Almost-certain eventualities and abstract probabilities in the quantitative temporal logic *qTL*

Annabelle McIver [a,1]

[a] *Dept. of Computing, Macquarie University, Sydney 2019 Australia*

Carroll Morgan [b]

[b] *Dept. of Engineering and Computer Science, University of New South Wales, Sydney 2052 Australia*

Abstract

'Almost-certain eventualities' are liveness properties that hold with probability 1. 'Abstract probabilities' in transition systems are those known only to be bounded away from zero and from one.

Vardi [1] showed that almost-certain properties in linear temporal logic depend only on abstract probabilities, rather than on the probabilities' precise values. We discuss the extent to which a similar result holds in the quantitative temporal logic *qTL* derived from the quantitative modal μ-calculus $qM\mu$ [2,3], and we show how to specialise the logic to those cases. The aim is to provide a simpler calculus than the full logic, one that is in a certain sense complete for proving almost-certain eventualities from abstract-probabilistic assumptions.

We conclude by considering the complexity of the specialised logic.

Key words: Probabilistic temporal logic, quantitative modal μ-calculus, probabilistic transition systems, 0-1 laws, predicate transformers.

Email addresses: anabel@ics.mq.edu.au (Annabelle McIver), carrollm@cse.unsw.edu.au (Carroll Morgan).

[1] McIver was supported by the UK's *EPSRC* during this research.

1 Introduction

Liveness properties of 'standard' non-probabilistic transition systems rely only on the connectivity of the system when considered as a graph. And the same is true in probabilistic systems, up to a point: 'almost-certain eventualities' depend only on 'abstract probabilities', not on precise probabilistic values.

For example, a typical *eventuality* is loop termination, expressed in temporal logic by the formula $\Diamond[\neg G]$ where G is the loop guard; it is *almost certain* iff it occurs with probability 1. Over the state space $\{H, T\}$ the 'coin-flipping' system

$$s{:=}\ H \ \ {}_p\!\oplus \ \ s{:=}\ T \ ,$$

in which ${}_p\!\oplus$ represents probabilistic choice, satisfies both $\Diamond[s{=}H]$ and $\Diamond[s{=}T]$ almost certainly provided constant p lies strictly between zero and one.

More generally an *abstract probabilistic choice*, written just $\oplus$, is one in which the associated probability is not necessarily constant but still is bounded away from 0 and from 1. [2]

In this paper we investigate those issues within our quantitative extension $qM\mu$ [2,3] of the modal μ-calculus [4]; the extension in many cases acts as a probabilistic μ-calculus or even as a probabilistic temporal logic. (It can go beyond those, however, dealing directly with more general aspects like expected complexity [5].)

Our principal contribution here is to show that the quantitative calculus can be specialised to a form of almost-certain eventualities and abstract probabilities, and that results are obtained that are similar to the 'traditional' probabilistic calculi: one does not need precise numeric values for the probabilistic transitions in the underlying system if one is interested only in almost-certain conclusions.

Our second contribution is to give a complexity bound for evaluation of almost certainties.

In the remainder of this section we describe the transition systems with which we will be concerned. Sections 2 and 3 review the existing calculi, in both their Boolean (traditional) and quantitative (our numeric extension) form; in Sections 4 and 5 we present our principal logical results. Section 6 presents a small example; and complexity is discussed in Section 7.

[2] If the state space is finite, or if the probability is constant, then "bounded away from" equates to "is not equal to".

Our main results are Thm. 14 and the complexity bound of Sec. 7.

1.1 Standard *transition systems and the μ-calculus*

We say that a system is *standard* if it is not probabilistic or, if it is probabilistic, when its probabilities are all either 0 or 1. Standard transition systems over a state space S support a *modal μ-calculus* [4] for reasoning about their behaviour; expressions in the calculus denote Boolean-valued *predicates* (equivalently subsets of S), which are sets of states that can be shown with the calculus to lead to certain behaviours of the transition system.

The transition system can be given as elements of a state-to-state relation $\mathcal{T}$: if $(s, s') \in \mathcal{T}$ then moving from state s to state s' is a possible transition; and if both (s, s') and (s, s'') are in $\mathcal{T}$, for $s' \neq s''$, then in a move from s the choice between s' and s'' can be resolved either 'demonically' or 'angelically' depending on one's application.

The μ-calculus can be specialised to a form of temporal logic by defining temporal operators within the calculus, like the eventually written $\Diamond$ above, and then using only those as a subset of the full language.

1.2 Probabilistic *transition systems and qMμ*

Probabilistic transition systems support a 'quantitative' modal μ-calculus $qM\mu$, whose expressions are real- rather than Boolean-valued over S; the expressions denote 'expected values' of random variables over probabilistic distributions on the state space. The transitions exhibit *probabilistic* nondeterminism as well as potentially demonic and angelic.

As in the standard μ-calculus, temporal operators can be defined within $qM\mu$: the result is a *quantitative* temporal logic which we have called qTL [2,3].

The standard μ-calculus embeds into $qM\mu$ by taking predicates, or their equivalent subsets, to the corresponding characteristic functions; and standard branching-time temporal logic embeds similarly into qTL.

For example, consider the probabilistic system of Fig. 1. If b holds and $n > 0$, then b is eventually *False* only with probability $1/n$ — that is, the eventuality $\Diamond[\neg b]$ depends on n's initial value — and in qTL (details below) we would simply say that $\Diamond[\neg b] = 1/n$ in all states that satisfy $b \wedge (n{>}0)$. Clearly the

[3] We use a UNITY-like [6] pseudo-code to describe the transitions.

// State space is $Bool \times \mathbb{N}$.

var $b\colon Bool;\ n\colon \mathbb{N}$;

// Transition is 'enabled' only when b holds; otherwise it acts as **skip**.

$b \quad \rightarrow \quad b{:=}\ False\ {}_{1/n^2}\!\oplus\ n{:=}\ n+1$

Fig. 1. A probabilistic transition system. [3]

$1/n$ result depends on the precise value $1/n^2$ given in the transition: that is, the proof of $\Diamond[\neg b] = 1/n$ in the calculus would involve quantitative reasoning based on that specific probability. (We give that proof in Sec. 3.2.)

Fig. 1 is a special case however of the probabilistic system

$$b \quad \rightarrow \quad b{:=}\ False\ {}_{p}\!\oplus\ n{:=}\ n+1\ , \tag{1}$$

one in which p is the function $1/n^2$ of the state. A different specialisation would make p abstract, in which case $\neg b$ is reached with probability 1 no matter what precise value(s) p may take. (Note that probability $1/n^2$ is not abstract, as it is not bounded away from 0.)

We say in that case that eventually $\neg b$ occurs *almost certainly* over the *abstract probability* p and, given that p's precise value is irrelevant for that conclusion, we could write the system (similarly to Rao's notation [7])

$$b \quad \rightarrow \quad b{:=}\ False \oplus n{:=}\ n+1\ , \tag{2}$$

with the additional implication however that the probability is abstract for both alternatives — that is, the implicit p indicated by $\oplus$ is bounded away from both 0 and 1.

In the sequel we show that in qTL, at least for finite state spaces, the truth of almost-certain eventualities depends only on abstract probabilities, never on their precise values; and we show how to specialise the calculus so that it can act directly over transition systems described as at (2).

A *standard* μ-calculus expression $\mathcal{E}$ is of the form

P	predicate over S, typed $S \to \mathit{Bool}$ or equivalently $\mathbb{P}S$
$\mathcal{E}$ **op** $\mathcal{E}$	for propositional operators **op**
$\circ\mathcal{E}$	'next-time' $\mathcal{E}$
$(\mu X.\mathcal{E}(X))$	least fixed-point of predicate transformer $\mathcal{E}(X)$
$(\nu X.\mathcal{E}(X))$	greatest fixed-point of predicate transformer $\mathcal{E}(X)$

Notes:

- For state s in S and predicate $\mathcal{E}$ we write $\mathcal{E}.s$ for the value of $\mathcal{E}$ at s, and we say that s *satisfies* $\mathcal{E}$, or $\mathcal{E}$ *holds at* s, whenever that value is *True*. When $\mathcal{E}$ is given explicitly as a subset S' of S, we can write $s \in S'$ for $S'.s$.
- In this paper we interpret the $\circ$ operator *demonically* with respect to the underlying transition system $\mathcal{T}$, so that s satisfies $\circ\mathcal{E}$ precisely when *for all* s' we have $(s, s') \in \mathcal{T} \Rightarrow \mathcal{E}.s'$.
- The next-time operator $\circ$ satisfies the *conjunctivity* property

$$\circ(P \wedge Q) \quad \equiv \quad \circ P \wedge \circ Q \ , \tag{3}$$

  for all predicates P, Q. Note that (3) implies $\Rightarrow$-monotonicity of $\circ$.
- Expressions $\mathcal{E}(X)$ are sometimes called *predicate transformers* (of X). We apply μ and ν only to transformers that are $\Rightarrow$-monotonic.

Fig. 2. The standard modal μ-calculus

2 Summary of the μ-calculi

In this section we give a brief description of both the standard [4] and quantitative [2,3] μ-calculi.

2.1 The standard calculus

Consider a transition system $\mathcal{T}: S \leftrightarrow S$ over a state space S. The standard modal μ-calculus comprises (expressions denoting) predicates of the form shown in Fig. 2, allowing propositional operators, least- and greatest fixed-points, and an implicit 'next-time' reference $\circ$ to the effect of taking one step in $\mathcal{T}$, with demonic resolution of any branching.

The transition system $\mathcal{T}$ is

$$s = a \quad \rightarrow \quad s{:=}\ c \ \Box\ s{:=}\ d \ \Box\ s{:=}\ e\ .$$

The state space S is $\{a, b, c, d, e, f\}$, and $\Box$ represents choice (interpreted demonically by $\circ$). For convenience we write the system using a programming-language like syntax, in which for example $s = a$ denotes the predicate $\{a\}$ and $s{:=}\ c$ denotes the single transition $S \times \{c\}$.
The overall system is thus the relation $\mathcal{T} := \{a\} \times \{c, d, e\}$.

Fig. 3. Example standard transition system

As an example, consider the transition system of Fig. 3. We have

$a \in \circ\{c, d, e\}$	one step from a is guaranteed to reach $\{c, d, e\}$.
$a \notin \circ\{c, d\}$	one step from a might go to e instead.
$a \notin \circ\{a\}$	one step from a cannot reach a at all.
$b \in \circ\{b\}$	"no explicit step" is interpreted as **skip**.

As an illustration of conjunctivity (3, Fig. 3) we have for example

$$\begin{array}{lll}
 & \circ(\{b, c, d, e\} \ \wedge\ \{c, d, e, f\}).a & \\
\equiv & \circ\{c, d, e\}.a & \text{propositional } \wedge \\
\equiv & \mathit{True} & a \in \circ\{c, d, e\} \text{ by inspection of } \mathcal{T} \\
\equiv & \mathit{True} \wedge \mathit{True} & \\
\equiv & \circ\{b, c, d, e\}.a \ \wedge\ \circ\{c, d, e, f\}.a\ . & \text{by inspection of } \mathcal{T}
\end{array}$$

2.2 The quantitative calculus qMμ

Consider a probabilistic transition system over a state space S, this time of the form $S \to \mathbb{P}\overline{S}$ in which initial states are taken to *sets* ($\mathbb{P}$) of *distributions* ($\bar{\cdot}$) over S.[4] (Discrete) distributions $\overline{S}$ over S are maps from S into the unit interval $[0, 1]$ of probabilities, and sum to 1 over the space.

The quantitative modal μ-calculus comprises $\mathbb{R}_{\geq}$-valued functions of the form shown in Fig. 4, called *expectations*, and by analogy with the standard case

[4] Note for comparison with the standard case that $S \leftrightarrow S$ is equivalently $S \to \mathbb{P}S$, so that we have merely changed the final 'set of points' S to the set of discrete distributions $\overline{S}$ (into which S can be embedded).

A *quantitative* μ-calculus expression $\mathcal{E}$ is of the form

A	expectation over S, typed $S \to \mathbb{R}_{\geq}$
$\mathcal{E}$ **op** $\mathcal{E}$	for $\mathbb{R}_{\geq}$-closed operators **op** (extended pointwise)
$\circ\mathcal{E}$	'next-time' $\mathcal{E}$
$(\mu X.\mathcal{E}(X))$	least fixed-point of expectation transformer $\mathcal{E}(X)$
$(\nu X.\mathcal{E}(X))$	greatest fixed-point of expectation transformer $\mathcal{E}(X)$

Notes:

- For state s in S we write $\mathcal{E}.s$ for the value of $\mathcal{E}$ at s. For predicate P we write $[P]$ for its characteristic function, which embeds it into the quantitative model: thus $[P].s = 1$ iff $s \in P$.
- The $\circ$ operator is interpreted over $\mathcal{T}$, and we assume here that it is demonic and *probabilistic* so that expression $\circ\mathcal{E}$ is the least (over the demonic nondeterminism) expected value (over the probabilistic nondeterminism) of $\mathcal{E}$ after the computational step. That is $\circ\mathcal{E}.s$ is the minimum over all distributions D with $(s, D) \in \mathcal{T}$ of the expected value $\mathrm{Exp}_D\mathcal{E}$ of $\mathcal{E}$ over distribution D.
- Note that the special case $\circ[P].s$ gives the (demonically least) probability that one step from s will reach a state satisfying P, since the probability assigned an event P by a (state) distribution is equal to the expected value of its characteristic function $[P]$ over that same distribution: thus $\mathrm{Exp}_D[P] = \mathrm{Prob}_D P$.
- We write $\Rrightarrow$ for "is everywhere no more than", and $\Lleftarrow, \equiv$ similarly.
- Operator $\circ$ is satisfies the new property of *sublinearity* [8], that is

$$\circ(aA + bB \ominus c) \quad \Lleftarrow \quad a(\circ A) + b(\circ B) \ominus c \tag{4}$$

  where $a, b, c \geq 0$ are scalars, juxtaposition is multiplication and A, B are expectations; *truncated subtraction* $\ominus$ is defined

$$x \ominus y \quad := \quad (x - y) \sqcup 0$$

  with lower syntactic precedence than $+$.

  Note that (4) implies $\Rrightarrow$-monotonicity of $\circ$.
- We write c both for the scalar and for the constant 'everywhere-c' function.

Fig. 4. The quantitative modal μ-calculus

---

we allow arithmetic operators, least- and greatest fixed-points, and an implicit reference $\circ$ to (the now demonic/probabilistic) $\mathcal{T}$.

As an example, consider the transition system of Fig. 5. We have

$$s = a \quad \rightarrow \quad s{:=}\ c \ {}_{2/3}\!\oplus\ (s{:=}\ d \,\Box\, s{:=}\ e)$$

The state space S is again $\{a, b, c, d, e, f\}$, and ${}_p\!\oplus$ represents probabilistic choice taking the left (resp. right) operand with probability p (resp. $1{-}p$).
The transition system here is

$$\{ \quad (a,\ \langle 0, 0, 2/3, 1/3, 0, 0\rangle),$$
$$\quad (a,\ \langle 0, 0, 2/3, 0, 1/3, 0\rangle)$$
$$\} \ ,$$

where $\langle \cdots \rangle$ lists the component probabilities of a discrete distribution over the space $a \cdots f$.

Fig. 5. Example probabilistic and demonic transition system

$\circ\{c, d, e\}.a = 1$	one step from a is guaranteed to reach $\{c, d, e\}$.
$\circ\{c, d\}.a = 2/3$	when the probabilistic choice resolves to the right, the demonic choice will avoid d.
$\circ\{a\}.a = 0$	one step from a cannot reach a at all.
$\circ\{b\}.b = 1$	no explicit step is interpreted as **skip**.

(To avoid the clutter of $[\{c, d, e\}]$ for example, we have omitted the embedding brackets $[\cdot]$ (see notes of Fig. 4) when they occur around set comprehensions.)

For an illustration of sublinearity (4, Fig. 4), consider the special case in which its scalars a, b, c are all 1. We define $x \,\&\, y := x + y \ominus 1$, and note that sublinearity then gives us *&-subdistribution through* $\circ$: for all expectations A, B we have

$$\circ(A \,\&\, B) \quad \Leftarrow \quad \circ A \,\&\, \circ B \ . \tag{5}$$

Operator & is useful because it both generalises Boolean conjunction [5] and, specialising sublinearity, satisfies a (sub-) distribution law (5). It is our 'best quantitative approximation' to conjunctivity (3), in the sense of being the only operator of which we are aware with both those properties.

In the system of Fig. 4, because we have for example that $\{c\} \equiv \{c, d\} \,\&\, \{c, e\}$, we can illustrate (5) by verifying that

$$\circ\{c\}.a$$

[5] That is, we have $[P] \wedge [Q] \equiv [P] \,\&\, [Q]$ for all predicates P, Q.

$$
\begin{array}{lll}
\equiv & 2/3 & \text{inspection of } \mathcal{T} \\
\Leftarrow & 1/3 & \\
\equiv & 2/3 \,\&\, 2/3 & \text{definition of } \& \\
\equiv & \circ\{c,d\}.a \;\&\; \circ\{c,e\}.a\ . & \text{inspection of } \mathcal{T}
\end{array}
$$

Note that we have only an inequality,[6] whereas in the standard case (conjunctivity) we have equality.

Consequences of sublinearity include (by simple arithmetic [8, Sec. 7 pp. 340ff]) the following properties for all expectations A, B, where we write $\sqcap$ for infimum and $\sqcup$ for supremum:

monotonicity — If $A \Rrightarrow B$ then $\circ A \Rrightarrow \circ B$.
feasibility — $\circ A \Rrightarrow \sqcup A$, where the right-hand side abbreviates the supremum $(\sqcup s{:}\, S \cdot A.s)$.
scaling — For $c \geq 0$ we have $\circ(cA) \equiv c(\circ A)$.
bounded up-continuity — Provided S is finite, the set of expectations $\mathcal{A}$ is up-directed and $\sqcup\mathcal{A}$ is bounded above, we have

$$\circ(\sqcup\mathcal{A}) \quad \equiv \quad (\sqcup A{:}\, \mathcal{A} \cdot \circ A)\ .$$

down-continuity — Provided S is finite and the set of expectations $\mathcal{A}$ is down-directed, we have

$$\circ(\sqcap\mathcal{A}) \quad \equiv \quad (\sqcap A{:}\, \mathcal{A} \cdot \circ A)\ .$$

3 Specialisations to the temporal calculi

The modal calculi act as *temporal* calculi if one identifies specific types of expression for concepts like (among others) 'eventually', 'always' and 'unless' [9]. When based on the standard calculus, they give absolute (*i.e.*, true or false) judgements; in the quantitative case, the judgements are probabilistic.

[6] The inequality is because $\circ\{c,d\}.a \equiv \circ\{c,e\}.a \equiv 2/3$ is true of other transition systems over S as well; one of those is for example

$$s = a \quad \rightarrow \quad s{:=}\ c \,{}_{1/3}\!\oplus (s{:=}\ d \,{}_{1/2}\!\oplus s{:=}\ e)\ ,$$

for which $\circ\{c\}.a$ is in fact as low as $1/3$. It can be shown that sublinearity gives the highest estimate possible under those general circumstances: it is only just as "pessimistic" as necessary.

"eventually P"

$\Diamond P$	$:=$	$(\mu X \cdot P \vee \circ X)$	If sufficiently many steps are taken, then P will hold.

"always P"

$\Box P$	$:=$	$(\nu X \cdot P \wedge \circ X)$	No matter how many steps are taken P will continue to hold.

"P unless Q"

$P \rhd Q$	$:=$	$(\nu X \cdot Q \vee (P \wedge \circ X))$	No matter how many steps are taken P will continue to hold, unless a state is reached in which Q holds.

We write ":=" for "is defined to be".

Fig. 6. Definition of some standard temporal operators in the modal μ-calculus

3.1 Standard temporal logic

We define some typical temporal operators in Fig. 6. The role of conjunctivity (3) here is that it allows high-level proofs of temporal properties *without* referring directly to the underlying transition system. For example, one such property is the *eventually-until lemma* [7]

$$P \rhd (P \wedge Q) \quad \wedge \quad \Diamond Q \quad \Rrightarrow \quad \Diamond(P \wedge Q)\ , \tag{6}$$

which states that if P holds up to *and including* a possible step at which Q holds, and Q eventually does hold, then in fact $P \wedge Q$ eventually holds. [8] In the appendix we give the straightforward proof of that as an example of the use of conjunctivity (Lem. 16).

[7] Compare the *PSP* lemma of UNITY [6].

[8] For uniformity within this paper we use $\Rrightarrow$ for 'entails' even in the standard context, which is consistent with its quantitative definition since $P \vdash Q$ iff $[P] \Rrightarrow [Q]$.

"eventually A"	$\Diamond A$	$:=$	$(\mu X \cdot A \sqcup \circ X)$
"always A"	$\Box A$	$:=$	$(\nu X \cdot A \sqcap \circ X)$
"A unless B"	$A \rhd B$	$:=$	$(\nu X \cdot B \sqcup (A \sqcap \circ X))$

In qTL we restrict expectations to the range $[0,1]$ instead of $\mathbb{R}_{\geq}$.

Fig. 7. Definition of the quantitative temporal operators for qTL in the quantitative modal μ-calculus

3.2 Quantitative temporal logic qTL

From here on we restrict our expectations to the range $[0,1]$ rather than $\mathbb{R}_{\geq}$, using only operators for which $[0,1]$ is closed. (Note that feasibility above gives the closure of $\circ$ itself.) We define the quantitative temporal operators in Fig. 7.

The operational interpretation of the quantitative operators can require some ingenuity. Consider "$\Diamond A$": clearly it generalises the standard $\Diamond[P]$, but for general expectation A it is not helpful to interpret it as "the probability that eventually A is established", because "establish A" conveys little if A is not a characteristic function. So what does $\Diamond A$ mean? (Similar remarks apply to the other temporal operators.)

Fortunately, it is true that in the special case $\Diamond[P]$, the expression is indeed the probability of eventually establishing P.[9] More generally [2] the interpretation of $\Diamond A$ relies on a game-like analogy: it is

> the supremum, over all strategies that determine in each state whether to make another transition or to stop, of the expected value of A when the strategy says "stop"; the strategy "never stop" gives 0 by definition.[10]

The situation with the other operators is similar.

Again (the generalisation of) conjunctivity plays an important role in high-level reasoning. Using &-subdistribution, for example, we can prove a gener-

[9] As is usual, we mean by that probability the measure, in the Borel algebra of 'cones' within the tree of possible executions, of the set of paths along which P eventually occurs.

[10] We have agreement with the standard case $\Diamond[P]$, since if P is guaranteed to hold eventually then the strategy "stop when P holds" will achieve that supremum *True*.

alisation of (6); it is the quantitative eventually-until lemma

$$A \rhd (A \,\&\, B) \quad \& \quad \Diamond B \quad \Rrightarrow \quad \Diamond(A \,\&\, B)\ , \tag{7}$$

which we prove (Appendix) as Lem. 17.

As an example of probabilistic eventualities, we return to the system of Fig. 1. We write out expectations as expressions over the program variables b, n, and calculate $\Diamond[\neg b]$ directly (and unimaginatively) from the least-fixed-point limit implied by its definition (Fig. 7).

term 0: 0 $\qquad\qquad \bot \equiv 0$

term 1: $[\neg b] \ \sqcup \ \circ 0$ $\qquad$ definition $\Diamond$: term $k{+}1 = [\neg b] \sqcup \circ(\text{term } k)$

$\equiv$ $\quad [\neg b]$ $\qquad\qquad \circ 0 \equiv 0$ by feasibility

term 2: $[\neg b] \ \sqcup \ \circ[\neg b]$

$\equiv$ $\quad [\neg b] \sqcup ([\neg b] \ \sqcup \ [b]/n^2)$ $\qquad$ inspection of $\mathcal{T}$

$\equiv$ $\quad [\neg b] \ \sqcup \ [b]/n^2$

term 3: $[\neg b] \ \sqcup \ \circ([\neg b] \ \sqcup \ [b]/n^2)$

$\equiv$ $\quad [\neg b] \ \sqcup \ [b](1/n^2 + (1 - 1/n^2)(1/(n+1)^2))$

$\equiv$ $\quad [\neg b] \ \sqcup \ 2[b]/n(n+1)$

term 4: $[\neg b] \ \sqcup \ \circ([\neg b] \ \sqcup \ 2[b]/n(n+1))$

$\equiv$ $\quad [\neg b] \ \sqcup \ 3[b]/n(n+2)$

$\vdots$

term k: $[\neg b] \ \sqcup \ (k-1)[b]/n(n+k-2)\ ,$ $\qquad$ induction

so that we have

$\Diamond[\neg b]$

$\equiv$ $\qquad$ terms ascending, so $\sqcup_k$ agrees with $\lim_{k\to\infty}$

$\lim_{k\to\infty} \quad [\neg b] \ \sqcup \ (k-1)[b]/n(n+k-2)$

$\equiv$ $\quad [\neg b] \ \sqcup \ [b]/n$ $\qquad\qquad \lim_{k\to\infty} \ (k-1)/(n+k-2) = 1$

$\equiv$ $\quad 1/n$ **if** b **else** 1 . $\qquad$ arithmetic

That is, termination is certain if $\neg b$ holds (at the start), and occurs with probability $1/n$ if it does not.

4 Abstract reasoning in *qTL*

We have now completed our review of the existing calculi, and turn to our present contribution.

At the end of Sec. 3, we gave a calculation of $\circ[\neg b]$ for the system of Fig. 1. Consider the more general System (1) following it, but restrict $p > 0$ to be a constant. Then we have [11]

term 0: 0 $\qquad\qquad \bot \equiv 0$

term 1: $[\neg b] \sqcup \circ 0$ $\qquad\qquad$ term $k{+}1 = [\neg b] \sqcup \circ(\text{term } k)$

$\equiv \quad [\neg b]$

term 2: $[\neg b] \sqcup \circ[\neg b]$

$\equiv \quad [\neg b] \sqcup p[b]$

term 3: $[\neg b] \sqcup \circ([\neg b] \sqcup p[b])$

$\equiv \quad [\neg b] \sqcup p[b](1 + (1{-}p))$ $\qquad\qquad$ p does not depend on n

term 4: $[\neg b] \sqcup \circ([\neg b] \sqcup p[b](1 + (1{-}p)))$

$\equiv \quad [\neg b] \sqcup p[b](1 + (1{-}p) + (1{-}p)^2)$

$\vdots$

term ∞: $[\neg b] \sqcup p \sum_{k=0}^{\infty} (1{-}p)^k \; [b]$, $\qquad\qquad$ induction

whence we conclude that $\Diamond[\neg b] \equiv [\neg b] \sqcup p(1/p)[b] \equiv 1$ because p is not 0.

[11] This heavy-handed 'limit' approach is not the only way to calculate $\Diamond[\neg b]$ here: an alternative is to show from the definitions that

$$\Diamond[\neg b] \quad \equiv \quad p \; + \; (1{-}p)\Diamond[\neg b]$$

holds for this system, whence rearrangement and dividing by p gives us $\Diamond[\neg b] \equiv 1$. But the point about explicit treatment of p remains.

We aim to show that in abstract systems like (1) it is possible to avoid explicit numeric calculations like the above.

The main technical result will be that the *floor* $\lfloor\cdot\rfloor$ and *ceiling* $\lceil\cdot\rceil$ operators can abstract from the 'intermediate' values lying strictly between 0 and 1: in finite state spaces we prove

$$\lfloor\, \Diamond[P] \,\rfloor \quad \equiv \quad \lfloor\, \lceil \Diamond[P] \rceil \rhd [P] \,\rfloor\,,$$

whose left-hand side is 1 if $\Diamond[P]$ is almost certain, and 0 otherwise; and the constructions $\lfloor\cdot \rhd \cdot\rfloor$ and $\lceil\Diamond\cdot\rceil$ used in the right-hand side will be shown to depend only on abstract probabilities.

We begin with a general discussion.

4.1 'Almost-certain' is special for probabilistic systems

We place our work in context by recalling the following facts from finite-state Markov process theory, but in our notation. Let S be the finite state space.

- Operator $\circ$ is a transition function over S. If we write state predicates P as $\{0,1\}$-valued column vectors of height $\#S$, then $\circ$ (if it contains no nondeterministic choice) can be seen as a Markov matrix, and $\circ[P]$ is post-multiplication of $\circ$ by the column vector representing P: each element $\circ[P].s$ of the product $\circ[P]$ gives the probability of reaching P from s.

  More generally, for expectation A as a column vector we have $\circ A$ as post-multiplication, and each element $\circ A.s$ of the product gives the expected final value of A when taking a transition from s.
- State s' is reachable from state s iff $\circ^n\{s'\}.s > 0$ for some finite n (the number of transitions taken).
- A subset P of S is closed (with respect to $\circ$) iff $[P] \Rrightarrow \circ[P]$.
- The probability of reaching P in one step from s — call it $\circ_1.P.s$ — is $\circ[P].s$.
- The probability of reaching P for the first time at the n^{th} step, for $n > 1$, is $\circ_n.P := \circ([\neg P] \sqcap \circ_{n-1}.P)$.
- The probability of eventually reaching a subset P from state s, say $\circ_\infty.P.s$, is

  $$\sum_{n>0} \circ_n.P.s\ ,$$

  which is also known as *the first-passage probability from s to P*.
- $\circ_\infty.\{s\}.s$ is the probability of eventual return to s.

In that notation we can state the following theorem for Markov processes:

> Let $\circ$ represent a Markov matrix, let S be a finite state space and s a state; and let C be the set of reachable states from s. Then
> $\circ_\infty.\{s\}.s = 1$ iff $p[C] \Rrightarrow \circ_\infty.\{s\}$ for some $p > 0$. [12]
> That is, eventual return to s is almost certain if it is non-zero at every state reachable from s.

The important thing to note about the result is that p is specified only to be greater than 0. Equivalently, only the connectivity of the Markov process is important, rather than the actual values of the probabilities — which is why that proof rule for $\circ_\infty.\{s\}.s$ is so simple.

We regard the result as a form of completeness, because it states that the connectivity information is always sufficient to establish the eventuality.

Our aim is to demonstrate that for probabilistic and demonic programs, a simpler calculus is all that is needed to prove (eventuality) properties with probability 1: as for standard programs only the "connectivity" of the program is important and not the actual probabilistic values. For many probabilistic programs, that will provide a sufficient proof rule, since probability 1 (or not) is all that is of interest.

Other recent work on the special properties of "probability 1" events in programs includes results of Rao [7], Pnueli/Zuck [10] and Hart/Sharir/Pnueli [11]. Their completeness results in some cases assume various kinds of fairness.

4.2 Relevant properties of our temporal operators

We concentrate on next-time $\circ$, eventually $\diamond$ and unless $\triangleright$. The following properties can be proved directly from the operators' definitions [3] or — in some cases — have been given above.

Lemma 1 Properties of next-time — *For all expectations* A, B,

(1) $\circ A \,\&\, \circ B \Rrightarrow \circ(A \,\&\, B)$.
(2) If $A \Rrightarrow A'$, *then* $\circ A \Rrightarrow \circ A'$.
(3) $\circ 1 \equiv 1$.

[12] Note that $p[C].s'$ is just (p **if** $s' \in C$ **else** 0), so that — after applying both sides to s' — the inequality $p[C] \Rrightarrow \circ_\infty.\{s\}$ says that for all $s' \in C$ the first-passage probability $\circ_\infty.\{s\}.s'$ from s' to s is at least p.

Lemma 2 Properties of eventually — *For all expectations A, B,*

(1) $A \Rrightarrow \Diamond A$.[13]
(2) $\circ\Diamond A \Rrightarrow \Diamond A$.
(3) If $B \sqcup \circ A \;\Rrightarrow\; A$, *then* $\Diamond B \Rrightarrow A$.
(4) If $A \Rrightarrow A'$, *then* $\Diamond A \Rrightarrow \Diamond A'$.

Lemma 3 Properties of unless — *For all expectations A, B,*

(1) $B \;\Rrightarrow\; A \rhd B \;\Rrightarrow\; A \sqcup B$.
(2) If $C \;\Rrightarrow\; B \sqcup (A \sqcap \circ C)$, *then* $C \Rrightarrow A \rhd B$.
(3) $A \rhd B \equiv B \sqcup (A \sqcap \circ(A \rhd B))$.
(4) If $A \Rrightarrow A'$ *and* $B \Rrightarrow B'$, *then* $A \rhd B \;\Rrightarrow\; A' \rhd B'$.

From these we have a form of completeness, based on the fact that the above properties determine the action of their respective operators.

Theorem 4 Standard completeness — *If $\circ, P, Q$ are interpreted over a finite state (standard) transition system, then the above properties are sufficient to calculate $\Diamond[P]$ and $[P] \rhd [Q]$ — only the transitions must be specified.*

Although for probabilistic programs the same idea of finding the least solution to an equation remains valid (and is in that sense complete[14]), even for finite-state programs discovering the actual real number values can still be rather tortuous, as we saw above. Indeed that is always going to be the case for non-(0-1) properties.

We seek a completeness property like Thm. 4 for abstract probabilistic programs — the idea is that if we only specify the transitions, merely indicating when they are probabilistic, then we only need use standard techniques, without having to introduce all the complications of the full quantitative calculus. It will turn out that merely replacing all probabilistic transitions by angelic, or by demonic choice will not do (see example in Sec. 8); rather, they must act angelically at some times, and demonically at others (see example at (16)).

Our first task is to show how to extract information "with probability 1".

From this point we assume that the transition system is probabilistic, and that the state space is finite. Recall our restriction in qTL to expectations that take values only in the unit interval $[0, 1]$ rather than in the more general range $\mathbb{R}_{\geq}$.

[13] Note how this follows from our intuitive 'strategic' explanation earlier of $\Diamond A$: since the simple strategy "stop right now" is guaranteed to return at least A, the value of $\Diamond A$ can never be less than that.
[14] ... provided we replace Lem. 1 Property (1) with full sublinearity.

4.3 Floor and ceiling for 'almost certain'

Our principal tool will be the ceiling $\lceil\cdot\rceil$ and floor $\lfloor\cdot\rfloor$ operators (both taking expectations to expectations), defined

$$\begin{array}{ll} \textbf{ceiling } \lceil A\rceil.s \;:=\; \lceil A.s\rceil, & \text{or equivalently } [A.s \neq 0] \\ \textbf{floor } \lfloor A\rfloor.s \;:=\; \lfloor A.s\rfloor, & \text{or equivalently } [A.s = 1] \end{array}$$

With them we can write "almost certainly $\Diamond[P]$" as $\lfloor\Diamond[P]\rfloor$, and our aim is to calculate that from the 'connectivity' alone — only the *abstract* probabilistic properties — of $\circ$.

4.4 Floor and ceiling for the 'connectivity' of $\circ$

We also use ceiling and floor to extract the connectivity (rather than the particular values of) the probabilistic transitions . With them we define two 'derived' transition operators, one converting probabilities to angelic choice, and the other converting them to demonic.

Definition 5 *The* angelic *and* demonic *projections of* $\circ$ *are defined*

$$\begin{array}{ll} \textbf{\textit{angelic projection}}\ \circ_a A \;:=\; \lceil\circ A\rceil \\ \textbf{\textit{demonic projection}}\ \circ_d A \;:=\; \lfloor\circ A\rfloor \end{array}$$

For example, if $\circ[P].s > 0$ then there is a non-zero probabilistic transition from s into P, which revealed by the fact $\circ_a[P].s = 1$. That means for example that

$$(s{:=}\ H \oplus s{:=}\ T)_a \quad = \quad (s{:=}\ H \sqcup s{:=}\ T)\ ,$$

where we are abusing notation to compare $\circ_a$ for the transition system on the left with $\circ$ for the system on the right. The operator $\sqcup$ is angelic choice.

On the other hand $\circ_d[P].s = 1$ iff all the transitions from s (whether probabilistic or not) end up in P, so that we have

$$(s{:=}\ H \oplus s{:=}\ T)_d \quad = \quad (s{:=}\ H \sqcap s{:=}\ T)\ .$$

Clearly $\circ_a$ and $\circ_d$ depend only on the connectivity, since they discard all numeric information; but it is not difficult to show that in fact they determine the connectivity. [15]

[15] For a purely probabilistic or purely demonic system, either $\circ_a$ or $\circ_d$ would be sufficient on its own to determine connectivity; only for a mixture of the two forms

4.5 Properties of $\circ_a$ and $\circ_d$

Before proceeding to almost-eventually properties, we need the following technical results for our connectivity operators.

Lemma 6 Some properties of $\circ_d$ — *Projection $\circ_d$ in effect replaces probabilistic by demonic choice: it is conjunctive over predicates and monotonic in general:*

conjunctive $\circ_d([P] \,\&\, [Q]) \quad \equiv \quad \circ_d[P] \,\&\, \circ_d[Q]$.
monotonic *If* $A \Rrightarrow A'$ *then* $\circ_d A \Rrightarrow \circ_d A'$.

Lemma 7 Some properties of $\circ_a$ — *Projection $\circ_a$ in effect replaces probabilistic by angelic choice, which is monotonic:*

monotonic *If* $A \Rrightarrow A'$ *then* $\circ_a A \Rrightarrow \circ_a A'$.

4.6 Almost-certainly is related to connectivity

We can now show that some almost-certainly properties — though not yet the one we want — depend only on the connectivity of $\circ$, as captured by $\circ_a$ and $\circ_d$.

Lemma 8 *Both $\lfloor A \rhd B \rfloor$ and $\lceil \Diamond A \rceil$ can be calculated from the connectivity $\circ_a$, $\circ_d$ of $\circ$, and do not depend on the actual values of the probabilistic transitions.*

Proof *$A \rhd B$ is a greatest fixed-point, and so the result follows from Lem. 20 (Appendix) once we notice from Lem. 18 that*

$$\lfloor B \sqcup (A \sqcap \circ X) \rfloor \quad \equiv \quad \lfloor B \rfloor \sqcup (\lfloor A \rfloor \sqcap \circ_d \lfloor X \rfloor) \ .$$

We treat $\Diamond A$ similarly (Lem. 19 and Lem. 21).[16] □

Unfortunately however, our aim is to calculate $\lfloor \Diamond A \rfloor$ (not $\lceil \Diamond A \rceil$), and indeed $\lfloor \cdot \rfloor$ does not distribute through *least* fixed-points. For consider $\circ$ over the system

$$s{:=}\ H \quad {}_{1/2}\!\oplus \quad s{:=}\ T \ ,$$

of choice does one need both operators.

[16] With the obvious definitions we could write just

$$\lfloor A \rhd B \rfloor \ \equiv \ \lfloor A \rfloor \rhd_d \lfloor B \rfloor \quad \text{and} \quad \lceil \Diamond A \rceil \ \equiv \ \Diamond_a \lceil A \rceil \ .$$

and compare $\lfloor \Diamond \{H\} \rfloor \equiv 1$ and $(\mu X \cdot \lfloor \{H\} \rfloor \sqcup \circ_d X) \equiv \{H\}$.

It will turn out that we can reach $\lfloor \Diamond A \rfloor$ indirectly, via $\lfloor \Diamond \cdot \rfloor$ of a more involved expression, at least when A is standard (see (10) in Thm. 14); for that we begin with the following lemma:

Lemma 9 *For all expectations A and transition systems $\circ$ we have*

$$\Diamond A \quad \Rrightarrow \quad \lceil \Diamond A \rceil \rhd A \ .$$

Proof *We show that $A \sqcup \circ(\lceil \Diamond A \rceil \rhd A) \Rrightarrow \lceil \Diamond A \rceil \rhd A$, which allows us to apply Property (3) of Lem. 2:*

$$\begin{array}{lll}
 & A \sqcup \circ(\lceil \Diamond A \rceil \rhd A) \quad \Rrightarrow \quad \lceil \Diamond A \rceil \rhd A & \\
\textit{iff} & A \sqcup \circ(\lceil \Diamond A \rceil \rhd A) \quad \Rrightarrow \quad A \sqcup (\lceil \Diamond A \rceil \sqcap \circ(\lceil \Diamond A \rceil \rhd A)) & \textit{definition } \rhd \\
\textit{iff} & \circ(\lceil \Diamond A \rceil \rhd A) \quad \Rrightarrow \quad \lceil \Diamond A \rceil & \textit{arithmetic; } A \Rrightarrow \lceil \Diamond A \rceil \textit{ (Lem. 2)} \\
\textit{iff} & \circ(\lceil \Diamond A \rceil \rhd A) \quad \Rrightarrow \quad \lceil A \rceil \sqcup \lceil \circ \Diamond A \rceil & \textit{definition } \Diamond A\textit{; arithmetic}
\end{array}$$

if $\lceil \Diamond A \rceil \rhd A \Rrightarrow \lceil \Diamond A \rceil \sqcup A \Rrightarrow \lceil \Diamond A \rceil$ *(Lemmas 2, 3); monotonicity* $\circ$

$$\circ \lceil \Diamond A \rceil \quad \Rrightarrow \quad \lceil \circ \Diamond A \rceil \ ,$$

which is a consequence of Lem. 19.

□

Lem. 9 gives us trivially a connectivity-calculable upper bound on $\lfloor \Diamond A \rfloor$: it is

Lemma 10 Upper bound for almost-certain eventuality

$$\lfloor \Diamond A \rfloor \quad \Rrightarrow \quad \lfloor \lceil \Diamond A \rceil \rhd A \rfloor \ .$$

Proof *Lem. 9 and the monotonicity of $\lfloor \cdot \rfloor$.* □

The right hand side is calculable from the connectivity of $\circ$, because by Lem. 8 we know that $\lceil \Diamond A \rceil$ is so calculable, and by Lem. 8 (again) so is $\lfloor \lceil \Diamond A \rceil \rhd A \rfloor$.

In the next section we show that we achieve equality when A is standard.

5 0-1 laws and temporal logic

In this section we show how the introduction of a 0-1 law (or axiom) is all that is needed to show that $\lfloor \Diamond[P] \rfloor$ does indeed rely only on connectivity.[17] We gave an example of the 0-1 law for purely probabilistic programs; the idea has been extended to probabilistic/demonic programs [12,13] using the notation and ideas of temporal logic.

Lemma 11 0-1 Law — *For any expectation A, predicate P and probability $p > 0$, if $p(A \rhd [P]) \Rrightarrow \Diamond[P]$ then in fact $A \rhd [P] \Rrightarrow \Diamond[P]$.*

Proof *The full proof — allowing demonic nondeterminism and possibly-aborting transitions — is beyond the scope of this paper; but it is a simple consequence of 0-1 results on the probabilistic treatment of loops [13, Lem. 6.1 p10], obtained (partly) by reasoning over the model.*

As an illustration, however, we give a proof entirely in qTL (Thm. 22 in the appendix) for the restricted case of non-demonic and terminating transitions. □

The above law is valid for all state spaces: but for finite state spaces it has a much more compact formulation.

Lemma 12 0-1 Law (finite state spaces) — *In finite state models, Lem. 11 is equivalent to*

$$\lceil \Diamond[P] \rceil \rhd [P] \quad \Rrightarrow \quad \Diamond[P] \ . \tag{8}$$

Proof *Suppose the interpretation of $\circ$ is over a finite state space.*[18] *That means that Lem. 11 is equivalent to the following, in which we have eliminated the abstract p by introducing $\lceil \cdot \rceil$:*[19]

$$\textit{if } A \rhd [P] \Rrightarrow \lceil \Diamond[P] \rceil \quad \textit{then} \quad A \rhd [P] \Rrightarrow \Diamond[P] \tag{9}$$

[17] It is only now that we must make some restrictions to predicates, rather than general expectations, which is why we write $[P]$ rather than A.

[18] To see that (9) does not hold for infinite state spaces, consider this system over $S := \mathbb{Z}$ that defines a random walker on the integers:

$$s := s + 1 \quad {}_{2/3}\oplus \quad s := s - 1 \ .$$

Observe that $\lceil \Diamond[s \leq 0] \rceil \equiv 1 \equiv [s > 0] \rhd [s \leq 0]$, but that $\Diamond[s \leq 0]$ is not equal to 1.

[19] We are relying on the fact that, for finite state spaces, "$pX \Rrightarrow Y$ for some $0 < p$" and "$X \Rrightarrow \lceil Y \rceil$" are equivalent: take p to be $(\sqcap s{:}\, S \mid X.s \neq 0 \cdot Y.s/X.s)$, which infimum cannot be 0 because S is finite.

We now show that (8) holds iff (9) holds.

(8) implies (9) *Suppose that $A \rhd [P] \Rrightarrow \lceil \Diamond [P] \rceil$. It follows from Lem. 3 (2) that $A \rhd [P] \Rrightarrow \lceil \Diamond [P] \rceil \rhd [P]$, because*

$$
\begin{array}{lll}
 & [P] \sqcup (\lceil \Diamond [P] \rceil \sqcap \circ (A \rhd [P]) & \\
\Leftarrow & [P] \sqcup (A \rhd [P] \sqcap \circ (A \rhd [P]) & \textit{assumption} \\
\equiv & A \rhd [P] \ , & \textit{by cases on P.s}
\end{array}
$$

whence our assumption (8) gives us $A \rhd [P] \Rrightarrow \Diamond [P]$, as desired overall.

(9) implies (8) *From Lems. 3(1) and 2(1) we have*

$$\lceil \Diamond [P] \rceil \rhd [P] \quad \Rrightarrow \quad \lceil \Diamond [P] \rceil \sqcup [P] \quad \equiv \quad \lceil \Diamond [P] \rceil \ ,$$

hence we have immediately from (9) that

$$\lceil \Diamond [P] \rceil \rhd [P] \quad \Rrightarrow \quad \Diamond [P] \ .$$

□

Corollary 13 *For finite models, $\Diamond [P] \equiv \lceil \Diamond [P] \rceil \rhd [P]$.*

Proof *In finite models we may use the second form Lem. 12 of the 0-1 law; the result then follows from Lemma 9.* □

Cor. 13 is the key to showing that for probability-1 properties, connectivity is sufficient.

Theorem 14 Completeness for probability-1 eventualities — *If $\circ$ is interpreted over a finite-state probabilistic system, and P is a state predicate, then $\lfloor \Diamond [P] \rfloor$ is determined by $\circ_a$ and $\circ_d$, the probabilistic/demonic connectivity of $\circ$.*

Proof *Cor. 13 gives us that $\Diamond [P] \equiv \lceil \Diamond [P] \rceil \rhd [P]$, from which we have*

$$\lfloor \Diamond [P] \rfloor \quad \equiv \quad \lfloor \lceil \Diamond [P] \rceil \rhd [P] \rfloor \ . \tag{10}$$

Since $\lfloor \cdot \rhd \cdot \rfloor$ and $\lceil \Diamond \cdot \rceil$ depend only on the connectivity, the result follows. □

6 Example

Consider again the abstract system

$$s{:=}\ H \quad \oplus \quad s{:=}\ T\ .$$

The probabilistic connectivity is given by

angelic $\circ_a[P] \equiv [P \not\equiv \{\}]$, because there is a non-zero probability of establishing any non-empty predicate over $\{H, T\}$.
demonic $\circ_d[P] \equiv [P \equiv \{H, T\}]$, because there is a non-zero probability of avoiding any non-total predicate over $\{H, T\}$.

Now we look at the almost-certain eventuality $\lfloor \Diamond\{H\} \rfloor$; we have

$$\begin{array}{lll}
 & \lfloor \Diamond\{H\} \rfloor & \\
\equiv & \lfloor \lceil \Diamond\{H\} \rceil \rhd \{H\} \rfloor & \text{Cor. 13} \\
\equiv & \lfloor \circ_a\{H\} \rhd \{H\} \rfloor & \text{Lem. 8} \\
\equiv & \lfloor 1 \rhd \{H\} \rfloor & \text{inspection: choice } \oplus \text{ is abstract} \\
\equiv & 1\ . & \text{Lems. 3(2), 1(3)}
\end{array}$$

7 Complexity analysis

We now look at the time-complexity of evaluating almost-certainties in qTL: the precise language and its interpretation is set out in Fig. 8; and our result is that the complexity of evaluating $\lfloor \Phi \rfloor$ over transition system $\mathcal{T}$ is linear in the number of temporal operators in Φ and in the number of transitions in $\mathcal{T}$. We outline a proof of that in this section.

Throughout the following we will use the specific formula Φ_0, defined

$$\Diamond(A \sqcup (B \rhd \Box C))\ ,$$

as a running example: we want to evaluate $\lfloor \Phi_0 \rfloor$.

A *qTL* formula Φ is of the form

A	explicitly given numeric function over S, typed $S \to [0,1]$
$\Phi \sqcap \Phi$	minimum, generalising $\wedge$
$\Phi \sqcup \Phi$	maximum, generalising $\vee$
$\circ\Phi$	next-time
$\Diamond\Phi$	eventually
$\Box\Phi$	always
$\Phi \rhd \Phi$	unless ,

and the interpretation of the formula is via the quantitative μ-calculus, as given earlier in Fig. 7. The formula is said to be *almost certain* at a state s of a given transition system if it evaluates to 1 at s.

Fig. 8. Quantitative temporal logic formulae and interpretation

---

"angelic-eventually A"	$\Diamond_a A$	$:=$	$(\mu X \cdot A \sqcup \circ_a X)$
"demonic-always A"	$\Box_d A$	$:=$	$(\nu X \cdot A \sqcap \circ_d X)$
"A demonic-unless B"	$A \rhd_d B$	$:=$	$(\nu X \cdot B \sqcup (A \sqcap \circ_d X))$

These operators are analogues of the $\exists\Diamond$, $\forall\Box$ *etc.* of conventional (probabilistic) temporal logic.

Fig. 9. Angelic/demonic temporal operators

7.1 Propagate $\lfloor\cdot\rfloor$ inwards

Recalling Lem. 8, define angelic/demonic versions of the temporal operators as in Fig. 9. (Compare Fig. 7.)

To distribute $\lfloor\cdot\rfloor$ inwards we use the equalities set out in this lemma: [20]

Lemma 15

$$\lfloor \circ A \rfloor \equiv \circ_d \lfloor A \rfloor \tag{11}$$
$$\lfloor \Diamond A \rfloor \equiv \lfloor \Diamond \lfloor A \rfloor \rfloor \tag{12}$$
$$\lfloor \Box A \rfloor \equiv \Box_d \lfloor A \rfloor \tag{13}$$

[20] Some of these have been defined/stated elsewhere in this report; we repeat them here for the convenience of having them all together.

$$\lfloor A \rhd B \rfloor \equiv \lfloor A \rfloor \rhd_d \lfloor B \rfloor \tag{14}$$

Proof *Only (12) needs comment. Its proof relies on the fact that $\Diamond$, like $\circ$, is semi-sublinear [14]; given that, its proof mimics that of Lem. 18.*

Note that we do not use $\Diamond_d$ (with the obvious definition) in this case, because we cannot: recall the remarks following Lem. 8. □

Using our lemma with Φ_0, we have

$$\begin{aligned} & \lfloor \Diamond(A \sqcup (B \rhd \Box C)) \rfloor \\ \equiv\ & \lfloor\, \Diamond(\lfloor A \rfloor \ \sqcup\ \lfloor B \rfloor \rhd_d (\Box_d \lfloor C \rfloor))\, \rfloor\ , \end{aligned}$$

in which all explicit expectations (A, B, C) have been made standard ($\lfloor A \rfloor$, $\lfloor B \rfloor$, $\lfloor C \rfloor$).

7.2 Convert $\Diamond$'s to standard operators

The procedure of the previous section eliminated all properly probabilistic modal operators, replacing them with demonic versions, except for $\Diamond$. To deal with $\Diamond$ we use our main result Cor. 13 which, combined with the above and Lem. 8, allows us to state that

$$\lfloor \Diamond A \rfloor \quad \equiv \quad (\Diamond_a A) \rhd_d A\ , \tag{15}$$

provided A is standard. Since the inward propagation of the previous section has made all sub-formulae standard, indeed (15) applies: in the case of Φ_0 we can continue

$$\begin{aligned} & \lfloor\, \Diamond(\lfloor A \rfloor \ \sqcup\ \lfloor B \rfloor \rhd_d (\Box_d \lfloor C \rfloor))\, \rfloor \\ \equiv\ & (\Diamond_a X) \rhd_d X\ , \\ & \text{where } X := \lfloor A \rfloor \ \sqcup\ \lfloor B \rfloor \rhd_d (\Box_d \lfloor C \rfloor)\,. \end{aligned} \tag{16}$$

We use the 'where'-clause to remember that X has been duplicated, so that we need calculate it only once.

7.3 Evaluate $\lfloor \Phi \rfloor$

The two translations of the previous sections transform Φ into an expression containing only $\circ_d, \diamond_a, \Box_d$ and $\rhd_d$. The number of those operators is no more than twice the number of operators in the original formula, provided the duplication inherent in (15) is properly noted. Thus our result will follow if we can establish that evaluation of each of those operators is linear in the size of the transition system. We discuss that briefly for each operator in turn; in each case P, Q are standard.

$\circ_d P$ — $\circ_d$ treats the system as entirely demonic. Examine all states, and select only those all of whose outgoing transitions lead into P.

$\diamond_a P$ — If the original system contains demonic (as well as probabilistic) choice, then the system will be treated as demonic/angelic by $\diamond_a$ — that is, although the probabilistic choice is made angelic, the pure demonic choice is retained. The operational behaviour for each complete transition is a 'first-stage' demonic choice of 'half-transition' followed by a 'second-stage' angelic choice of half-transition.

Start with the set of states P, and for each of its states follow all second-stage angelic half-transitions back, colouring their sources; if the source was uncoloured, continue on to follow back the first-stage half-transition, decrementing the 'first-stage transition count' of its originating state (prepared beforehand).

Having done that for all of P, go over the transitions again this time deleting all second-stage transitions followed, and adding all states whose first-stage count has become zero, in that case deleting the first-stage transitions as well.

Continue the process until no states are added; each transition will have been followed at most a constant number of times (amortised).

$\Box_d P$ — Treat it as $P \rhd_d 0$.

$P \rhd_d Q$ — $\rhd_d$ treats the system as entirely demonic; we work with the complement. Start with the set of states $\neg P \wedge \neg Q$, and for each transition leading backwards from there:

- if it leads into Q, ignore it; and
- if it leads into $P \wedge \neg Q$, add that state to the set.

In either case, delete the transition; and repeat the process with the added states, stopping the whole procedure when no new states are added. The result is the complement of the accumulated states; and in the process, each transition is considered at most once.

In the case of Φ_0 we carry out four calculations from the above, two within X and two outside it.

8 Conclusion

Abstract probabilities and 0-1 laws have long been recognised as important techniques for simplifying analysis in probabilistic systems. However the tendency has been to use formulations of those laws at the level of models [15,7,1] and not to integrate them formally as axioms of program logic, as is customary for other operational phenomena.

There are certainly difficulties in importing well-understood concepts directly from probability theory to a computational context, due to the complicating factor of nondeterminism: it is not present in classical probability theory. Many of those difficulties can be resolved using the probabilistic version of Dijkstra/Hoare-style program logic [8] which is intended to deal naturally with nondeterminism, probability and their interaction. In addition temporal logic provides a framework for handling properties of infinite (repeated) executions of programs — precisely the situation where 0-1 laws begin to bite. The resulting fragment of $qM\mu$ described in this paper, and used to define the temporal operators of qTL, is thus ideal for studying probability, nondeterminism and 0-1 laws all together.

In qTL we find, as in other works, that probabilistic choice when used specifically for "probability-1" properties can (to an extent) be interpreted angelically. But this is definitely not sound in all situations, and sometimes a demonic interpretation is necessary.

For example consider the formula $\lfloor\Diamond[s{=}2]\rfloor$ interpreted in the system defined by

$$s \neq 0 \quad \rightarrow \quad s{:=}\ 0 \ \oplus\ s{:=}\ 1 \ \oplus\ s{:=}\ 2\ .$$

A direct calculation shows that the probability of eventually reaching $s{=}2$ is strictly less than 1 (unless the system is initially in that state). But an angelic interpretation for $\oplus$ in $\lfloor\Diamond[s{=}2]\rfloor$ would give 1, and therefore must be unsound. To see that a demonic interpretation is also unsound consider the probability of eventually reaching $s{=}0$. Again a direct calculation shows that it is 1 irrespective of the initial state, whereas a demonic interpretation of $\oplus$ in the formula $\lfloor\Diamond[s{=}0]\rfloor$ gives 0 (except from $s{=}0$ initially).

Indeed finding an optimal balance between the two interpretations — in order to maintain soundness in all situations — is a major challenge. Using Lems. 8, 15 and the notations of Fig. 9, we can rewrite the conclusion of Thm. 14 as

$$\lfloor\Diamond[P]\rfloor \quad \equiv \quad (\Diamond_a P) \rhd_d P \tag{17}$$

$$
\begin{array}{lrcl}
* & \Box(A \rightrightarrows B) & \Rrightarrow & \Box A \rightrightarrows \Box B \\
 & \circ(A \rightrightarrows B) & \Rrightarrow & \circ A \rightrightarrows \circ B \\
 & \Box A & \Rrightarrow & \circ A \sqcap \circ\Box A \\
 & A \,\&\, \Box(A \Rightarrow \circ A) & \Rrightarrow & \Box A \\
** & \Box(A \rightrightarrows B) \,\&\, \Diamond A & \Rrightarrow & \Diamond B \\
 & A \sqcup \circ\Diamond A & \Rrightarrow & \Diamond A \\
 & \Box A & \Rrightarrow & \underline{1} - \Diamond(\underline{1} - A) \\
 & \Diamond A \,\&\, \Box(\circ A \Rightarrow A) & \Rrightarrow & A
\end{array}
$$

The 'extra implications' are defined $(A \Rightarrow B) := [A \leq B]$, and (via a Galois connection) $A \Rrightarrow (B \rightrightarrows C)$ iff $(A \,\&\, B) \Rrightarrow C$. They arise during the proof of these laws, designed to mimic Ben-Ari's axiomatisation [16] of standard branching-time temporal logic.

Fig. 10. Quantitative *qTL* generalisation of universal fragment of branching-time temporal logic [3, Fig. 7].

---

where, on the right, we omit the $[\cdot]$ brackets to bring out its resemblance to standard branching-time temporal logic, and to highlight its use of both angelic- and demonic abstractions of probabilistic choice. Rao [7] also uses two abstractions of probabilistic choice, though he imposes fairness on the execution sequences, which we do not. Others (Hart *et al.* [12], Vardi [1] use similar ideas, but their work is model- rather than logic-based.

A more general comparison with the standard logics is given in the laws [3, Fig. 7], which we reproduce (partially) as Fig. 10. They are valid in *qTL* generally (though not claimed to be complete), but can be specialised to "with probability 1" by applying $\lfloor\cdot\rfloor$ and using only standard expectations: thus $(*)$ becomes the well-known $\Box_d(P \Rightarrow Q) \Rrightarrow (\Box_d P \Rightarrow \Box_d Q)$. In case $(**)$ however, cannot eliminate the $\lfloor\cdot\rfloor$ so easily: we are left with the less attractive-looking but still reasonable [21]

$$\Box_d(P \Rightarrow Q) \;\wedge\; (\Diamond_a P \rhd_d P) \quad \Rrightarrow \quad \Diamond Q \;,$$

which means "if all reachable states satisfying P satisfy Q also, and P is reached with probability 1, then so is Q." It is worth investigating whether there is a complete collection in this style of laws for with-probability-1 properties.

The emphasis of our work has been to clarify exactly when each of the two

[21] Since the *lhs* is standard, there is no need for $\lfloor\cdot\rfloor$ on the right.

interpretations of $\oplus$ is appropriate for the interpretation of temporal formulae in probabilistic systems. Granting the 0-1 law the status of a logical axiom proved to be critical in doing so.

To summarise, we have shown that the demonic interpretation goes with greatest fixed-points ("always" and "unless") and "=1" probabilities , and that the angelic goes with least fixed points ("eventually") and ">0" probabilities, finally leaving the 0-1 law standing out as the key idea underlying their combination in "=1" eventually properties.

A secondary contribution of this work is the complexity of the model checking problem. The result sketched in Sec. 7 shows that for the logic corresponding to "worst case" probabilistic *CTL* the complexity is linear in the size of the formula and the size of the underlying transition system. That matches the best known complexity for nonprobabilistic *CTL* interpreted over nonprobabilistic transition systems [17]. We note however that this work presents a very specialised case of the more general model-checking problem, which allows for the possibility of *angelic* as well as demonic nondeterminism [1]. Indeed it still appears that the luxury of enhancing the logic's expressivity in this way is paid by the complexity in the model checking, for the best known algorithms imply that (in this case) it is quadratic (*e.g.* de Alfaro and Henzinger [18], Courcoubetis and Yannakakis [19] and Vardi [1]).

References

[1] M. Vardi, Automatic verification of probabilistic concurrent finite-state programs, in: Proc. 26th IEEE Symp. on Foundations of Computer Science, Portland, 1985, pp. 327–338.

[2] C. Morgan, A. McIver, A probabilistic temporal calculus based on expectations, in: L. Groves, S. Reeves (Eds.), Proc. Formal Methods Pacific '97, Springer Verlag Singapore, 1997, available at [20].

[3] C. Morgan, A. McIver, An expectation-based model for probabilistic temporal logic, Logic Journal of the IGPL 7 (6) (1999) 779–804, `http://www3.oup.co.uk/igpl/Volume_07/Issue_06`; also available via [20].

[4] D. Kozen, Results on the propositional μ-calculus, Theoretical Computer Science 27 (1983) 333–354.

[5] A. McIver, Quantitative program logic and counting rounds in probabilistic distributed algorithms, in: Proc. 5th Intl. Workshop ARTS '99, Vol. 1601 of LNCS, 1999.

[6] K. M. Chandy, J. Misra, Parallel Program Design — a Foundation, Addison-Wesley, 1988.

[7] J. Rao, Reasoning about probabilistic parallel programs, ACM Trans. Prog. Lang. Syst. 16 (3).

[8] C. Morgan, A. McIver, K. Seidel, Probabilistic predicate transformers, ACM Trans. Prog. Lang. Syst. 18 (3) (1996) 325–353.

[9] E. Emerson, Temporal and modal logics, in: J. van Leeuwen (Ed.), Handbook of Theoretical Computer Science, Volume B: Formal Models and Semantics, Elsevier and MIT Press, 1990, pp. 995–1072.

[10] A. Pnueli, L. Zuck, Probabilistic verification, Information and Computation 103 (1) (1993) 1–29.

[11] M. Sharir, A. Pnueli, S. Hart, Verification of probabilistic programs, SIAM J. Comput. 13 (2) (1984) 292–314.

[12] S. Hart, M. Sharir, A. Pnueli, Termination of probabilistic concurrent programs, ACM Trans. Prog. Lang. Syst. 5 (1983) 356–380.

[13] C. Morgan, Proof rules for probabilistic loops, in: H. Jifeng, J. Cooke, P. Wallis (Eds.), Proceedings of the BCS-FACS 7th Refinement Workshop, Workshops in Computing, Springer Verlag, 1996, `http://www.springer.co.uk/ewic/workshops/7RW`.

[14] A. McIver, C. Morgan, Demonic, angelic and unbounded probabilistic choices in sequential programs, Acta Inf. 37 (2001) 329–354.

[15] A. Bianco, L. de Alfaro, Model checking of probabilistic and nondeterministic systems, in: Foundations of Software Technology and Theoretical Computer Science, Vol. 1026 of LNCS, 1995, pp. 499–512.

[16] M. Ben-Ari, A. Pnueli, Z. Manna, The temporal logic of branching time, Acta Inf. 20 (1983) 207–226.

[17] R. Cleaveland, B. Steffen, A linear-time model-checking algorithm for the alternation-free modal-μ calculus, in: Proc. CAV, 1991.

[18] L. de Alfaro, T. Henzinger, Concurrent ω-regular games, in: Proc. 15th IEEE Symp. Logic in Computer Science, IEEE, 2000.

[19] C. Courcoubetis, M. Yannakakis, The complexity of probabilistic verification, JACM 42 (4) (1995) 857–907.

[20] PSG, Probabilistic Systems Group: Collected reports, `http://web.comlab.ox.ac.uk/oucl/research/areas/probs/bibliography.html`.

A Proofs of lemmas

Lemma 16 eventually-until — *For all predicates P, Q we have*

$$P \rhd (P \wedge Q) \ \wedge \ \Diamond Q \quad \Rrightarrow \quad \Diamond(P \wedge Q) \ .$$

Proof *Let L_n and R_n be the n^{th} terms respectively in the $\sqcup$-limits for the least fixed-points $\Diamond Q$ and $\Diamond(P \wedge Q)$. We show by induction that*

$$P \rhd (P \wedge Q) \ \wedge \ L_n \quad \Rrightarrow \quad R_n$$

for all n.

Base case: *$L_0 \equiv R_0 \equiv False$.*

Inductive case:

$$\begin{array}{lll}
 & P \rhd (P \wedge Q) \ \wedge \ L_{n+1} & \\
\equiv & \quad (P \wedge Q) \ \vee \ (P \wedge \circ(P \rhd (P \wedge Q))) & \textit{definitions } \rhd, \Diamond \\
 & \wedge \quad Q \ \vee \ \circ L_n & \\
\equiv & \quad (P \wedge Q) \ \wedge \ (Q \vee \circ L_n) & \textit{propositional reasoning} \\
 & \vee \ (P \wedge \circ(P \rhd (P \wedge Q))) \ \wedge \ Q & \\
 & \vee \ (P \wedge \circ(P \rhd (P \wedge Q))) \ \wedge \ \circ L_n & \\
\Rrightarrow & \quad P \wedge Q & \textit{propositional reasoning; conjunctivity (3)} \\
 & \vee \ P \wedge Q & \\
 & \vee \ \circ((P \rhd (P \wedge Q)) \wedge L_n) & \\
\Rrightarrow & \quad P \wedge Q & \textit{propositional reasoning; inductive hypothesis; monotonicity} \\
 & \vee \ \circ R_n & \\
\equiv & \Diamond R_{n+1} \ . & \textit{definition } \Diamond
\end{array}$$

We complete the proof by observing that "$(P \rhd (P \wedge Q)) \wedge$" distributes through $\sqcup$-limits. □

Lemma 17 probabilistic eventually-until — *For all expectations A, B we have*

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

Proof *We follow the proof of Lem. 16, but must be careful in two respects: first, that we generalise $\wedge$ sometimes to $\sqcap$ and sometimes to $\&$; and second that*

— unlike $\wedge$ — the operator $\&$ is not idempotent. It is associative, however.

Let L_n and R_n be the n^{th} terms respectively in the $\sqcup$-limits for the least fixed-points $\Diamond B$ and $\Diamond(A \,\&\, B)$. We show by induction that

$$A \rhd (A \,\&\, B) \;\&\; L_n \quad \Rrightarrow \quad R_n$$

for all n.

Base case: $L_0 \equiv R_0 \equiv 0$.

Inductive case:

$$\begin{array}{lll}
 & A \rhd (A \,\&\, B) \;\&\; L_{n+1} & \\
\equiv & \quad (A \,\&\, B) \;\sqcup\; (A \sqcap \circ(A \rhd (A \,\&\, B))) & \textit{definitions } \rhd, \Diamond \\
 & \& \quad B \;\sqcup\; \circ L_n & \\
\equiv & \quad (A \,\&\, B) \;\&\; (B \sqcup \circ L_n) & \textit{arithmetic: } \sqcup, \sqcap \textit{ distribute through } \& \\
 & \sqcup\, (A \sqcap \circ(A \rhd (A \,\&\, B))) \;\&\; B & \\
 & \sqcup\, (A \sqcap \circ(A \rhd (A \,\&\, B))) \;\&\; \circ L_n & \\
\Rrightarrow & \quad A \,\&\, B & \textit{arithmetic; } \&\textit{-subadditivity (5)} \\
 & \sqcup\, A \,\&\, B & \\
 & \sqcup\, \circ((A \rhd (A \,\&\, B)) \,\&\, L_n) & \\
\Rrightarrow & \quad A \,\&\, B & \textit{propositional reasoning; inductive hypothesis; monotonicity} \\
 & \sqcup\, \circ R_n & \\
\equiv & \quad \Diamond R_{n+1}\ . & \textit{definition } \Diamond
\end{array}$$

We complete the proof by observing that "$(A \rhd (A \,\&\, B))\ \&$" distributes through $\sqcup$-limits. □

Lemma 18 *For all expectations A we have $\circ_d A \equiv \circ_d \lfloor A \rfloor$.*

Proof *We use sublinearity (Property 4 Fig. 4). For any $n \geq 0$ we have by arithmetic that*

$$\lfloor A \rfloor \quad \Rrightarrow \quad (n{+}1)A \ominus n \tag{A.1}$$

and, because the state space S is finite, there is some (large enough) n_A for which (A.1) is actually an equality. Now

$$
\begin{array}{lll}
 & \circ_d\lfloor A\rfloor & \\
\equiv & \lfloor\circ((n_A{+}1)A \ominus n_A)\rfloor & \textit{definition } \circ_d\textit{; choose } n_A \textit{ large enough} \\
\Leftarrow & \lfloor(n_A{+}1)\circ A \ \ominus \ n_A\rfloor & \textit{sublinearity of } \circ \\
\Leftarrow & \lfloor\lfloor\circ A\rfloor\rfloor & \textit{(A.1)} \\
\equiv & \circ_d A\ . &
\end{array}
$$

The reverse inequality is immediate from monotonicity. □

Lemma 19 *For all expectations A we have $\circ_a A \equiv \circ_a\lceil A\rceil$.*

Proof *Again we use sublinearity (as scaling and feasibility; see end Sec. 2.2). For any $n \geq 0$ we have that*

$$\lceil A\rceil \quad \Leftarrow \quad nA \sqcap 1 \tag{A.2}$$

and, because the state space S is finite, there is some (large enough) n_A for which (A.2) is actually an equality. Now

$$
\begin{array}{lll}
 & \circ_a\lceil A\rceil & \\
\equiv & \lceil\circ(n_A A \sqcap 1)\rceil & \textit{definition } \circ_a\textit{; choose } n_A \textit{ large enough} \\
\Rrightarrow & \lceil\circ(n_A A) \ \sqcap \ \circ 1\rceil & \textit{monotonicity} \\
\Rrightarrow & \lceil n_A(\circ A) \ \sqcap \ 1\rceil & \textit{scaling and feasibility of } \circ \\
\Rrightarrow & \lceil\lceil\circ A\rceil\rceil & \textit{(A.2)} \\
\equiv & \circ_a A\ . &
\end{array}
$$

The reverse inequality is immediate from monotonicity. □

Lemma 20 *If $\lfloor\mathcal{F}.X\rfloor \equiv \mathcal{G}.\lfloor X\rfloor$ for all expectations X, then*

$$\lfloor\nu\mathcal{F}\rfloor \quad \equiv \quad \nu\mathcal{G}\ .$$

Proof *Because $\lfloor\cdot\rfloor$ distributes through infimum $\sqcap$, we prove by induction that*

$$\lfloor\mathcal{F}^n.1\rfloor \quad \equiv \quad \mathcal{G}^n.1\ .$$

For the base case we require trivially that $\lfloor \mathcal{F}^0.1 \rfloor \equiv 1 \equiv \mathcal{G}^0.1$. *For the induction we have*

$$
\begin{array}{lll}
 & \lfloor \mathcal{F}^{n+1}.1 \rfloor & \\
\equiv & \lfloor \mathcal{F}.(\mathcal{F}^n.1) \rfloor & \\
\equiv & \mathcal{G}.\lfloor \mathcal{F}^n.1 \rfloor & \textit{assumption} \\
\equiv & \mathcal{G}.(\mathcal{G}^n.1) & \textit{inductive hypothesis} \\
\equiv & \mathcal{G}^{n+1}.1 \ . &
\end{array}
$$

□

Lemma 21 *If* $\lceil \mathcal{F}.X \rceil \equiv \mathcal{G}.\lceil X \rceil$ *for all expectations* X*, then*

$$\lceil \mu\mathcal{F} \rceil \quad \equiv \quad \mu\mathcal{G} \ .$$

Proof *Because* $\lceil \cdot \rceil$ *distributes through supremum* $\sqcup$*, we prove by induction that*

$$\lceil \mathcal{F}^n.1 \rceil \quad \equiv \quad \mathcal{G}^n.1 \ .$$

For that the proof is analogous to Lem. 20. □

Theorem 22 0-1 Law for deterministic/abort-free systems *If for some probability* p *satisfying* $0 < p \leq 1$ *we have*

$$p(I \rhd [\neg G]) \quad \Rrightarrow \quad \Diamond[\neg G] \ , \tag{A.3}$$

then in fact we have

$$I \rhd [\neg G] \quad \Rrightarrow \quad \Diamond[\neg G] \ , \tag{A.4}$$

provided $\circ$ *is deterministic and terminating.*

Proof *We rely on four main ideas, based on thinking of* I *as a loop invariant and* G *as the loop guard. The first idea is that* $I \rhd [\neg G]$ *is an invariant of any loop with guard* G*: if* $I \rhd [\neg G]$ *holds*[22] *initially, then it continues to hold up to and including loop termination, the point at which* $\neg G$ *is established.*

[22] We say "holds" even if I might not be standard: it assists the intuition when I is in fact standard; and the reasoning is sound in any case.

The second idea is that invariance is preserved by scaling: if J is any invariant, then so is pJ for any scalar $0 \leq p$. That will tell us, from above, that $p(I \rhd [\neg G])$ is invariant too.

The third idea is that $1 - \Diamond[\neg G]$ is invariant also, provided the system is deterministic and terminating. Its being invariant says "if $\neg G$ is not a guaranteed eventuality here, then taking a computational step won't make it so".

The fourth idea is that the sum of two invariants, provided that sum is well defined in the sense of lying between 0 and 1, is also an invariant.

Combining all those, we will be able to show that the complicated expression

$$J \quad := \quad p(I \rhd [\neg G]) + (1 - \Diamond[\neg G]) \tag{A.5}$$

is an invariant; but from it we'll conclude that

$$p(I \rhd [\neg G]) \quad \Rrightarrow \quad p(\Diamond[\neg G]) \ , \tag{A.6}$$

whence division by p will give us our desired conclusion (A.4). The only place we use our assumption (A.3) is to to note that it ensures (trivially) that J is well defined (lies in $[0,1]$); the only place we use $p > 0$ is in the division that takes us from (A.6) to (A.4).

We begin by noting that invariance of J conventionally means "if it holds now, then it continues to hold up until and including the step in which $\neg G$ becomes true, if $\neg G$ ever does become true". That is, to say that J is invariant we require

$$J \quad \Rrightarrow \quad J \rhd (J \,\&\, [\neg G]) \ , \tag{A.7}$$

where the extra $J\&$ ensures it remains true for the final step ('as the loop exits'). But (A.7) follows from the simpler

$$J \,\&\, [G] \quad \Rrightarrow \quad \circ J \ , \tag{A.8}$$

which is just the way one reasons about loop invariants:[23] *to show that we calculate*

$$\begin{array}{ll} & (J \,\&\, [\neg G]) \sqcup (J \sqcap \circ J) \\ \Leftarrow & (J \,\&\, [\neg G]) \sqcup (J \sqcap (J \,\&\, [G])) \qquad \textit{assumption (A.8)} \end{array}$$

[23] ... because (A.8) just says "invariant J is preserved by executing the loop body while the guard holds".

$$\equiv \qquad J \,\&\, [\neg G] \quad \sqcup \quad J \,\&\, [G] \qquad \textit{arithmetic}$$

$$\equiv \qquad J \ ,$$

whence we get (A.7) from Lem. 3 (2). So we check that our particular J (A.5) satisfies (A.8) by calculating

$$\circ(p(I \rhd [\neg G]) + (1 - \Diamond[\neg G]))$$

$$\equiv \qquad \circ(p(I \rhd [\neg G])) + \circ 1 - \circ\Diamond[\neg G] \qquad \circ \textit{ deterministic}$$

$$\Leftarrow \qquad \circ \textit{ scaling and abort-free; } \circ\Diamond[\neg G] \Rrightarrow \Diamond[\neg G]$$

$$p(\circ(I \rhd [\neg G])) + 1 - \Diamond[\neg G]$$

$$\Leftarrow \qquad (I \rhd [\neg G]) \,\&\, [G] \Rrightarrow \circ(I \rhd [\neg G])$$

$$(p(I \rhd [\neg G]) + 1 - \Diamond[\neg G]) \ \ \& \ \ [G] \ .$$

We have now shown that J satisfies (A.7).

To finish off, we put "$\&\Diamond[\neg G]$" on both sides of (A.7), and use Lem. 17 to conclude by reasoning

$$J \,\&\, \Diamond[\neg G]$$

$$\Rrightarrow \qquad J \rhd (J \,\&\, [\neg G]) \ \ \& \ \ \Diamond[\neg G] \qquad \textit{from (A.7)}$$

$$\Rrightarrow \qquad \Diamond(J \,\&\, [\neg G]) \ . \qquad \textit{Lem. 17}$$

Now by arithmetic $J \,\&\, \Diamond[\neg G]$ is just $p(I \rhd [\neg G])$, and $J \,\&\, [\neg G]$ is just $p[\neg G]$ whence — using scaling of $\Diamond$ — we end up with (A.6), as required. □