcup \quad \circ(\Box B \mathrel{-\!\!\triangleright} \Diamond(A \,\&\, B)) \,\&\, \Box B$ $\qquad$ $\Diamond$ **fixed point**

$\Rrightarrow \quad A \,\&\, B \;\sqcup\; \circ\Diamond(A \,\&\, B)$

if $\quad \circ(\Box B \mathrel{-\!\!\triangleright} \Diamond(A \,\&\, B)) \,\&\, \circ\Box B$ $\qquad$ $\Box B \Rrightarrow B, \circ\Box B$

$\Rrightarrow \quad \circ\Diamond\,(A \,\&\, B)$

Example proofs (2) eventually-and-always ◇&□

Lemma: For all A, B we have $\boxed{\Diamond A \,\&\, \Box B \Rrightarrow \Diamond(A \,\&\, B).}$

Proof: We reason

if $\quad \circ(\Box B \mathrel{-\!\!\triangleright} \Diamond(A \,\&\, B)) \;\&\; \circ\Box B \qquad \Box B \Rrightarrow B, \circ\Box B$

$\quad \Rrightarrow \quad \circ\Diamond\,(A \,\&\, B)$

if $\quad \circ((\Box B \mathrel{-\!\!\triangleright} \Diamond(A \,\&\, B)) \,\&\, \Box B) \qquad \circ$ **conjunction**

$\quad \Rrightarrow \quad \circ\Diamond\,(A \,\&\, B)$

if $\quad \Box B \,\&\, (\Box B \mathrel{-\!\!\triangleright} \Diamond(A \,\&\, B)) \qquad \circ$ monotonic

$\quad \Rrightarrow \quad \Diamond(A \,\&\, B)$,

which is a trivial consequence of $\&, \mathrel{-\!\!\triangleright}$ 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 $0 < c \leq 1$,

$$\text{if } \underline{c} \Rrightarrow \Diamond P, \quad \text{then in fact } \underline{1} \Rrightarrow \Diamond P,$$

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

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

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

$\diamond$ scaling

P standard

$\diamond$-$\Box$ lemma

$\Box$ sub-distributes $+$

purely probabilistic system

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

Example proofs (3) *Algebraic properties used*

- $\Diamond$ **scaling** $\Diamond(cA) \equiv c(\Diamond A)$.
- $\Box$ **scaling** $\Box(cA) \equiv c(\Box A)$.
- $\Box$ **subdistributes** ${}_p\oplus$ $\Box(A \mathrel{{}_p\oplus} B) \Leftarrow \Box A \mathrel{{}_p\oplus} \Box B$.
- **purely probabilistic system** In a purely probabilistic system we have
  - **non-divergence** $\circ\underline{1} \equiv \underline{1}$.
  - **unreachability invariance** $\underline{1} - \Diamond A \Rrightarrow \Box(\underline{1} - \Diamond A)$.

  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** $\circ(A \,{}_p\!\oplus\, B) \equiv \circ A \;{}_p\!\oplus\; \circ B$ 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

$$
\begin{array}{lll}
 & \underline{1} - \diamond A \;\Rrightarrow\; \Box(\underline{1} - \diamond A) & \\
\text{if} & \underline{1} - \diamond A \;\Rrightarrow\; \circ\,(\underline{1} - \diamond A) & \text{property of } \Box \\
\text{iff} & \underline{1} - \diamond A \;\Rrightarrow\; \circ\,\underline{1} - \circ\diamond A & \textbf{linearity} \\
\text{iff} & \diamond A \;\Lleftarrow\; \circ\diamond A & \textbf{non-divergence} \\
\text{iff} & A \sqcup \circ\diamond A \;\Lleftarrow\; \circ\diamond A\,, & \diamond \textbf{ fixed point}
\end{array}
$$

which is trivial.

Example proofs (3) *Unreachability invariance*

A system is … is a one-summing p… s: in qTL that is jus…

- **non-dive…**
- **linearity**

$$
\begin{array}{lll}
 & \circ B \;+\; \circ(\underline{1} - B) & \\
\equiv & 2(\circ B \;{}_{1/2}\!\oplus\; \circ(\underline{1} - B)) & \\
\equiv & 2(\;\circ(B \;{}_{1/2}\!\oplus\; (\underline{1} - B))\;) & \text{linearity} \\
\equiv & 2(\;\circ(\underline{1/2})\;) & \\
\equiv & 2(1/2)(\circ\underline{1}) & \text{scaling} \\
\equiv & \circ\underline{1}\ . &
\end{array}
$$

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

$$
\begin{array}{ll}
 & \underline{1} - \diamond A \;\Rrightarrow\; \Box(\underline{1} - \diamond A) \\
\text{if} & \underline{1} - \diamond A \;\Rrightarrow\; \circ\,(\underline{1} - \diamond A) \\
\text{iff} & \underline{1} - \diamond A \;\Rrightarrow\; \circ\,\underline{1} - \circ\diamond A \\
\text{iff} & \diamond A \;\Lleftarrow\; \circ\diamond A \\
\text{iff} & A \sqcup \circ\diamond A \;\Lleftarrow\; \circ\diamond A\ ,
\end{array}
$$

property of $\Box$

linearity

non-divergence

$\diamond$ **fixed point**

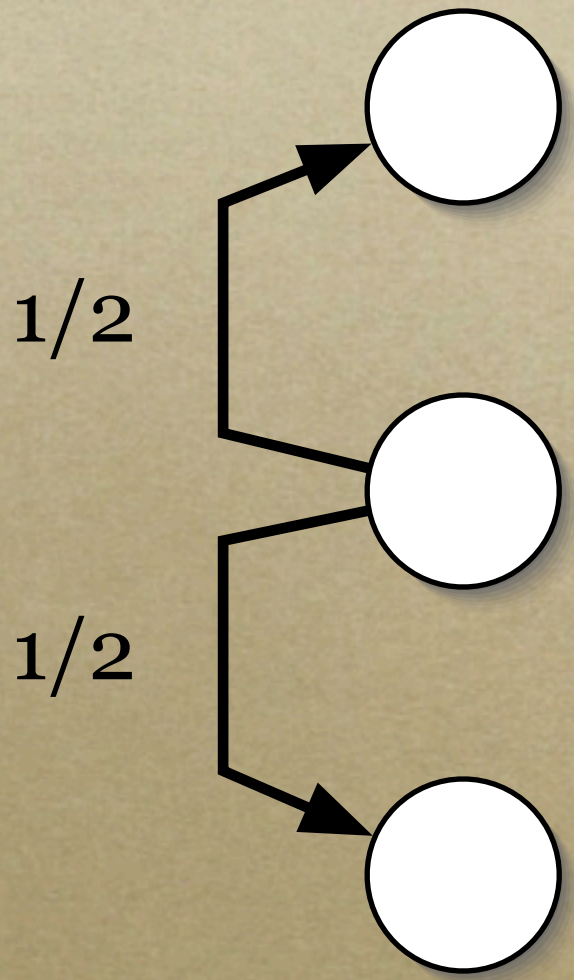
which is trivial.

Example application — *The Jumping Bean*

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

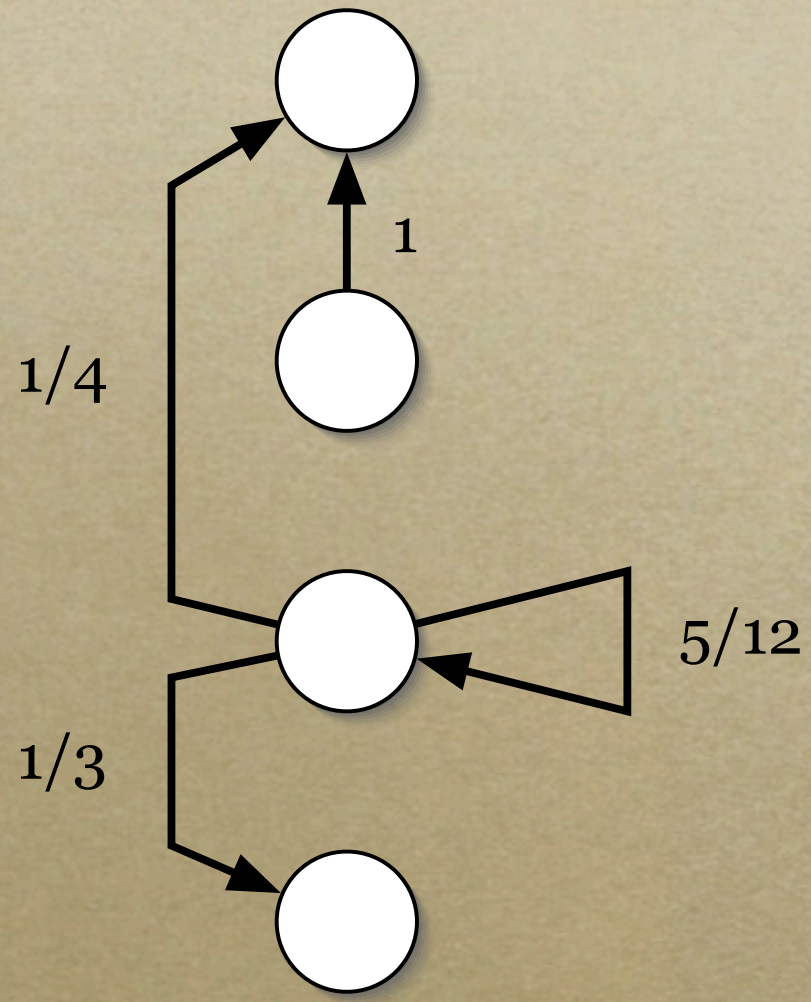


The symmetric random walk…

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

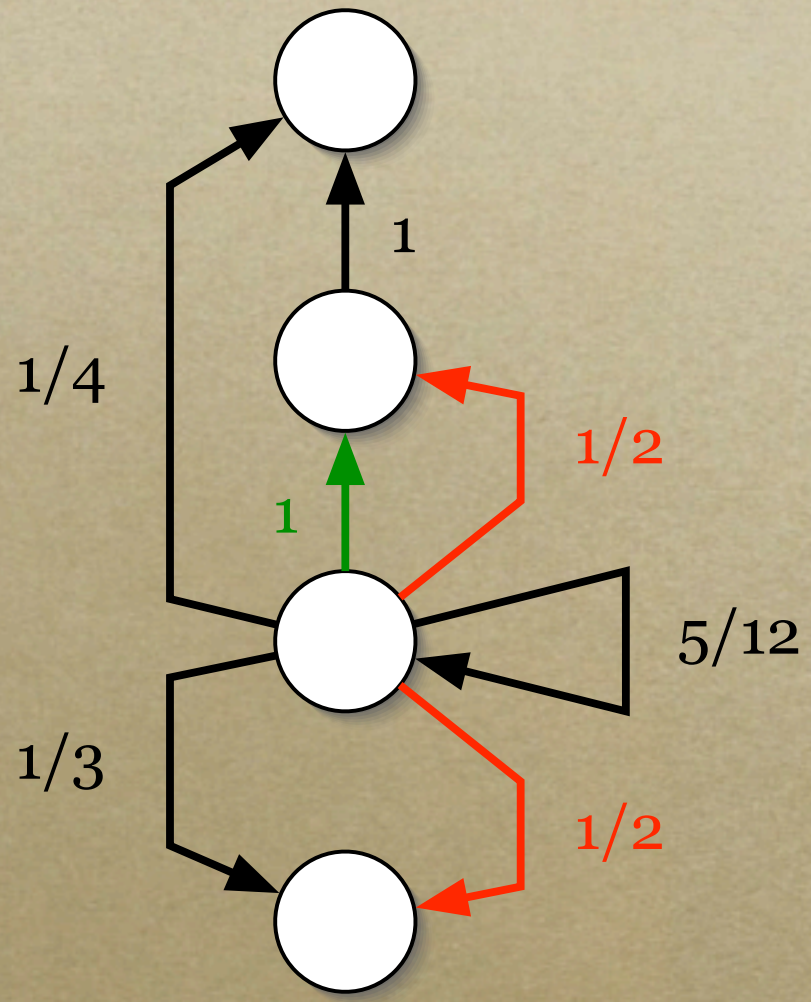


...or something more exotic,

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



or even unpredictably demonic!

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*

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,

$$[n = N] \quad \Rrightarrow \quad \lceil \circ [n \neq N] \rceil$$

- 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,

$$[n = N] \quad \Rrightarrow \quad \lceil \circ[n \neq N] \rceil$$

There exists K such that, for all N,

$$\begin{array}{ll} & [n = N] \\ \Rrightarrow & \circ[N{-}K \leq n \leq N{+}K] \end{array}$$

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,

$$[n = N] \quad \Rrightarrow \quad \lceil \circ[n \neq N] \rceil$$

There exists K such that, for all N,

$$\begin{array}{ll} & [n = N] \\ \Rrightarrow & \circ[N{-}K \leq n \leq N{+}K] \end{array}$$

$$n \quad \Rrightarrow \quad \circ\, n$$

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,

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

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

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

$$n \quad \Rrightarrow \quad \circ n$$

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

Example application

The Jumping Bean

For all N,

$$[n = N] \quad \Rrightarrow \quad \lceil \circ [n \neq N] \rceil$$

Property *JB1*

- 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.

Property *JB2*

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

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

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 $(N\text{-}L)/(H+K\text{-}L)$, 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.

Step 1

Lemma: For all L

$\underline{\langle L :$ $\leq n]$.

Proof: We

$\langle L : n$ $\leq n]$

if $\langle L$

$\Rrightarrow$ $[H \leq$ $/(H+K-L)))$

if $\langle L : n :$

$\Rrightarrow$ $\circ(\ \langle L : n : H$ $)\ )$

if Property *JB2*.

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.

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

$$\frac{\langle L : n : H{+}K \rangle}{H + K - L} \quad \Rrightarrow \quad [L \leq n] \rhd [H \leq n] \ .$$

Proof: We reason

$$\langle L : n : H{+}K \rangle / (H{+}K{-}L) \ \Rrightarrow \ [L \leq n] \rhd [H \leq n]$$

if $\quad \langle L : n : H{+}K \rangle / (H{+}K{-}L)$
$\Rrightarrow \quad [H \leq n] \sqcup ([L \leq n] \sqcap \circ(\langle L : n : H{+}K \rangle / (H{+}K{-}L)))$

if $\quad \langle L : n : H \rangle / (H{+}K{-}L)$
$\Rrightarrow \quad \circ(\ \langle L : n : H{+}K \rangle / (H{+}K{-}L)\ )$

if Property *JB2*.

We have just prove

$$\frac{\langle L : n}{H -} \qquad [H \leq n] \ .$$

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

Thus, given initi oose L satisfying

$$(N - \qquad = \quad 1/2 \ ,$$

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

We have just proved

$$\boxed{\frac{\langle L : n : H{+}K \rangle}{H + K - L} \quad \Rrightarrow \quad [L \leq n] \rhd [H \leq n] \ .}$$

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

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

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

Example application

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

then on every ju with some nonze probability, it mus move up...

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

The Jumping Bean
Step 3, informally

We argue that the bean *will* eventually leave the interval [*L* , *H*] , w i t h probability one.

With some nonzero bility, however small, it *e* at least one unit .

iform maximum bitrarily large but t 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

$$
\begin{array}{lll}
 & K(\circ[N < n]) & \\
\geq & \circ\langle N : n : N{+}K\rangle & \\
= & \circ(\langle N{-}1 : n : N\rangle + \langle N : n : N{+}K\rangle - [n = N]) & \\
= & \circ(\langle N{-}1 : n : N{+}K\rangle + [n \neq N] - \underline{1}) & \\
= & \circ\langle N{-}1 : n : N{+}K\rangle + \circ[n \neq N] - 1 & \circ \text{ sub-linearity} \\
= & \langle N{-}1 : n : N\rangle + \circ[n \neq N] - 1 & \text{Property } \textit{JB2} \\
= & \circ[n \neq N] & \text{state satisfies } n = N, \\
> & 0\ . & \text{and Property } \textit{JB1}
\end{array}
$$

Example application — *The Jumping Bean*

Step 4

We reason

$$
\begin{array}{rl}
 & \Diamond[H \le n] \\
\Leftarrow & [L \le n] \rhd [H \qquad\qquad \rhd [H \le n]) \\
\equiv & [L \le n] \rhd [\qquad\qquad \le n]) \\
\Leftarrow & \underline{1/2} \ \& \ \underline{1} \\
\equiv & \underline{1/2} \ .
\end{array}
$$

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

The second step us law whose proof is similar to the proof g *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.

We reason

$$
\begin{array}{ll}
 & \Diamond[H \leq n] \\
\Lleftarrow & [L \leq n] \triangleright [H \leq n] \;\;\&\;\; \Diamond([L \leq n] \mathrel{-\!\!\triangleright} [H \leq n]) \\
\equiv & [L \leq n] \triangleright [H \leq n] \;\;\&\;\; \Diamond([n < L \vee H \leq n]) \\
\Lleftarrow & \underline{1/2} \;\;\&\;\; \underline{1} \\
\equiv & \underline{1/2}\;.
\end{array}
$$

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:

$$n < 0 \quad \longrightarrow \quad n := n^2 \;\;{}_{1/n^2}\!\oplus\;\; n := n - 1$$

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

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?