Almost-certain eventualities and abstract probabilities in quantitative temporal logic

Annabelle McIver [1]

Programming Research Group
University of Oxford
Oxford OX1 3QD UK
anabel@comlab.ox.ac.uk [2]

Carroll Morgan

Dept. of Engineering and Computer Science
University of New South Wales
Sydney 2052 Australia
carrollm@cse.unsw.edu.au

Abstract

'Almost-certain eventualities' are liveness properties that hold with probability 1. 'Abstract probabilities' are probabilities in transition systems about which we know only that they are neither 0 nor 1.

Vardi [16] 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 quantitative temporal logic [8,9], 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 consider briefly the complexity of the specialised logic.

1 Introduction

Liveness properties of 'standard', that is non-probabilistic transition systems rely only on the connectivity of the system (considered as a graph). The same

[1] McIver was supported by the UK's *EPSRC* during this research.
[2] From Feb. 2001: Dept. of Computing, Macquarie University, Sydney 2019 Australia.

This is a preliminary version. The final version will be published in
Electronic Notes in Theoretical Computer Science
URL: www.elsevier.nl/locate/entcs

is true in probabilistic systems, up to a point: 'almost-certain eventualities' depend only on 'abstract probabilities', not on precise probabilistic values.

A typical *eventuality* is loop termination, for example, 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 probablistic choice, satisfies both $\Diamond[s{=}H]$ and $\Diamond[s{=}T]$ almost certainly: no matter where the system is started, the state s will evenually be H, and will eventually be T, provided $0 < p < 1$.

An *abstract probability* is one which — like p above — is known only to be neither 0 nor 1: beyond that, its precise value is immaterial for the conclusions that are to be drawn.

In this paper we consider a quantitative extension $qM\mu$ [8,9] of the modal μ-calculus [6]; 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 [7].)

Our principal contribution here is 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.

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 their Boolean (traditional) and quantitative (our numeric extension) form; in Sections 4 and 5 we present our principal results. Complexity is considered in Section 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* [6] 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, like eventually $\Diamond$ above, within the calculus and then

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

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

// 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]

using only those, a subset of the full language.

1.2 Probabilistic *transition systems and qMμ*

Probabilistic transition systems support a 'quantitative' modal μ-calculus — which we call $qM\mu$ — 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 the other two kinds.

As in the standard μ-calculus, temporal operators can be defined within $qM\mu$: the result is a *quantitative* temporal logic which we call qTL [8,9].

The standard μ-calculus embeds into $qM\mu$ by taking predicates, or their equivalent subsets, to the corresponding characteristic functions; as a consequence, standard 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 $1/n$ 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 the proof in Sec. 3.2.)

On the other hand, in the probabilistic system

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

$\neg b$ is reached with probability 1, provided p is bounded away from zero. [4]

[3] We use a UNITY-like [1] pseudo-code to describe the transitions.

[4] By "bounded away from zero" we mean that if we allow p to be some function $p.(b,n)$ of the state, then we require the existence of a fixed $\varepsilon > 0$ such that $p.(b,n) \geq \varepsilon$ for all b, n. When S is finite, however, it is sufficient to say "p is non-zero"; and if p is some constant (*e.g.*, is $1/2$), then "p is non-zero" is sufficient whether S is finite or not.
Note that in Fig. 1 the probability $1/n^2$ is everywhere non-zero but is not bounded away from zero.

We say in that case that eventually $\neg b$ occurs *almost certainly* over *abstract probability* p and, given that p's precise value is irrelevant for that conclusion, we could write the system (as Rao does for example [14])

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

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

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).

2 Summary of the μ-calculi

In this section we give a brief description of both the standard [6] and quantitative [8,9] 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.

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.
$a \notin \circ\{a\}$	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) we have for example

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

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' $\mathcal{E}$
$\mu\mathbb{E}$	least fixed-point of predicate-to-predicate function $\mathbb{E}$
$\nu\mathbb{E}$	greatest fixed-point of predicate-to-predicate function $\mathbb{E}$

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 $(s, s') \in \mathcal{T} \Rightarrow \mathcal{E}.s'$.
- Predicate-to-predicate functions $\mathbb{E}$ are sometimes called *predicate transformers*. We apply μ and ν only to $\mathbb{E}$ that are $\Rightarrow$-monotonic. Note that operator $\circ$ is monotonic by construction.
- The next-time operator $\circ$ is interpreted demonically, and is assumed (beyond monotonicity) to satisfy the *conjunctivity* property

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

  for all predicates P, Q.

Fig. 2. The standard modal μ-calculus

The transition system $\mathcal{T}$ is

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

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. Standard transition system

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* ($\overline{\cdot}$) over S.[5] (Discrete) distributions $\overline{S}$ over S are maps from S into the unit

[5] Note for comparison with the standard case that $S \leftrightarrow S$ is just $S \to \mathbb{P}S$, 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' $\mathcal{E}$
$\mu\mathbb{E}$	least fixed-point of expectation transformer $\mathbb{E}$
$\nu\mathbb{E}$	greatest fixed-point of expectation transformer $\mathbb{E}$

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 distibution: 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 assumed to satisfy the new property of *sublinearity* [11], 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 we write c both for the scalar and for the constant 'everywhere-c' function.

Fig. 4. The standard modal μ-calculus

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

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

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

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

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

Fig. 5. Probabilistic and demonic transition system

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

$\circ\{c, d, e\}.a = 1$	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 (Property 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[6] and specialises sublinearity: it is our 'best quantitative approximation' to conjunctivity (3).

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

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

Note that we have only an inequality,[7] whereas in the standard case (conjunctivity) we have equality.

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

[7] The inequality is because $\circ\{c, d\}.a \equiv \circ\{c, e\}.a \equiv 2/3$ is true of other transition systems

Consequences of sublinearity include (by simple arithmetic [11, Sec. 7 pp. 340ff]) the following properties for all expectations A, B:

monotonicity If $A \Rrightarrow B$ then $\circ A \Rrightarrow \circ B$.
feasibility $\circ A \Rrightarrow \sqcup A$.
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

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

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

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

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' [4]. When based on the standard calculus, they give absolute (*i.e.*, true or false) judgements; in the quantitative case, the judgements are probabilistic.

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* [8]

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

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. [9] We give the straightforward proof of that (Lem. A.1) as an example of the use of conjunctivity.

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.)

---

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 as "pessimistic" as necessary.

[8] Compare the *PSP* lemma of UNITY [1].

[9] Here for uniformity we use $\Rrightarrow$ for 'entails', which is consistent with its quantitative definition since $P \vdash Q$ iff $[P] \Rrightarrow [Q]$.

"eventually P"			
	$\Diamond P$	$:= \quad (\mu X \cdot P \vee \circ X)$	If sufficiently many steps are taken, then P will hold.
"always P"			
	$\Box P$	$:= \quad (\nu X \cdot P \wedge \circ X)$	No matter how many steps are taken P will continue to hold.
"P unless Q"			
	$P \rhd Q$	$:= \quad (\nu X \cdot Q \vee (P \wedge \circ X))$	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

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

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

In the quantitative case, we define the temporal operators as in Fig. 7.

Consider "$\Diamond A$" however: for general expectation A it is not helpful to interpret it as "the probability that eventually A is established", because the meaning of "establish A" is itself unclear if A is a number. So what does $\Diamond A$ mean? (Similar remarks apply of course to the other temporal operators.)

It can be shown that the special case $\Diamond[P]$ is indeed the probability of

eventually establishing P.[10] More generally [8] the expression $\diamond A$ is

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

The situation with the other operators is similar.[11]

Again (the generalisation of) conjunctivity plays an important role in high-level reasoning. Using &-subdistribution, for example, we can prove a generalisation of (6); it is the quantitative eventually-until lemma

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

which we prove as Lem. A.2.

As an example of probabilistic eventualities, we return to the system 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: $[\neg b] \;\sqcup\; \circ([\neg b] \;\sqcup\; 2[b]/n(n+1))$

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

$\vdots$

[10] 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.
[11] Again we have agreement with the standard case, since if P is guaranteed to hold eventually then the strategy "stop when P holds" will establish *True*; if P is not guaranteed to hold eventually then, given any strategy, demonic choice could force either a "stop" in a state where P is false or an infinite run, also giving *False* (by definition).

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

so that we have

$\diamond[\neg b]$

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

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

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

$\equiv$ $1/n$ **if** b **else** 1 . 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. In System (1) following it, a similar calculation would be [12]

term 0: 0 $\bot \equiv 0$

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

$\equiv$ $[\neg b]$

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

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

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

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

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

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

[12] 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.

$\vdots$

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

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

Our aim is simply 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 $p > 0$. [13]

The important thing to note about this result is that p is only specified 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 the 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 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. We will prove a similar completeness result for general eventuality properties. 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 [14], Pnueli/Zuck [12] and Hart/Sharir/Pnueli [15]. 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 $\rhd$. The following properties can be proved directly from the operators' definitions [9] or — in some cases — have been given above.

Lemma 4.1 Properties of next-time — *For all expectations A, B,*

(i) $\circ A \,\&\, \circ B \Rrightarrow \circ(A \,\&\, B)$.

(ii) *If $A \Rrightarrow A'$, then $\circ A \Rrightarrow \circ A'$.*

(iii) $\circ 1 \equiv 1$.

Lemma 4.2 Properties of eventually — *For all expectations A, B,*

(i) $A \Rrightarrow \Diamond A$. [14]

(ii) $\circ\Diamond A \Rrightarrow \Diamond A$.

(iii) *If $B \sqcup \circ A \;\Rrightarrow\; A$, then $\Diamond B \Rrightarrow A$.*

(iv) *If $A \Rrightarrow A'$, then $\Diamond A \Rrightarrow \Diamond A'$.*

[13] 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.

[14] Note how this follows from our intuitive 'strategic' explanation earlier of $\Diamond A$: since the strategy "stop right now" is guaranteed to return at least A, the value of $\Diamond A$ can never be less than that.

Lemma 4.3 Properties of unless — *For all expectations A, B,*

(i) $B \;\Rrightarrow\; A \rhd B \;\Rrightarrow\; A \sqcup B$.

(ii) *If* $C \;\Rrightarrow\; B \sqcup (A \sqcap \circ C)$, *then* $C \Rrightarrow A \rhd B$.

(iii) $A \rhd B \equiv B \sqcup (A \sqcap \circ(A \rhd B))$.

(iv) *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 4.4 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 [15]), 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 desire a completeness property like Thm. 4.4 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.

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 $\mathbb{R}_{\geq}$.

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

ceiling $\lceil A\rceil.s \;:=\; \lceil A.s\rceil$, that is $[A.s \neq 0]$
floor $\lfloor A\rfloor.s \;:=\; \lfloor A.s\rfloor$, that is $[A.s = 1]$

With them we can write "almost certainly $\Diamond[P]$" as $\lfloor\Diamond[P]\rfloor$, and our aim is to calculate that from the 'connectivity' — 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

[15] provided we replace Lem. 4.1 Property (i) with full sublinearity.

'derived' transition operators, one converting probabilities to angelic choice, and the other converting them to demonic.

Definition 4.5 The *angelic* and *demonic* projections of $\circ$ are defined

angelic projection $\circ_a A \;:=\; \lceil \circ A \rceil$
demonic projection $\circ_d A \;:=\; \lfloor \circ A \rfloor$

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

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

provided $0 < p < 1$, 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

$$(s{:=}\ H \;{}_p\!\oplus\; s{:=}\ T)_d \quad = \quad s{:=}\ H \sqcap s{:=}\ T \ ,$$

again provided $0 < p < 1$. Clearly $\circ_a$ and $\circ_d$ depend only on the connectivity, since they discard all numeric information; it is not difficult to show that they determine the connectivity.[16]

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 4.6 Some properties of $\circ_d$ — *Projection $\circ_d$ in effect replaces probabilistic by demonic choice: it is conjunctive over predicates, monotonic in general, and distributes through greatest fixed-points:*

conjunctive $\circ_d([P] \,\&\, [Q]) \quad \equiv \quad \circ_d[P] \,\&\, \circ_d[Q]$.
monotonic *If $A \Rrightarrow A'$ then $\circ_d A \Rrightarrow \circ_d A$.*
gfp-distributive *If $\mathbb{E}.\circ$ is an expression containing the operator $\circ$, and $\mathbb{F}.\circ_d$ similarly, and they together satisfy $\lfloor \mathbb{E}.\circ.X \rfloor \equiv \mathbb{F}.\circ_d.\lfloor X \rfloor$ for all expectations X, then*

$$\lfloor \nu\mathbb{E}.\circ \rfloor \quad \equiv \quad \nu(\mathbb{F}.\circ_d) \ .$$

Proof. *Lemmas A.3 and A.5.* □

Lemma 4.7 Some properties of $\circ_a$ — *Projection $\circ_a$ in effect replaces probabilistic by angelic choice: it is monotonic, and distributes through least fixed-points:*

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

[16] For a purely probabilistic or purely demonic system, either $\circ_a$ or $\circ_d$ would be sufficient on its own; only for a mixture of the two forms of choice do you need both operators.

lfp-distributive *If $\mathbb{E}.\circ$ is an expression containing the operator $\circ$, and $\mathbb{F}.\circ_a$ similarly, and they together satisfy $\lceil \mathbb{E}.\circ.X \rceil \equiv \mathbb{F}.\circ_a.\lceil X \rceil$ for all expectations X, then*

$$\lceil \mu\mathbb{E}.\circ \rceil \quad \equiv \quad \mu(\mathbb{F}.\circ_a) \ .$$

Proof. *Lemmas A.4 and A.6.* □

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 4.8 *$\lfloor A \rhd B \rfloor$ 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 gfp-distribution of $\circ_d$ (Lem. 4.6) once we notice from Lem. A.3 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 (lfp-distribution (Lem. 4.7) and Lem. A.4).[17] □

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 $\circ$ interpreted as

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

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 $\lfloor \Diamond \cdot\cdot \rfloor$, at least when A is standard; for that we begin with the following lemma:

Lemma 4.9 *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 (iii) of Lem. 4.2:*

$$\begin{array}{lll}
 & A \sqcup \circ(\lceil \Diamond A \rceil \rhd A) \quad \Rrightarrow \quad \lceil \Diamond A \rceil \rhd A & \\
\textit{iff} & A \sqcup \circ(\lceil \Diamond A \rceil \rhd A) \quad \Rrightarrow \quad A \sqcup (\lceil \Diamond A \rceil \sqcap \circ(\lceil \Diamond A \rceil \rhd A)) & \textit{definition } \rhd \\
\textit{iff} & \circ(\lceil \Diamond A \rceil \rhd A) \quad \Rrightarrow \quad \lceil \Diamond A \rceil & \textit{arithmetic; } A \Rrightarrow \lceil \Diamond A \rceil \textit{ (Lem. 4.2)} \\
\textit{iff} & \circ(\lceil \Diamond A \rceil \rhd A) \quad \Rrightarrow \quad \lceil A \rceil \sqcup \lceil \circ \Diamond A \rceil & \textit{definition } \Diamond A\textit{; arithmetic}
\end{array}$$

if $\lceil \Diamond A \rceil \rhd A \Rrightarrow \lceil \Diamond A \rceil \sqcup A \Rrightarrow \lceil \Diamond A \rceil$ *(Lemmas 4.2, 4.3); monotonicity* $\circ$

[17] With the obvious definitions we could write just

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

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

which is a consequence of Lem. A.4. □

Lem. 4.9 gives us trivially a connectivity-calculable upper bound on $\lfloor\Diamond A\rfloor$:

Lemma 4.10 Upper bound for almost-certain eventuality

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

Proof. *Lem. 4.9 and the monotonicity of* $\lfloor\cdot\rfloor$. □

The right hand side is calculable from the connectivity of $\circ$, because by Lem. 4.8 we know that $\lceil\Diamond A\rceil$ is so calculable, and by Lem. 4.8 (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.[18] We gave an example of the 0-1 law for purely probabilistic programs; the idea has been extended to probabilistic/demonic programs [5,10] using the notation and ideas of temporal logic.

Lemma 5.1 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 [10, Lem. 6.1 p10]. As an illustration, however, we give a proof entirely in qTL (Thm. A.7) 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 5.2 0-1 Law (finite state spaces) — *In finite state models, Lem. 5.1 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. That means that Lem. 5.1 is equivalent to the following, in which we have eliminated*

[18] 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.

the abstract p.[19]

$$\text{(9)} \qquad \text{if } A \rhd [P] \Rrightarrow \lceil \Diamond [P] \rceil \quad \text{ then } \quad A \rhd [P] \Rrightarrow \Diamond [P]$$

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. 4.3 (ii) 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. 4.3(i) and 4.2(i) 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 5.3 *For finite models,* $\Diamond [P] \equiv \lceil \Diamond [P] \rceil \rhd [P]$*.*

Proof. *In finite models we may use the second form Lem. 5.2 of the 0-1 law; the result then follows from Lemma 4.9.* □

Cor. 5.3 is the key to showing that for probability-1 properties, connectivity is sufficient.

Theorem 5.4 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. 5.3 gives us that* $\Diamond [P] \equiv \lceil \Diamond [P] \rceil \rhd [P]$*, from which we have*

$$\text{(10)} \qquad \lfloor \Diamond [P] \rfloor \quad \equiv \quad \lfloor \lceil \Diamond [P] \rceil \rhd [P] \rfloor \ .$$

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

6 Example

Consider the abstract system

$$s{:=}\ H \quad | \quad s{:=}\ T \ ,$$

[19] 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.

where the "|" represents an abstract ${}_p\oplus$ with $0 < p < 1$. 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

$$
\begin{array}{lll}
 & \lfloor \Diamond\{H\} \rfloor & \\
\equiv & \lfloor \lceil \Diamond\{H\} \rceil \rhd \{H\} \rfloor & \text{Cor. 5.3} \\
\equiv & \lfloor \circ_a\{H\} \rhd \{H\} \rfloor & \text{Lem. 4.8} \\
\equiv & \lfloor 1 \rhd \{H\} \rfloor & \text{inspection: choice } | \text{ is abstract} \\
\equiv & 1 \ . & \text{Lems. 4.3(ii), 4.1(iii)}
\end{array}
$$

7 Complexity analysis

8 Conclusion

The implications of our result are that for almost-certain eventualities in the quantitative temporal logic we can simplify both the description of the transition system (as *e.g.* does Rao [14]), merely giving sufficient information to establish connectivity. That etsablishes the analog of similar results in the more traditional probabilistic calculi/logics [3,2].

For example, define *Prog* to be

$$
\mathit{Prog0} \mid \mathit{Prog1} \mid \cdots \mid \mathit{ProgN} \ , \tag{11}
$$

where the successive $\mid \cdots \mid$'s represent unknown but bounded-away-from-zero probabilities $p_0 \cdots p_N$ of selecting $\mathit{Prog0} \cdots \mathit{ProgN}$. From our definitions Def. 4.5 we have clearly, for any postcondition P,

$$
\begin{array}{lll}
 & \mathit{Prog}_a.[P] & \\
\equiv & \lceil p_0(\mathit{Prog0}.[P]) + \cdots + p_N(\mathit{ProgN}.[P]) \rceil & \\
\equiv & \mathit{Prog0}_a.[P] \sqcup \cdots \sqcup \mathit{ProgN}_a.[P] \ , & \text{arithmetic: no } p_i \text{ is zero}
\end{array}
$$

whose last line we could therefore take as part of the definition of (11) in the cut-down calculus. (The other part would be the behaviour of Prog_d.)

References

[1] K. Mani Chandy and Jayadev Misra. *Parallel Program Design — a Foundation.* Addison-Wesley, 1988.

[2] C. Courcoubetis and Mihalis Yannakakis. The complexity of probabilistic verification. *JACM*, 42(4):857–907, 1995.

[3] L. de Alfaro. Computing minimum and maximum reachability times in probabilistic systems. In *Proceedings of CONCUR99*, LNCS. Springer Verlag, 1999.

[4] E.A. Emerson. Temporal and modal logics. In Jan van Leeuwen, editor, *Handbook of Theoretical Computer Science, Volume B: Formal Models and Semantics*, pages 995–1072. Elsevier and MIT Press, 1990.

[5] S. Hart, M. Sharir, and A. Pnueli. Termination of probabilistic concurrent programs. *ACM Transactions on Programming Languages and Systems*, 5:356–380, 1983.

[6] D. Kozen. Results on the propositional μ-calculus. *Theoretical Computer Science*, 27:333–354, 1983.

[7] A.K. McIver. (annabelle's paper on expected steps). *Theoretical Computer Science*, 0:0, 2000.

[8] Carroll Morgan and Annabelle McIver. A probabilistic temporal calculus based on expectations. In Lindsay Groves and Steve Reeves, editors, *Proc. Formal Methods Pacific '97*. Springer Verlag Singapore, July 1997. Available at [13].

[9] Carroll Morgan and Annabelle McIver. An expectation-based model for probabilistic temporal logic. *Logic Journal of the IGPL*, 7(6):779–804, 1999.

[10] C.C. Morgan. Proof rules for probabilistic loops. In He Jifeng, John Cooke, and Peter Wallis, editors, *Proceedings of the BCS-FACS 7th Refinement Workshop*, Workshops in Computing. Springer Verlag, July 1996. `http://www.springer.co.uk/ewic/workshops/7RW`.

[11] C.C. Morgan, A.K. McIver, and K. Seidel. Probabilistic predicate transformers. *ACM Transactions on Programming Languages and Systems*, 18(3):325–353, May 1996.

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

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

[14] J.R. Rao. Reasoning about probabilistic parallel programs. *ACM Transactions on Programming Languages and Systems*, 16(3), May 1994.

[15] M. Sharir, A. Pnueli, and S. Hart. Verification of probabilistic programs. *SIAM Journal on Computing*, 13(2):292–314, May 1984.

[16] M.Y. Vardi. Automatic verification of probabilistic concurrent finite-state programs. In *Proc. 26th IEEE Symp. on Foundations of Computer Science*, pages 327–338, Portland, October 1985.

A Proofs of lemmas

Lemma A.1 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:

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

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

Lemma A.2 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. A.1, 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 A.3 *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

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

$$\begin{array}{lll} \Leftarrow & \lfloor \lfloor \circ A \rfloor \rfloor & \textit{(A.1)} \\ \equiv & \circ_d A \ . & \end{array}$$

The reverse inequality is immediate from monotonicity. □

Lemma A.4 *For all expectations A we have $\circ_a A \equiv \circ_a \lceil A \rceil$.*

Proof. *Again we use sublinearity (as scaling and feasibility). 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 A.5 *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 A.6 *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. A.5. □

Theorem A.7 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*[20] *initially, then it continues to hold up to and including loop termination, the point at which $\neg G$ is established.*

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

[20] 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.

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:[21] *to show that we calculate*

$$\begin{array}{lll}
 & (J \,\&\, [\neg G]) \sqcup (J \sqcap \circ J) & \\
\Lleftarrow & (J \,\&\, [\neg G]) \sqcup (J \sqcap (J \,\&\, [G])) & \textit{assumption (A.8)} \\
\equiv & J \,\&\, [\neg G] \quad \sqcup \quad J \,\&\, [G] & \textit{arithmetic} \\
\equiv & J \;, &
\end{array}$$

whence we get (A.7) from Lem. 4.3 (ii). So we check that our particular J (A.5) satisfies (A.8) by calculating

$$\begin{array}{lll}
 & \circ(p(I \rhd [\neg G]) + (1 - \Diamond[\neg G])) & \\
\equiv & \circ(p(I \rhd [\neg G]) + \circ 1 - \circ\Diamond[\neg G] & \circ \textit{ deterministic} \\
 & & \\
\Lleftarrow & & \circ \textit{ scaling and abort-free; } \circ\Diamond[\neg G] \Rrightarrow \Diamond[\neg G] \\
 & p(\circ(I \rhd [\neg G])) + 1 - \Diamond[\neg G] & \\
 & & \\
\equiv & & (I \rhd [\neg G]) \,\&\, [G] \Rrightarrow \circ(I \rhd [\neg G]) \\
 & (p(I \rhd [\neg G]) + 1 - \Diamond[\neg G]) \;\; \& \;\; [G] \;. &
\end{array}$$

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. A.2 to conclude by reasoning*

$$\begin{array}{lll}
 & J \,\&\, \Diamond[\neg G] & \\
\Rrightarrow & J \rhd (J \,\&\, [\neg G]) \;\; \& \;\; \Diamond[\neg G] & \textit{from (A.7)} \\
\Rrightarrow & \Diamond(J \,\&\, [\neg G]) \;. & \textit{Lem. A.2}
\end{array}$$

Now $J \,\&\, \Diamond[\neg G]$ *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.* □

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