An expectation-transformer model for probabilistic temporal logic

Carroll Morgan and A.K. McIver[*]

November 1999

Abstract

We interpret the modal μ-calculus over a new model [10], to give a temporal logic suitable for systems exhibiting both probabilistic and demonic nondeterminism. The logical formulae are real-valued, and the statements are not limited to properties that hold with probability 1.

In achieving that conceptual step, our technical contribution is to determine the correct quantitative generalisation of the Boolean operators: one that allows many of the standard Boolean-based temporal laws to carry over the reals with little or no structural alteration, even for properties that hold with probability strictly between 0 and 1. The generalisation is not obvious, but is dictated by our discovery elsewhere of the algebraic property that characterises the next-time operator over the new model: it is arithmetic 'sublinearity' [20, Fig.4 p.342], which replaces the Boolean *conjunctivity* that characterises next-time in a modal algebra.

We confirm by example that the new modal laws can be used for quantitative reasoning about probabilistic/demonic behaviour. The *random walk* is treated using only those laws and real-number arithmetic: arguing from precise numeric premises, more specific than simply 'with some non-zero probability', we reach numeric conclusions that are not simply 'with probability 1'.

Keywords: Temporal logic, probability, formal semantics, program correctness, weakest precondition.

1 Introduction

1.1 Background

Since Pnueli introduced temporal logic to computer science, the logic has been extended in various ways to include probability. One approach is to retain the standard syntax while altering the interpretation: probabilistic transitions are

[*] McIver is a member of the Programming Research Group at Oxford University, and is supported by the EPSRC: Wolfson Building, Parks Road, Oxford OX1 3QD, {*carroll,anabel*}*@comlab.ox.ac.uk*.

allowed in the computation, and the validity of the formulae is weakened to 'with probability 1'. The *0-1 law* of Sharir, Pnueli and Hart [9] shows that there are many systems in which such validity depends only on the transition probabilities' being nonzero, not on their precise values, and that has been exploited by many authors (for example Vardi [27] and Rao [23]).

Vardi's treatment of the "probabilistic universality problem" [27] extends that to demonic nondeterminism, thus an early example of combining both quantitative and qualititative uncertainty: the latter is characteristic of adversarial schedulers, for example. By removing the demonic choices first — a determinising 'subset' construction — he reduces the problem to a (nearly) deterministic version, and then proceeds from there. The results however remain qualititive: verification with respect to 'proper' probabilities (neither 0 nor 1) or other quantitative aspects (expected efficiency) requires different techniques.

Other approaches address explicit probabilities, but then forgo demonic nondeterminism [6]; yet nondeterminism is not only an unavoidable aspect of some problems but — as abstraction — is essential for forming layered descriptions of complex systems.

Finally, recent work by Bianco and de Alfaro [3], based on the pCTL of Aziz [1] and ultimately ideas of Hansson and Jonsson [8], allows both explicit probability and nondeterminism, recognising that the effect of standard nondeterminism is to force probabilistic judgements to give upper- or lower bounds rather than exact values: one speaks of judgements that hold 'with probability at least (or at most) p'. The formulae contain both Boolean and numeric components.

Our approach differs from all the above. It is quantitative (not only universal), it includes demonic (and potentially angelic) nondeterminism, it does not determinise to reduce to pure probabilities, and finally it does not mix Boolean and numeric formulae: the formulae are uniformly numeric. This report describes the two principal contributions: one contribution is conceptual, and the other is technical.

1.2 Conceptual contribution

The conceptual contribution (Sec. 3.1) is that probabilistic and demonic temporal behaviour can be described by a μ-calculus [15] based on reals rather than Booleans. The underlying model is of a branching-time computation using the now-common 'sets of probability distributions', and it is connected to a program logic via the 'expectation transformers' originally introduced by Kozen [13] for deterministic probabilistic programs and extended by us [20] to include demonic programs as well.

Formulae become real- rather than Boolean-valued functions of the state space; they can then be interpreted directly as probabilities, but more generally they are to be regarded as expectations (of random variables from probability theory). The resulting 'quantitative logic' easily accommodates analogues of temporal operators like 'next' ($\circ$ or $\forall X$), 'eventually' ($\diamond$ or $\forall F$) and 'always' ($\square$ or $\forall G$) — the first is interpreted as the effect of executing a single step within a probabilistic transition system, and the last two operators can express the *probability* of 'eventually' or 'always' properties with respect to probability distributions over paths in a computation tree generated by repeated probabilistic steps.[1] The path-distributions are determined by transition probabilities in the usual way (measures over Borel sets based on cylinders).

One advantage of using μ-calculus is to side-step explicit mention of the path distributions, relying instead on the correspondence proved elsewhere [14, 13, 20] between program logic and transition semantics. But there are practical benefits as well: we find that general expectations allow us to treat more than probabilities — indeed often an *expected quantitity* such as 'number of steps to termination' is required, rather than a specific probability. This logic based on expectations allows us to calculate the desired value directly [25, 16].

1.3 Technical contribution

The technical contribution is to determine what the correct generalisations of the standard Boolean propositional and modal operators should be: what are conjunction, disjunction and implication between real numbers; and what μ-formulae should represent the temporal operators over the reals? For the propositional operators (Sec. 3.2) we rely on the main result of our earlier work [20] which gave an exact arithmetic characterisation of 'demonic and probabilistic expectation transformers'; from it we extract definitions of probabilistic conjunction, disjunction and implication. For the temporal operators (Sec. 3.3) we appeal to operational arguments given in a companion paper [19] which tells us what their corresponding fixed-point formulations should be. With those together, we obtain an extension of Ben-Ari's axiomatisation [2] of branching-time temporal logic in which the structure of the formulae is largely preserved, even when reasoning over properly quantitative values (*i.e.* those not only 0 or 1).

The main insight is that probabilistic conjunction enables modular reasoning that is applicable *even* for probabilistic information. Although the probabilistic conjunction arises from the novel axioms characterising probabilistic sequential programs [20], where the distributions are over states, here we see it is equally apt when the probabilities derive instead from distributions over paths.

In obtaining our extension of the laws we observe that much of the operational intuition underlying standard temporal logic is valid for probability as well; because the laws are so similar to the standard ones, many proofs of probabilistic temporal properties will merely be replayings of their standard counterparts; both observations encourage us in the expectation-transformer approach.

1.4 Overview

Sec. 2 reviews nonprobabilistic branching-time temporal logic, in its predicate transformer formulation; Sec. 3 describes the probabilistic/demonic model, illustrated by a running example of demonically-nondeterministic coin-flipping;

[1] We discuss the angelic duals $\exists X$, $\exists F$ and $\exists G$ in the conclusion.

and Sec. 4 examines properties of the model and investigates the identities it supports.

In Sec. 5 we treat the random walk, an elementary example but one which nevertheless is completely beyond the reach of logics that do not quantify probabilities explicitly. Even the 'universal' [27] conclusion "the walker moves left eventually with probability 1" requires properly numeric premises, that the one-step probability is 1/2 in either direction. But in the more general case where those specific probabilities are not 1/2, even the conclusion is no longer universal: the probability of an eventual move is somewhere strictly between 0 and 1. In the example, without referring to the underlying computation tree at all, we reproduce the elementary result that a probabilistic demonic walker whose probability of moving left or right is bounded below by 1/3 (*i.e.* it is not known exactly) will return eventually with probability at least $1 - \sqrt{5}/3$.

In Sec. 6 we examine the benefits and limitations of using expectations, and discuss how our contributions relate to other approaches, in particular to pCTL and pCTL*. We also discuss model checking briefly.

We write $f.x$ for function f applied to argument x, left-associative and binding more tightly than all except modal operators; and $\mathit{this} := \mathit{that}$ introduces or instantiates *this*, defining it to be equal to *that*.

2 Standard temporal logic

Standard (nonprobabilistic) branching-time temporal logic is usually interpreted over computation trees; but an equivalent alternative is to use predicate transformers [4, 21], which we now review. Via probabilistic predicate transformers [20] we will then, in the next section, generalise the model to include probability.

The model is based on a state space S; we identify *predicates* with the subsets $\mathbb{P}S$ of S, and define the *predicate transformers* $\mathcal{T}S$ to be the functions *step* in $\mathbb{P}S \to \mathbb{P}S$ satisfying the *healthiness conditions* [4]

excluded miracle $\mathit{step}.\emptyset = \emptyset$,

monotonicity if $A \subseteq B$ then $\mathit{step}.A \subseteq \mathit{step}.B$ and

positive conjunctivity $\mathit{step}.(A \cap B) = \mathit{step}.A \cap \mathit{step}.B$,

for all predicates A, B.

A *predicate-transformer model* (S, step) for standard temporal logic comprises a state space S and a (predicate) transformer *step* in $\mathcal{T}S$ — the transformer represents one step in the computation about which temporal statements can be made, so that S corresponds to the nodes and *step* to the arcs of a computation tree in which branching represents nondeterminism.[2]

The temporal operators are functions in $\mathbb{P}S \to \mathbb{P}S$ more generally: although monotonic, they are not necessarily healthy. In their definitions below [5, p1066]

[2] Note however that divergence (**abort**) is possible in the predicate transformer model. For an exact match with the conventional view we would add the healthiness condition $\mathit{step}.S = S$.

we fix the model $(S, step)$, and use μ, ν denote least- and greatest fixed point respectively of monotonic transformers over $\mathbb{P}S$.

Definition 2.1 *next*

$$\circ A \quad := \quad step.A \; .$$

Predicate $\circ A$ holds[3] in just those states from which one execution of *step* will reach a state in which A holds. ■

In Definition 2.1 and below we have allowed both nondeterminism and nontermination in *step*, so that $\circ A$'s holding in state s implies that *all*[4] computations from s lead to a state in which A holds, and that none of those computations fail to terminate. Thus in particular $\circ S$ is the set of states from which *step* is guaranteed to terminate.

Definition 2.2 *eventually*

$$\Diamond A \quad := \quad (\mu X \bullet A \cup \circ X) \; .$$

Predicate $\Diamond A$ holds in just those states from which repeated steps (possibly none) will reach a state in which A holds. ■

The least fixed point is used because if infinite execution is possible from s without reaching A then $s \notin \Diamond A$.

Note that $\Diamond$ is not healthy: it fails *positive conjunctivity.*

Definition 2.3 *always*

$$\Box A \quad := \quad (\nu X \bullet A \cap \circ X) \; .$$

Predicate $\Box A$ holds in just those states from which repeated steps (possibly none) never leave states in which A holds. ■

The greatest fixed point is used because if infinite execution is possible from s without leaving A then $s \in \Box A$.

Operationally, we now note the correspondence with branching-time temporal logic, via the isomorphism [11] that links healthy transformers with relations between initial and final states. That ensures that *step* represents a state-to-state relation.

Taking *eventually* for example, define some syntactic program *Step* so that $step = \mathrm{wp}.Step$, where the semantic function wp takes programs to their meanings as transformers, and consider the predicate

$$\mathrm{wp}.(\mathbf{do}\ \neg A \rightarrow Step\ \mathbf{od}).true \tag{1}$$

that holds in just those states from which repeated execution of *Step* eventually establishes A. Simple calculation using the μ-semantics of $\mathbf{do} \cdots \mathbf{od}$ [4] shows that indeed (1) equals $\Diamond A$ as defined above.

[3] We use the original symbols $\circ$, $\Diamond$ and $\Box$ here, instead of $(\forall X)$, $(\forall F)$ and $(\forall G)$.

[4] The existential versions $\exists X$, $\exists F$ and $\exists G$ are discussed in Sec. 6.

$$\begin{array}{rcl}
\Box(A \Rightarrow B) & \Rightarrow & \Box A \Rightarrow \Box B \\
\circ(A \Rightarrow B) & \Rightarrow & \circ A \Rightarrow \circ B \\
\Box A & \Rightarrow & \circ A \wedge \circ\Box A \\
A \wedge \Box(A \Rightarrow \circ A) & \Rightarrow & \Box A \\
\Box(A \Rightarrow B) \wedge \Diamond A & \Rightarrow & \Diamond B \\
A \vee \circ\Diamond A & \Rightarrow & \Diamond A \\
\Box A & \Rightarrow & \neg\Diamond(\neg A) \\
\Diamond A \wedge \Box(\circ A \Rightarrow A) & \Rightarrow & A
\end{array}$$

Figure 1: Axioms for standard branching-time temporal logic, based on those of Ben-Ari [2].

A more thorough justification of Definition 2.2 appears elsewhere [19, Sec.4.2]; and a similar justification can be given for $\Box A$.

We note that Definitions 3.3–3.5 have all the properties[5] listed in Fig. 1; as a further illustration we give a direct proof of the following familiar fact.

Lemma 2.4 *double eventually*

$$\Diamond\Diamond A \quad = \quad \Diamond A\ .$$

Proof Directly from Definition 2.2 we have $A \subseteq \Diamond A$ and $\circ\Diamond A \subseteq \Diamond A$. Taking $A{:=}\ \Diamond A$ in the former gives $\Diamond A \subseteq \Diamond\Diamond A$ trivially; from the latter we have that $X{:=}\ \Diamond A$ satisfies

$$X \quad = \quad \Diamond A \cup \circ X\ ,$$

of which however $\Diamond\Diamond A$ is the $\subseteq$-least solution. ■

3 Probabilistic temporal logic

3.1 Expectations and their transformers

Standard predicate transformer semantics can be generalised to replace demonic choice by probabilistic choice [6] — but more interesting is to add probabilistic choice while retaining demonic nondeterminism [10, 20]. By doing the latter, and generalising the definitions of the previous section, we obtain a model for probabilistic branching-time temporal logic.

Again take state space S; but define now the *expectations* $\mathcal{E}S$ over S as the functions $S \rightarrow [0, 1]$ from S into the closed interval $[0, 1]$, and define *expectation transformers* $\mathcal{P}S$ to be the functions *step* in $\mathcal{E}S \rightarrow \mathcal{E}S$ satisfying the probabilistic healthiness conditions given further below.

[5] For familiartity we use Boolean rather than set-theoretic operators in the figure. Ben-Ari *et al.* [2] show those axioms to be complete for standard temporal logic. Here we use them as examples of what is reasonable for a model.

Expectation transformers are due to Kozen [14] for programs containing probabilistic choice but no demonic nondeterminism, and correspond to an operational model in which programs are functions from initial states to final probabilistic distributions over states [13]:

> Let program *prog* take initial states in S to final distributions over S; write $\int_D X$ for the expected value of random variable X over distribution D. Then the pre-expectation at state s of program *prog*, with respect to post-expectation A, is defined to be the expected value of A over the distribution *prog.s* obtained by executing *prog* from s:
>
> $$\mathrm{wp}.\mathit{prog}.A.s \quad := \quad \int_{\mathit{prog}.s} A \ .$$

In particular, if the post-expectation is the characteristic function of some predicate, then the pre-expectation is the probability that the program will establish that predicate.

Kozen's deterministic model [13] was extended to include nondeterminism by He [10], where programs are functions from initial state to *sets* of final distributions with certain closure conditions; Kozen's deterministic logic [14] was similarly extended by Morgan [20], who showed further that He's model corresponds exactly to the healthy expectation transformers of the logic.[6] The interpretation becomes

> Let program *prog* take initial states in S to *sets* of final distributions over S. Then the *greatest* pre-expectation of program *prog* with respect to post-expectation A is defined:
>
> $$\mathrm{wp}.\mathit{prog}.A.s \quad := \quad (\sqcap D\colon \mathit{prog}.s \bullet \int_D A) \ . \tag{2}$$

Nondeterminism is therefore demonic in the sense that it acts to minimise the pre-expectation at each initial state; the definition above is thus the greatest expectation everywhere no more than those pointwise minima.

Predicates embed into expectations as functions in $S \rightarrow \{0, 1\}$, so that the constant expectations $\underline{0}$ and $\underline{1}$, yielding 0 and 1 respectively in all states, replace predicates $\emptyset$ and S. (To avoid the clutter of an explicit embedding function, for predicate A and state s we will write either $s \in A$ or $A.s = 1$ *etc.* as convenient.)

The relations $\subseteq$, $=$ and $\supseteq$, acting between predicates, embed to

$\Rrightarrow$ — everywhere no more than,
$\equiv$ — (everywhere) equal and
$\Lleftarrow$ — everywhere no less than,

which are relations between expectations.

[6] Morgan [20] imposes an additional constraint of finiteness of S, which is weakened to continuity of *step* by McIver [17] when S is infinite. Neither constraint is needed here.

Embedded predicate transformers take characteristic functions to characteristic functions, and the weakest precondition becomes a greatest pre-expectation. We refer to the embeddings as *standard* expectations and transformers.

For example, let S be $\{x, y, z\}$ and consider the (deterministic) program that takes any initial state s to the final distribution

$$\text{states } x, y, z \text{ with probabilities } p, q, r \text{ respectively,} \tag{3}$$

where $p + q + r = 1$. Its corresponding predicate transformer *step* is defined

$$\mathit{step}.A.s \quad := \quad p(A.x) + q(A.y) + r(A.z) \ ,$$

which is the expected value of A over the given final distribution. (Note that it is a constant expectation, independent of s, since the action of the program does not depend on the initial state.)

Now consider the embedding of the predicate $\{x, y\}$; writing the set for its embedding, we have

$$\mathit{step}.\{x, y\}.s \quad = \quad p(1) + q(1) + r(0) \quad = \quad p + q \ ,$$

since $\{x, y\}.x = \{x, y\}.y = 1$ and $\{x, y\}.z = 0$, giving the probability $p + q$ that executing *step* results in a state in $\{x, y\}$. Note that *step* itself is standard when exactly one of p, q, r is 1 (and the others 0), and the pre-expectation is then standard also: it is 1 (S or 'true') when the program guarantees a result x or y, and 0 ($\emptyset$ or 'false') otherwise.

3.2 Probabilistic healthiness conditions

In this section we discuss the generalisations of the propositional operators.

The healthiness conditions for standard programs (Sec. 2) serve two purposes; (theoretical) they characterise exactly the predicate transformers that correspond to 'real' programs as relations between initial and final states; and (practical) they allow the proof of many algebraic laws over programs — for example, *positive conjunctivity* shows that nondeterminism right-distributes over sequential composition.

We discovered elsewhere [20] that the exact characterisation of probabilistic/demonic transformers is given by the conditions of Fig. 2; and they lead directly to the characterisation of probabilistic *next* (Fig. 6 below). That in turn will allow us to prove probabilistic analogues (Fig. 7 below) of the standard properties in Fig. 1.

The probabilistic healthiness conditions are listed in Fig. 2, where we use the notations

constant expectation $\underline{p}.s\!:= p$ for any p in $[0, 1]$

scalar multiplication $(pA).s := \ p \times A.s$ for all p in $[0, 1]$

weighted average $a\,{}_p\!\oplus b := \ p \times a + (1{-}p) \times b$ for p, a, b in $[0, 1]$

truncated subtraction $a \ominus b := \ (a - b) \sqcup 0$ for a, b in $[0, 1]$,

excluded miracle $\quad step.A \Rrightarrow \underline{\sqcup A}$

monotonicity $\quad$ if $A \Rrightarrow B$ then $step.A \Rrightarrow step.B$

scaling $\quad step.(pA) \equiv p(step.A)$

subdistributivity $\quad step.(A\ {}_p\!\oplus B) \Lleftarrow step.A\ {}_p\!\oplus step.B$

truncation $\quad step.(A \ominus \underline{p}) \Lleftarrow step.A \ominus \underline{p}$

The above together are equivalent to the single condition *sublinearity*,

$$step.(aA + bB \ominus \underline{c}) \quad \Lleftarrow \quad a(step.A) + b(step.B) \ominus c\ ,$$

which characterises [20, Thm.8.7 p.345] probabilistic/demonic transformers.

Figure 2: Probabilistic healthiness conditions.

together with the convention that binary scalar operators apply pointwise between expectations.

We note first that *excluded miracle* and *monotonicity* are simple generalisations of their standard versions. *Scaling* does not have a standard counterpart; but it reflects merely that expectations of random variables distribute scalar multiplication. We show that the remaining two probabilistic conditions act together to generalise positive conjunctivity, and that an 'obvious choice' $\sqcap$ (minimum) is incorrect.

It is not true in general that $step.(A \sqcap B) \equiv step.A \sqcap step.B$. Taking *step* from (3), we have for example

$$step.(\{x,y\} \sqcap \{y,z\}) \quad \equiv \quad step.\{y\} \quad \equiv \quad \underline{q}\ ,$$

but on the other hand

$$step.\{x,y\} \sqcap step.\{y,z\} \quad \equiv \quad \underline{p+q} \sqcap \underline{q+r} \quad \not\equiv \quad \underline{q}$$

when neither p nor r is 0.[7]

The correct generalisation of positive conjunctivity is subdistributivity of '&', defined as follows:

Definition 3.1 *ampersand* For a, b in $[0,1]$ we have

$$a \,\&\, b \quad := \quad (a+b) \ominus 1\ .$$

■

The definition is motivated by taking a, b, c all 1 in sublinearity (Fig. 2), and is justified by Lemma 3.2 to follow and the fact that it implies conjunctivity when restricted to standard arguments (shown below).

[7] The example shows the unsuitability of multiplication also, another 'obvious' contender for the probabilistic generalisation of conjunction.

Lemma 3.2 *subdistributivity of* & Any healthy expectation transformer *step* satisfies

$$step.(A \mathbin{\&} B) \quad \Lleftarrow \quad step.A \;\&\; step.B \ ,$$

for all expectations A, B.

Proof

$$\begin{array}{lll}
 & step.(A \mathbin{\&} B) & \\
\equiv & step.((A+B) \ominus \underline{1}) & \text{definition \&} \\
\equiv & 2(step.((A \,{}_{\frac{1}{2}}{\oplus}\, B) \ominus \underline{1/2})) & \text{scaling} \\
\Lleftarrow & 2(step.(A \,{}_{\frac{1}{2}}{\oplus}\, B) \ominus \underline{1/2}) & \text{truncation} \\
\Lleftarrow & 2((step.A \,{}_{\frac{1}{2}}{\oplus}\, step.B) \ominus \underline{1/2}) & {}_p{\oplus}\text{-subdistributivity} \\
\equiv & step.A \mathbin{\&} step.B \ . & \text{arithmetic; definition \&}
\end{array}$$

■

Returning to the example above, we note that indeed $(p+q) \mathbin{\&} (q+r) = q$; the special case of equality is due to *step*'s being deterministic and terminating.

To show that &-subdistributivity implies positive conjunctivity, let all of $step, A, B$ be standard. We have $step.(A \sqcap B) \Rrightarrow step.A \sqcap step.B$ by *monotonicity*, and we have the converse $step.(A \sqcap B) \Lleftarrow step.A \sqcap step.B$ from &-*subdistributivity* because on standard expectations & and $\sqcap$ agree.

3.3 A probabilistic model

In this section we discuss the generalisation of the modal operators; following Definition 3.4 below we give the operational justification for them.

The probabilistic model merely replaces the standard transformer by a probabilistic one, and generalises the standard operators' definitions (Defs. 2.1–2.3) to act with maximum and minimum over expectations rather than with union and intersection over sets. We now give those definitions, and use a running example to illustrate them.

An *expectation-transformer* model $(S, step)$ for probabilistic temporal logic comprises a state space S and a healthy expectation transformer *step*, with the following definitions.

Definition 3.3 *probabilistic next*

$$\circ A \quad := \quad step.A \ .$$

Expectation $\circ A$ is the expected value of A after exactly one step. If A is standard then $\circ A$ is the greatest guaranteed probability that one step will establish A. ■

If from some initial state *step* can yield several possible final distributions, the greatest probability with which *step* is *guaranteed* to reach A is the infimum of the expectation of A over those distributions.

We now illustrate Definition 3.3 with a simple example, involving both probabilistic and nondeterministic choice.

Consider two fair coins: the *thin* coin gives heads or tails with probability 1/2 each; the *fat* coin gives heads, tails or edge with probability 1/3 each. At most one coin is flipped at a time, and the state space S is $\{h, t, e\}$, representing the result of the most recent flip. The computation *step* is defined

current state	action of *step*
heads h	flip *thin* or *fat*
tails t	flip *fat* or do nothing
edge e	do nothing,

where 'or' in an action represents demonic nondeterminism. Fig. 3 tabulates $\circ A$ for that *step* over all standard A: note how the demon acts to *minimise* the probability of achieving the postcondition, when there is a choice.

For an illustration of proper expectations consider $\circ\circ\{t, e\}.h$, that is, applying $\circ$ to the nonstandard expectation $\circ\{t, e\}$ and evaluating it at state h. We have

$$
\begin{array}{lll}
 & \circ\circ\{t,e\}.h & \\
= & \quad (\circ\{t,e\}.h)/2 + (\circ\{t,e\}.t)/2 & \text{Definition 3.3} \\
 & \sqcap \; (\circ\{t,e\}.h)/3 + (\circ\{t,e\}.t)/3 + (\circ\{t,e\}.e)/3 & \\
= & \quad (1/2)/2 + (2/3)/2 & \text{Fig. 3} \\
 & \sqcap \; (1/2)/3 + (2/3)/3 + (1)/3 & \\
= & 7/12 \; , &
\end{array}
$$

which is the largest guaranteed probability of reaching state t or e in exactly two steps from state h.

Definition 3.4 *probabilistic eventually*

$$\Diamond A \quad := \quad (\mu X \bullet A \sqcup \circ X) \; .$$

Expectation $\Diamond A$ is the greatest expected value of A that can be realised by deciding 'angelically' ($\sqcup$) whether to take one step ($\circ X$) or to stop (A), with 'never stop' interpreted as 0 (μ). If A is standard then $\Diamond A$ is the greatest probability that repeated steps are guaranteed to reach a state in which A holds. ■

In Definition 3.4 we have generalised Boolean $\vee$ to arithmetic $\sqcup$ (and below in Definition 3.5 we take $\wedge$ to $\sqcap$). The justification for that (for $\sqcup$ rather than say the dual of &) is operational: it can be shown [19] that $\Diamond A$ as defined here is the supremum over all Boolean guards G of the pre-expectation

$$\text{wp}.(\textbf{do } G \rightarrow \textit{Step } \textbf{od}).A \; .$$

$$
\begin{array}{lrcll}
 & \circ\emptyset & \equiv & \underline{0} & \text{Excluded miracle, since } \sqcup\{\} = 0. \\
 & & & & \\
 & \circ\{h\}.h & = & 1/3 & \text{Flip } \textit{fat}\text{; flipping } \textit{thin} \text{ would give } 1/2. \\
 & \circ\{h\}.t & = & 0 & \text{Do nothing; flipping would give } 1/3. \\
 & \circ\{h\}.e & = & 0 & \text{Cannot leave } e. \\
 & & & & \\
 & \circ\{t\}.h & = & 1/3 & \text{Flip } \textit{fat}\text{; flipping } \textit{thin} \text{ would give } 1/2. \\
 & \circ\{t\}.t & = & 1/3 & \text{Flip; doing nothing would give } 1. \\
 & \circ\{t\}.e & = & 0 & \text{Cannot leave } e. \\
 & & & & \\
 & \circ\{e\} & \equiv & \{e\} & \text{At } \{h\} \text{ flip } \textit{thin}\text{, at } \{t\} \text{ do nothing: both avoid } e. \\
 & & & & \\
 & \circ\{h,t\}.h & = & 2/3 & \text{Flip } \textit{fat}\text{; flipping } \textit{thin} \text{ would give } 1. \\
 & \circ\{h,t\}.t & = & 1 & \text{The choice makes no difference.} \\
 & \circ\{h,t\}.e & = & 0 & \text{Cannot leave } e. \\
 & & & & \\
 * & \circ\{t,e\}.h & = & 1/2 & \text{Flip } \textit{thin}\text{; flipping } \textit{fat} \text{ would give } 2/3. \\
 & \circ\{t,e\}.t & = & 2/3 & \text{Flip; doing nothing would give } 1. \\
 & \circ\{t,e\}.e & = & 1 & \text{Cannot leave } e. \\
 & & & & \\
 & \circ\{e,h\}.h & = & 1/2 & \text{Flip } \textit{thin}\text{; flipping } \textit{fat} \text{ would give } 2/3. \\
 & \circ\{e,h\}.t & = & 0 & \text{Doing nothing remains at } t. \\
 & \circ\{e,h\}.e & = & 1 & \text{Cannot leave } e. \\
 & & & & \\
 & \circ\{h,t,e\} & \equiv & \underline{1} & \text{Termination guaranteed.}
\end{array}
$$

At $*$ we have for example

$$
\begin{array}{lll}
 & \circ\{t,e\}.h & \\
 & & \\
= & \quad\quad (\{t,e\}.h)/2 + (\{t,e\}.t)/2 & \text{Definition 3.3} \\
 & \sqcap \;\; (\{t,e\}.h)/3 + (\{t,e\}.t)/3 + (\{t,e\}.e)/3 & \\
 & & \\
= & (0/2 + 1/2) \;\sqcap\; (0/3 + 1/3 + 1/3) & \{t,e\}.h = 0 \textit{ etc.} \\
= & 1/2\ . &
\end{array}
$$

Figure 3: Coin-flipping to illustrate $\circ$: the *thin* coin gives heads or tails; the *fat* coin can land on its edge.

	$\Diamond\emptyset$	$\equiv$	$\underline{0}$	Excluded miracle.
	$\Diamond\{h\}$	$\equiv$	$\{h\}$	Do nothing at t and e.
$*$	$\Diamond\{t\}.h$	$=$	$1/2$	Flipping either coin repeatedly is guaranteed to leave h; repeating *thin* would guarantee reaching t. Repeating *fat* splits the eventual departure fairly between arriving at t and at e.
	$\Diamond\{t\}.t$	$=$	1	Already at t.
	$\Diamond\{t\}.e$	$=$	0	Cannot leave e.
	$\Diamond\{e\}$	$\equiv$	$\{e\}$	At h flip *thin*, at t do nothing; both avoid e.
	$\Diamond\{h,t\}$	$\equiv$	$\{h,t\}$	If at e, cannot leave it.
	$\Diamond\{t,e\}$	$\equiv$	$\underline{1}$	Flipping either coin repeatedly is guaranteed to leave h eventually.
	$\Diamond\{e,h\}$	$\equiv$	$\{e,h\}$	Forever do nothing at t.
	$\Diamond\{h,t,e\}$	$\equiv$	$\underline{1}$	At h,t,e already: termination not required.

At $*$ we have for example

$$\begin{array}{lll}
 & \Diamond\{t\}.h & \\
= & \{t\}.h \sqcup \circ\Diamond\{t\}.h & \text{Definition 3.4} \\
= & \begin{array}{ll} & (\Diamond\{t\}.h)/2 + (\Diamond\{t\}.t)/2 \\ \sqcap & (\Diamond\{t\}.h)/3 + (\Diamond\{t\}.t)/3 + (\Diamond\{t\}.e)/3 \end{array} & \{t\}.h = 0\text{; definition } \mathit{step} \\
= & \begin{array}{ll} & (\Diamond\{t\}.h)/2 + 1/2 \\ \sqcap & (\Diamond\{t\}.h)/3 + 1/3 \end{array} & \Diamond\{t\}.t = 1;\ \Diamond\{t\}.e = 0 \\
= & (\Diamond\{t\}.h)/3 + 1/3\ , &
\end{array}$$

whence by arithmetic we have $\Diamond\{t\}.h = 1/2$.

Figure 4: Coin-flipping: illustration of $\Diamond$.

It is the highest attainable probability over all 'strategies' G that determine whether or not to take another step in attempting to reach A. That interpretation is the same as in the standard case, where however the strategy is particularly simple: it is 'keep going as long as A does not hold', equivalently 'take G to be $\neg A$'.

The interplay of angelic and demonic nondeterminism in $\Diamond$ is significant: the choice of whether to stop or to step is made to *maximise* the expectation; but the resolution of nondeterminism during a step is made to *minimise* it.

Fig. 4 tabulates $\Diamond A.s$ for standard A and s varying over S, again in the coin example.

For proper expectations consider $\Diamond\Diamond\{t\}$. At state t we have

$$\Diamond\Diamond\{t\}.t \quad = \quad \Diamond\{t\}.t \sqcup \circ\Diamond\Diamond\{t\}.t \quad = \quad 1\ ,$$

since $\Diamond\{t\}.t = 1$. At state e we have

$$\Diamond\Diamond\{t\}.e \quad = \quad \Diamond\{t\}.e \sqcup \circ\Diamond\Diamond\{t\}.e \quad = \quad \Diamond\Diamond\{t\}.e \; ,$$

of which the least solution[8] is $\Diamond\Diamond\{t\}.e{:=}\,0$. Finally, we calculate

$$\begin{array}{lll}
 & \Diamond\Diamond\{t\}.h & \\
= & \Diamond\{t\}.h \;\sqcup\; \circ\Diamond\Diamond\{t\}.h & \text{Definition 3.4} \\[1em]
= & \begin{array}{ll} & 1/2 \\ \sqcup & \begin{array}{ll} & (\Diamond\Diamond\{t\}.h)/2 + (\Diamond\Diamond\{t\}.t)/2 \\ \sqcap & (\Diamond\Diamond\{t\}.h)/3 + (\Diamond\Diamond\{t\}.t)/3 + (\Diamond\Diamond\{t\}.e)/3 \end{array} \end{array} & \text{Fig. 4; definition } \mathit{step} \\[2.5em]
= & \begin{array}{ll} & 1/2 \\ \sqcup & \begin{array}{ll} & (\Diamond\Diamond\{t\}.h)/2 + 1/2 \\ \sqcap & (\Diamond\Diamond\{t\}.h)/3 + 1/3 \end{array} \end{array} & \Diamond\Diamond\{t\}.t = 1;\ \Diamond\Diamond\{t\}.e = 0 \\[2em]
= & 1/2 \;\sqcup\; (\Diamond\Diamond\{t\}.h + 1)/3 \; , &
\end{array}$$

whose only solution is $\Diamond\Diamond\{t\}.h{:=}\,1/2$. Thus we have

$$\Diamond\Diamond\{t\} \quad \equiv \quad \Diamond\{t\} \; ,$$

which is an instance of Lemma A.1 below (generalising Lemma 2.4).

Definition 3.5 *probabilistic always*

$$\Box A \quad := \quad (\nu X \bullet A \sqcap \circ X) \; .$$

Expectation $\Box A$ is the least expected value of A that can be realised by deciding 'demonically' ($\sqcap$) whether to take one step ($\circ X$) or to stop (A), with 'never stop' interpreted as 1 (ν). If A is standard then $\Box A$ is the greatest probability that repeated steps are guaranteed never to leave states in which A holds. ■

Both the choice of whether to stop or to step, and the resolution of nondeterminism during a step, are demonic in this case.

Fig. 5 tabulates $\Box A.s$ for standard A and s varying over S in the coin example.

For proper expectations define $A{:=}\,\{e\} \sqcup \Diamond\{t\}$, and consider $\Box A$. Expectation A is the probability that the last flip was edge or — if it was not — that tails will be flipped eventually. To calculate $\Box A$ we first consider state e, where we have

$$\Box A.e \quad = \quad 1 \sqcap \circ\Box A.e \quad = \quad \Box A.e \; ,$$

whose greatest solution is $\Box A.e{:=}\,1$.

At state h we have

[8] Here and below we will be calculating extremal solutions pointwise, which of course does not guarantee that the result *is* a solution overall. But if the result is a solution then it is an extremal one, as required; and in our examples all pointwise calculations give solutions.

	$\Box\emptyset$	$\equiv$	$\underline{0}$	Excluded miracle.
	$\Box\{h\}$	$\equiv$	$\underline{0}$	Repeated flips of either coin eventually leave h.
	$\Box\{t\}$	$\equiv$	$\underline{0}$	Repeated flips eventually leave t.
	$\Box\{e\}$	$\equiv$	$\{e\}$	Cannot leave e.
	$\Box\{h,t\}$	$\equiv$	$\underline{0}$	Repeated flips leave h,t.
	$\Box\{t,e\}.h$	$=$	0	Already not in t,e.
$*$	$\Box\{t,e\}.t$	$=$	$1/2$	Repeated flips are guaranteed to leave t eventually, then reaching e with probability $1/2$.
	$\Box\{t,e\}.e$	$=$	1	Cannot leave e.
	$\Box\{e,h\}$	$\equiv$	$\{e\}$	Repeated flips of *thin* at h are guaranteed to reach t.
	$\Box\{h,t,e\}$	$\equiv$	$\underline{1}$	Termination guaranteed.

At $*$ we have for example

$$\begin{array}{lll}
 & \Box\{t,e\}.t & \\
= & \{t,e\}.t \;\sqcap\; \circ\Box\{t,e\}.t & \text{Definition 3.5} \\
= & & \{t,e\}.t = 1\text{; definition } \textit{step} \\
 & \quad (\Box\{t,e\}.h)/3 + (\Box\{t,e\}.t)/3 + (\Box\{t,e\}.e)/3 & \\
 & \sqcap \quad \Box\{t,e\}.t & \\
= & (1/3 + (\Box\{t,e\}.t)/3) \;\sqcap\; \Box\{t,e\}.t\ , & \Box\{t,e\}.h = 0\text{; } \Box\{t,e\}.e = 1
\end{array}$$

whose greatest solution is $\Box\{t,e\}.t = 1/2$.

Figure 5: Coin-flipping: illustration of $\Box$.

$$
\begin{array}{lll}
 & \Box A.h & \\
= & \quad 1/2 & \text{Definition 3.5; Fig. 4; definition } \textit{step} \\
 & \sqcap \quad (\Box A.h)/2 + (\Box A.t)/2 & \\
 & \quad \sqcap \; (\Box A.h)/3 + (\Box A.t)/3 + (\Box A.e)/3 & \\
= & 1/2 \;\sqcap\; (\Box A.h + \Box A.t)/2 \;, & \Box A.e = 1;\ \Box A.h, \Box A.t \le 1
\end{array}
$$

whence we have trivially $\Box A.h \le 1/2$. At state t we have

$$
\begin{array}{lll}
 & \Box A.t & \\
= & \quad 1 & \text{Definition 3.5; Fig. 4; definition } \textit{step} \\
 & \sqcap \quad (\Box A.h)/3 + (\Box A.t)/3 + (\Box A.e)/3 & \\
 & \quad \sqcap \; \Box A.t & \\
\le & (1/2 + (\Box A.t)/3) \;\sqcap\; \Box A.t \;, & \Box A.e = 1;\ \Box A.h \le 1/2
\end{array}
$$

whence by arithmetic we have $\Box A.t \le 3/4$. It is easily checked from the above that the pointwise maxima

$$\Box A.h, \Box A.t, \Box A.e \quad := \quad 1/2,\ 3/4,\ 1$$

are a solution collectively, and thus give the maximal one.

The operational meaning of $\Box(\{e\} \sqcup \Diamond\{t\}).t = 3/4$ is perhaps not obvious, however; we interpret it as follows. The demon 'in $\Box$' will take repeated steps in order to minimise the expectation $\{e\} \sqcup \Diamond\{t\}$ — it will seek a state that is not e, and from which the probability of eventually reaching t is lowest. Thus the demon seeks h.

To seek h the demon flips *fat* repeatedly, but with a risk of $1/2$ that on leaving t it ends up in e instead. If it does reach h (probability $1/2$), it must hand over to an angel 'in $\Diamond$' who then tries to reach t again (probability $\Diamond\{t\}.h = 1/2$).

Thus $\Box\{e\} \sqcup \Diamond\{t\}.t$ is $1/2 \times 1$ for the demon's leaving t to end up in e directly — plus $1/2$ for leaving t to reach h times $1/2$ for the probability of the angel's subsequent return to t.

4 Properties of the model

Given the structural correspondence between the standard and probabilistic models, one would expect them to share many temporal laws. Although we do not attempt a complete axiomatisation, in this section we give a systematic presentation of the basic temporal laws, and show how with suitable choices of probabilistic 'propositional' operators ($\sqcup, \sqcap, \&$, and $\Rightarrow, \rightrightarrows$ below) the standard axioms (Fig. 1) can be generalised and proved (Fig. 7).

The basic properties of the temporal operators are summarised in Fig. 6, whose structure is as follows. The healthiness conditions generate the properties for *next*, ensuring [20] the existence of a corresponding relational probabilistic

healthiness conditions	
excluded miracle	$\circ A \ \Rrightarrow\ \underline{\sqcup A}$
monotonicity	$A \Rrightarrow B$ implies $\circ A \Rrightarrow \circ B$
scaling	$\circ(pA) \ \equiv\ p(\circ A)$
weighted sum	$\circ(A\, {}_p\!\oplus B) \ \Lleftarrow\ \circ A\, {}_p\!\oplus \circ B$
ampersand	$\circ(A \mathbin{\&} B) \ \Lleftarrow\ \circ A \mathbin{\&} \circ B$
truncation	$\circ A \ominus \underline{p} \ \Lleftarrow\ \circ A \ominus \underline{p}$
least fixed point	
fixed point	$\Diamond A \ \equiv\ A \sqcup \circ\Diamond A$
least	$A \sqcup \circ B \ \Rrightarrow\ B$ implies $\Diamond A \Rrightarrow B$
greatest fixed point	
fixed point	$\Box A \ \equiv\ A \sqcap \circ\Box A$
greatest	$A \sqcap \circ B \ \Lleftarrow\ B$ implies $\Box A \Lleftarrow B$

Figure 6: Basic properties of probabilistic temporal operators.

computation [10] to whose single step *next* refers.[9] The pairs of properties for *eventually* and *always* are the usual for extremal fixed points, determining them uniquely.

Since the probabilistic definitions of the temporal operators replace the standard $\cup, \cap$ with $\sqcup, \sqcap$ respectively, whose properties are so similar, many standard results — and their proofs — are trivially retained: Lemma 2.4 generalises to Lemma A.1 for example.

For probabilistic implication there are several choices, one of which is the trivial embedding of standard implication.

Definition 4.1 *implication* For scalars a, b define

$$a \Rightarrow b \quad := \quad 1 \ \underline{\text{if}}\ \ a{\leq}b\ \ \underline{\text{else}}\ \ 0 \ .$$

■

Another form of implication is found as the $\Rrightarrow$-adjoint of &; its utility is its (reverse) $\circ$-subdistributivity property (see Fig. 7 below), which $\Rightarrow$ does not have.

Definition 4.2 & *implication* For scalars a, b define

$$a \rightrightarrows b \quad := \quad 1 - (a \ominus b) \ ,$$

so that for expectations A, B, C we have the adjoint property

$$(A \mathbin{\&} B) \ \Rrightarrow\ C \quad \text{iff} \quad A \ \Rrightarrow\ (B \rightrightarrows C) \ .$$

■

[9] The list includes *subdistributivity of* & for convenience; but we cannot then remove *truncation*, unfortunately, even in the context of the other healthiness conditions.

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

For $*$ — $\circ$-superdistributivity of $\rightrightarrows$ — we reason

$$\begin{array}{lll}
 & \circ(A \rightrightarrows B) \;\Rrightarrow\; \circ A \rightrightarrows \circ B & \\
\text{iff} & \circ(A \rightrightarrows B) \,\&\, \circ A \;\Rrightarrow\; \circ B & \text{adjoint} \\
\text{if} & \circ((A \rightrightarrows B) \,\&\, A) \;\Rrightarrow\; \circ B & \circ\text{-subdistributivity of } \& \\
\text{if} & \circ B \;\Rrightarrow\; \circ B\;. & \text{adjoint: } (A \rightrightarrows B) \,\&\, A \Rrightarrow B
\end{array}$$

Figure 7: Probabilistic generalisation of standard axioms in Fig. 1.

With those definitions we can write probabilistic analogues of the standard axioms, listed in Fig. 7. All can be proved from the basic properties Fig. 6 and the definitions of the two implications; possibly the longest proof is of $**$.

Lemma 4.3 *always-eventually* For all expectations A, B we have

$$\Box(A \rightrightarrows B) \,\&\, \Diamond A \quad \Rrightarrow \quad \Diamond B\;.$$

Proof

$$\begin{array}{lll}
 & \Box(A \rightrightarrows B) \,\&\, \Diamond A \;\Rrightarrow\; \Diamond B & \\
\text{iff} & \Diamond A \;\Rrightarrow\; \Box(A \rightrightarrows B) \rightrightarrows \Diamond B & \text{adjoint} \\
 & & \\
\text{if} & \quad A \sqcup \circ(\Box(A \rightrightarrows B) \rightrightarrows \Diamond B) & \textit{least}\text{ property of } \Diamond A \\
 & \Rrightarrow\; \Box(A \rightrightarrows B) \rightrightarrows \Diamond B & \\
 & & \\
\text{iff} & \qquad A \sqcup \circ(\Box(A \rightrightarrows B) \rightrightarrows \Diamond B) & \text{adjoint} \\
 & \quad \& \;\; \Box(A \rightrightarrows B) & \\
 & \Rrightarrow\; \Diamond B & \\
 & & \\
\text{iff} & \qquad A \,\&\, \Box(A \rightrightarrows B) & \text{distribute } \sqcup \text{ through } \& \\
 & \quad \sqcup \;\; \circ(\Box(A \rightrightarrows B) \rightrightarrows \Diamond B) \,\&\, \Box(A \rightrightarrows B) & \\
 & \Rrightarrow\; \Diamond B & \\
 & & \\
\text{iff} & \qquad A \,\&\, \Box(A \rightrightarrows B) & \textit{fixed-point}\text{ property of } \Diamond B \\
 & \quad \sqcup \;\; \circ(\Box(A \rightrightarrows B) \rightrightarrows \Diamond B) \,\&\, \Box(A \rightrightarrows B) & \\
 & \Rrightarrow\; B \sqcup \circ\Diamond B &
\end{array}$$

if $\qquad A \mathbin{\&} \Box(A \rightrightarrows B) \;\Rrightarrow\; A \mathbin{\&} (A \rightrightarrows B) \;\Rrightarrow\; B$

$\qquad \circ(\Box(A \rightrightarrows B) \rightrightarrows \Diamond B) \;\&\; \Box(A \rightrightarrows B)$

$\Rrightarrow\; \circ\Diamond B$

if $\qquad \circ(\Box(A \rightrightarrows B) \rightrightarrows \Diamond B) \qquad\qquad \Box(A \rightrightarrows B) \;\Rrightarrow\; \circ\Box(A \rightrightarrows B)$

$\qquad \&\; \circ\Box(A \rightrightarrows B)$

$\Rrightarrow\; \circ\Diamond B$

if $\qquad \circ((\Box(A \rightrightarrows B) \rightrightarrows \Diamond B) \mathbin{\&} \Box(A \rightrightarrows B))$ $\qquad$ $\circ$-subdistributivity of &

$\Rrightarrow\; \circ\Diamond B$

if $\qquad \circ\Diamond B \;\Rrightarrow\; \circ\Diamond B\ .$ $\qquad$ monotonicity; adjoint

■

Our generalisation of Ben-Ari's laws establishes that the operational intuitions underlying standard branching-time temporal logic apply also to the quantitative logic. The real surprise however lies in our choice of operators; specifically our insistence on two kinds of 'probabilistic implication' reveals the operational principles communicated by the laws in Fig. 1, and we conclude this section with a brief examination of what they are.

The axioms in Fig. 7 (and in Fig. 1) essentially fall into two classes: those which combine quantities 'conjunctively' (indicated by the $\lhd$ symbol in the Fig. 7) and those which are designed to be more specific about the operational meaning of the temporal operators in relation to 'next'.

Considering the former kind we find exclusive use of & and its adjoint $\rightrightarrows$. Recall from Fig. 6 that & generalises ordinary (Boolean) conjunction to the probabilistic context; thus its appearance here is explained once we notice that the purpose of the $\lhd$-indicated laws is to set out appropriate ways of combining probabilities.

The remaining two laws (without $\lhd$ in the figure) require the introduction of $\Rrightarrow$, our alternative generalisation of implication; and by taking a closer look at the laws' operational motivation we see why. Considering the fourth law from Fig. 7 we notice that the expression '$A \Rrightarrow \circ A$' defines a $\{0,1\}$-valued expectation (and thus corresponds to a predicate). Used as a guard in the loop

$$\mathbf{do}\ (A \Rrightarrow \mathrm{wp}.\mathit{Step}.A) \;\rightarrow\; \mathit{Step}\ \mathbf{od}\ ,$$

we obtain the operational interpretation of $\Box(A \Rrightarrow \circ A)$ using a *greatest* fixed point semantics for the loop (compare Sec. 2), when we instantiate $\circ$ by wp.*step*. With A standard, the effect is to select the proportion of paths in which $A \Rrightarrow \circ A$ ('the probability that if A holds now then next time it certainly holds') is always true. The law then states that if, in addition, A holds initially ('A &' in the formula) then A itself must *always* hold along the selected paths, and as such correctly encodes the relationship between 'next' unfoldings and the desired temporal interpretation for $\Box A$. Similar operational interpretations have

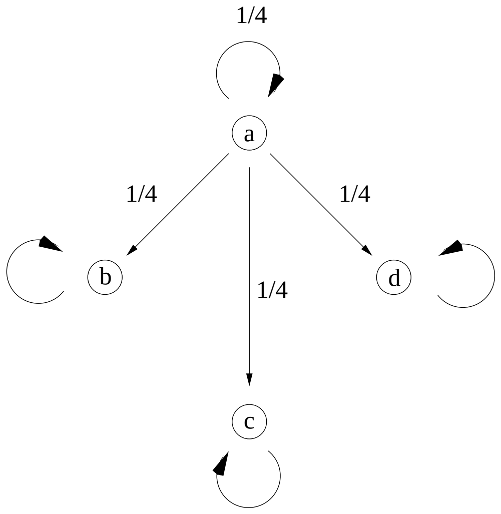

Figure 8: Transition system showing necessity of operators chosen

been explored elsewhere [19]. Attempting to find any operational relationship between the alternative $A \mathbin{\&} \Box(A \rightrightarrows \circ A)$ and $\Box A$ has proved to be fruitless.

In spite of the above explanations, one might nevertheless be tempted to experiment by replacing & by $\sqcap$ and $\rightrightarrows$ by $\Rightarrow$ in Fig. 7; the hope would be to obtain a set of stonger laws using fewer operators, since the inequalities

$$A \mathbin{\&} B \;\Rrightarrow A \sqcap B \quad \text{and} \quad A \Rightarrow B \;\Rrightarrow\; A \rightrightarrows B \tag{4}$$

(holding for all expectations A, B over S) would supply tighter relationships between probabilistic expressions than those set out in Fig. 7. We present a trivial example to illustrate the failure of such experiments.

Consider the transition diagram set out in Fig. 8 which describes a single computation step; we interpret $\circ$ as that step, in the temporal formulae.

We take as our example an attempted strengthening of ** in Fig. 7 by showing that

$$\Box(\{b,c\} \rightrightarrows \{c\}) \sqcap \Diamond\{b,c\} \quad \Rrightarrow \quad \Diamond\{c\}$$

does *not* hold for the system of Fig. 8. We compare the left-hand side, a lower bound on the probability that both $\{b,c\}$ 'implies' $\{c\}$' always holds 'and' $\{b,c\}$ eventually holds, with the right-hand side, the probability that $\{c\}$ eventually holds. We now reason

$$\begin{array}{lll}
 & \Box(\{b,c\} \rightrightarrows \{c\}) \sqcap \Diamond\{b,c\} & \\
\equiv & \Box(\underline{1} - \{b\}) \sqcap \Diamond\{b,c\} & \text{Definition 4.2} \\
\equiv & (2\{a\}/3 + \{c,d\}) \sqcap (2\{a\}/3 + \{b,c\}) & \text{Fig. 8; Defs. 3.4, 3.5}
\end{array}$$

$$\begin{array}{lll}
\equiv & 2\{a\}/3 + \{c\} & \\
\not\Rrightarrow & \{a\}/3 + \{c\} & \\
\equiv & \Diamond\{c\}\ . & \text{Fig. 8; Definition 3.4}
\end{array}$$

On the other hand combining the probabilities with & (on the left) correctly is comparable to $\Diamond\{c\}$:

$$\begin{array}{lll}
 & (2\{a\}/3 + \{c, d\})\ \&\ (2\{a\}/3 + \{b, c\}) & \\
\equiv & \{a\}/3 + \{c\} & \text{Definition 3.1} \\
\equiv & \Diamond\{c\}\ . &
\end{array}$$

Similarly, replacing $\Rightarrow$ by $\rightrightarrows$ in the fourth axiom in Fig. 7 is incorrect:

$$\{a, b\}\ \&\ \Box(\{a, b\} \rightrightarrows \circ\{a, b\}) \quad \Rrightarrow \quad \Box\{a, b\}$$

does *not* hold. We have

$$\begin{array}{lll}
 & \{a, b\}\ \&\ \Box(\{a, b\} \rightrightarrows \circ\{a, b\}) & \\
\equiv & \{a, b\}\ \&\ \Box(\{a, b\} \rightrightarrows \{a\} + \{b\}/2) & \text{Fig. 8; Definition 3.3} \\
\equiv & \{a, b\}\ \&\ \Box(\underline{1} - \{b\}/2) & \text{Definition 4.2} \\
\equiv & \{a, b\}\ \&\ (\underline{1} - \{b\}/2) & \text{Fig. 8; Definition 3.5} \\
\equiv & \{a\} + \{b\}/2 & \text{Definition 3.1} \\
\not\Rrightarrow & \{a\} + \{b\}/3 & \\
\equiv & \Box\{a, b\}\ . & \text{Fig. 8; Definition 3.5}
\end{array}$$

5 Examples: demonic random walker

We conclude our presentation with an example combining demonic nondeterminism, explicit numeric premises and an explicit numeric conclusion.

The *unbounded random walk* [7] treats a (Markov) process that moves up or down in discrete steps with certain probabilities. We consider a 'demonic' walker whose transition probabilities are uncertain: our premise is that the up and the down transition each are taken with probability at least 1/3; our conclusion will be that the walker moves up (or down) *eventually* with probability u at least $(3 - \sqrt{5})/2$, and that the *recurrence* probability r of the walker's eventually returning to his starting position is at least $1 - \sqrt{5}/3$.

In summary we use the elementary argument that u is at least 1/3, for an immediate move up, plus $u^2/3$ for an immediate move down followed by two eventual moves up: then the least solution of $u \geq (u^2 + 1)/3$ is our quoted $(3 - \sqrt{5})/2$; and finally r is calculated from u. Our treatment below with the modal operators thus will formalise that the probabilities may be added that way, that u is independent of the starting position, that the eventualities may be composed, and that r is determined by u.

5.1 The demonic walker

We begin with the premise: a specification of the walker. Take the state space S to be the integers $\mathbb{Z}$, so that expectations are of type $\mathbb{Z} \to [0,1]$. For integer s and expectation A we capture the walker's step-by-step behaviour by the inequation for all states s and expectations A that

$$\circ A.s \quad \geq \quad A.(s{-}1)/3 \;+\; A.(s{+}1)/3\;. \tag{5}$$

The walker is nondeterministic in the sense that the probabilities are not given exactly — that in (5) they are only bounded below — and demonic in the sense that our reasoning will hold even if the walker uses the freedom allowed by (5) to make the probability of eventually moving up as low as possible.

Let $\Diamond\{s{+}1\}.s$ be u (for *up*). We have

$$\begin{array}{lll}
 & u & \\
= & \Diamond\{s{+}1\}.s & \text{definition } u \\
= & \{s{+}1\}.s \;\sqcup\; \circ\Diamond\{s{+}1\}.s & \text{Definition 3.4} \\
\geq & \Diamond\{s{+}1\}.(s{-}1)/3 + \Diamond\{s{+}1\}.(s{+}1)/3 & \{s{+}1\}.s = 0\text{; from (5)} \\
= & (\Diamond\{s{+}1\}.(s{-}1))/3 + 1/3 & \Diamond\{s{+}1\}.(s{+}1) = 1 \\
= & (\Diamond\Diamond\{s{+}1\}.(s{-}1))/3 + 1/3 & \text{Lemma A.1} \\
\geq & \Diamond u\{s\}.(s{-}1)/3 + 1/3 & \text{see below; Lemma A.3: } \Diamond \textit{ monotonicity} \\
= & u(\Diamond\{s\}.(s{-}1))/3 + 1/3 & \text{Lemma A.5: } \Diamond \textit{ scaling} \\
\geq & u^2/3 + 1/3\;, & \Diamond\{s\}.(s{-}1) \text{ is } u \text{ also}^{10}
\end{array}$$

giving $u \geq (u^2+1)/3$ as promised.

For the deferred justification we note that for any expectation A we have

$$A \quad \Lleftarrow \quad A.s \times \{s\}$$

since the right-hand side is just $A.s$ at s and 0 elsewhere; in the proof we used $\Diamond\{s{+}1\} \;\Lleftarrow\; \Diamond\{s{+}1\}.s \times \{s\}$.

A similar proof establishes $\Diamond\{s{-}1\}.s = u$ also; and we can then bound the probability of eventual return by reasoning

$$\circ\Diamond\{s\}.s \quad \geq \quad \Diamond\{s\}.(s{-}1)/3 + \Diamond\{s\}.(s{+}1)/3 \quad = \quad 2u/3 \quad = \quad 1 - \sqrt{5}/3\;.$$

5.2 The demonic stumbler

Now we consider a generalisation: suppose that instead of (5) we have the weaker specification

$$\Diamond A.s \quad \geq \quad A.(s{-}1)/3 + A.(s{+}1)/3\;, \tag{6}$$

[10] That follows from Lemma A.2 considering monotonic transformers $(\downarrow k)$ defined

$$(A{\downarrow}k).s \quad := \quad A.(s{-}k)$$

for integer k: using $t := (\downarrow s)$ shows that $\Diamond\{s{+}1\}.s = \Diamond\{1\}.0$ for all s.

in which $\circ A$ is replaced on the left by $\Diamond A$. It is satisfied for example by a random *stumbler* who on each step with some probability remains where he is: but when he eventually does move, it is with probability at least 1/3 in each direction. (Taking $A:=\{s{-}1\}$ and $A:=\{s{+}1\}$ in (6) implies that.)

Analysis of the stumbler is almost as for the walker, beginning however with

$$\begin{array}{lll} & \Diamond\{s{+}1\}.s & \\ = & \Diamond\Diamond\{s{+}1\}.s & \text{Lemma A.1} \\ \geq & \Diamond\{s{+}1\}.(s{-}1)/3 + \Diamond\{s{+}1\}.(s{+}1)/3\ . & \text{from (6)} \end{array}$$

We then reason as before to the same conclusion at no 'extra cost'.

The stumbler example exposes an important aspect of our specifications: the walker could have been specified as two statements separately, for all s that

$$\begin{array}{rl} \circ\{s{+}1\}.s \ \geq\ 1/3 & \text{the walker moves up with probability at least 1/3 and} \\ \circ\{s{-}1\}.s \ \geq\ 1/3 & \text{the walker moves down with probability at least 1/3.} \end{array}$$

But specifying the stumbler similarly would be wrong: the conditions

$$\begin{array}{rl} \Diamond\{s{+}1\}.s \ \geq\ 1/3 & \text{the walker \textit{eventually} moves up, with probability at least 1/3 and} \\ \Diamond\{s{-}1\}.s \ \geq\ 1/3 & \text{the walker \textit{eventually} moves down, with probability at least 1/3} \end{array} \tag{7}$$

are strictly weaker than (6) because they allow stumblers that 'piggyback' — that reach $s{-}1$ only after having visited $s{+}1$ on the way. And for them the conclusion $r \geq 1-\sqrt{5}/2$ is not valid.

6 Conclusions

Our contribution is the reinterpretation of fixed-point logic — the modal μ-calculus — over expectation- rather than predicate transformers, and a determination of how the standard operators should be embedded in the expanded framework:

- Sec. 3.2 showed how the probabilistic healthiness conditions for expectation transformers [20] give the proper generalisations of the propositional operators;

- Sec. 3.3 used operational arguments [19] to generalise the Boolean modalities to expectations, and explained how they can be extended still further to describe various probabilistic 'gambling games' involving demonic and angelic choice, with the values of the formulae being the expected reward gained from playing the game.

- Sec. 4 (Fig. 7) establishes the reasoning principles analogous to those for standard temporal logic, when the operators are restricted to the usual modalities $\circ$, $\Diamond$ and $\Box$. The postulated axioms for $\circ$ — characterising probabilistic transitions — facilitate proofs of the laws, whilst our use of probabilistic conjunction rather than some other generalisation of ordinary conjunction retains modular reasoning, even for quantitative information.[11]

- Sec. 5 demonstrates those principles in practice, especially where the result depends on explicit probabilities.

A logic built over that interpretation [19] thus has the advantages of specialising smoothly to the standard case, giving quantitative results where desired yet via the *0-1 Law* [25, 18] allowing explicit probabilities to be discarded if irrelevant[12], having reasoning principles that generalise familiar ones and finally offering the possibility of new applications, beyond strict temporal logic, to probabilistic games, together with a framework for the direct calculation of expected quantities such as space or time complexity [16].

Finally the greater distinguishing power of $[0,1]$ over $\{0,1\}$ also has compelling implications for specification — the use of (5) for example illustrates how quantitative temporal properties may be expressed in a manner both pleasingly succinct and well-suited for reasoning.

Our emphasis has been on reasoning rather than (for example) on model checking. Huth and Kwiatkowska [12] have interpreted the modal μ-calculus as we do, and take a complementary approach: they show for non-demonic systems that the expectation formulae can be checked by reducing the problem to linear programming or in some cases to simple Gaussian elimination. They establish also that the equivalence induced between formulae by the expectation interpretation lies between probabilistic bisimulation and probabilistic ready bisimulation.

There may also be a connection between model checking and the gambling-game view [26, 19].

The approach of *pCTL* (but not *pCTL**) [3] is close to ours in the following sense. Omit *pCTL*'s operators **A** and **E** (expressing absolute judgements rather than extremal probabilities), and consider only the $\mathbb{P}_{\geq p}$-form of probability measures.[13] Then a *pCTL* state-formula is true in just those states in which the 'equivalent' expectation formula takes the value 1, where the expectation formula is obtained by

- replacing the propositional operators $\vee, \wedge, \neg$ by the arithmetic $\sqcup, \sqcap, (1-)$ respectively,

[11] Adding *unless* and/or *until* as (binary) expectation transformers is also possible [19], and more standard properties can then be generalised. We omitted it here for brevity.

[12] We use probabilistic *unless* [19, written $\rhd$ there], and the *0-1 law* becomes

If B is standard and $p(A \rhd B) \Rrightarrow \Diamond B$ for some nonzero p, then $A \rhd B \Rrightarrow \Diamond B$.

[13] The fact that we use *eventually* and *always* rather than *until* is not important.

- leaving the modal operators as they are and
- replacing $\mathbb{P}_{\geq p}$ by $(\underline{p} \Rightarrow)$, as in Definition 4.1,

at all levels of the *pCTL* formula. Thus for example the *pCTL* judgement $\mathbb{P}_{\geq p}\Diamond A$ — expressing that (standard) A will be established eventually with probability at least p — becomes $\underline{p} \Rightarrow \Diamond A$ (where we interpret A as a characteristic function).

Huth and Kwiatkowska establish similar correspondences, but for different sets of formulae: in their Theorem 1 [12] they show that the 'optimistic' view (in our terms the ceiling $\lceil\cdot\rceil$) distributes through any positive existential formula, and that the 'pessimistic' view ($\lfloor\cdot\rfloor$)) distributes through universal formulae.

Moving to *pCTL** however we find that there the logics diverge. For example we cannot translate

$$\mathbb{P}_{\geq p}\ (\Diamond A\ \wedge\ \Diamond B)$$

directly into expectations, because there is no equivalent operator acting between expectations (just numbers) in the way that $\wedge$ acts between path formulae, that contain so much more information. To write as above 'the probability is at least p that both A will be established eventually and B will be established eventually' we would proceed from first principles, thinking of the probability of winning a suitable game:

- if A and B are both false then take a step;
- if one is true but not the other, then take a step but subsequently seek only the other; and
- if both are true then stop (and win).

The expectation formula is thus

$$\underline{p} \quad \Rightarrow \quad \Diamond((A \sqcap \Diamond B)\ \sqcup\ (B \sqcap \Diamond A))\ .$$

There may be a more general translation process, based on explicit access to the game interpretations of the modal operators [19]; and it does seem that simple propositional-free formulae carry over even if they are not in *pCTL*. For example

$$\mathbb{P}_{\geq p}\Box\Diamond A \quad \text{and} \quad \underline{p} \Rightarrow \Box\Diamond A$$

are equivalent for standard A, both expressing that with probability at least p the predicate A is established infinitely often. Those are topics for further study.

Finally, our treatment of nondeterminism does not explicitly mention a scheduler [24, 3] because it does not have to: the (demonic) schedule is built-in to the semantics [20] of expectation transformers. (Recall the infimum used in (2).) A *probabilistic* scheduler [3], able to interpolate between discrete choices, corresponds to the probabilistic (convex) closure condition of He [10]. To treat the existential duals $\exists X$, $\exists F$ and $\exists G$, we would allow both demonic and angelic nondeterminism in *step*: as in the standard case, the existential modalities are obtained via a double complementation. The impact of that on the healthiness conditions in that case is discussed elsewhere [17].

Acknowledgements

We thank our hosts in Israel, in particular David Harel, Orna Grumberg and Yishai Feldman, for allowing us to present this material to them and for their comments, Michael Huth and Marta Kwiatkowska for our interesting discussions on the use of expectations in modal logic and Jeff Sanders for his involvement in all aspects of this work.

References

[1] A. Aziz, V. Singhal, F. Balarin, R.K. Brayton, and A.L. Sangiovanni-Vincentelli. It usually works: The temporal logic of stochastic systems. In *Computer-Aided Verification, 7th Intl. Workshop*, number 939 in LNCS. Springer Verlag, 1995.

[2] M. Ben-Ari, A. Pnueli, and Z. Manna. The temporal logic of branching time. *Acta Informatica*, 20:207–226, 1983.

[3] Andrea Bianco and Luca de Alfaro. Model checking of probabilistic and nondeterministic systems. In *Foundations of Software Technology and Theoretical Computer Science*, number 1026 in LNCS, pages 499–512, December 1995.

[4] E.W. Dijkstra. *A Discipline of Programming.* Prentice Hall International, Englewood Cliffs, N.J., 1976.

[5] 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.

[6] Yishai A. Feldman and David Harel. A probabilistic dynamic logic. *J. Computing and System Sciences*, 28:193–215, 1984.

[7] G. Grimmett and D. Welsh. *Probability: an Introduction.* Oxford Science Publications, 1986.

[8] H. Hansson and B. Jonsson. A logic for reasoning about time and probability. *Formal Aspects of Computing*, 6(5):512–535, 1994.

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

[10] Jifeng He, K. Seidel, and A. K. McIver. Probabilistic models for the guarded command language. *Science of Computer Programming*, 28:171–192, 1997.

[11] Wim H Hesselink. *Programs, Recursion and Unbounded Choice.* Number 27 in Cambridge Tracts in Theoretical Computer Science. Cambridge University Press, Cambridge, U.K., 1992.

[12] Michael Huth and Marta Kwiatkowska. Quantitative analysis and model checking. To appear in LICS '97, March 1997.

[13] D. Kozen. Semantics of probabilistic programs. *Journal of Computer and System Sciences*, 22:328–350, 1981.

[14] D. Kozen. A probabilistic PDL. In *Proceedings of the 15th ACM Symposium on Theory of Computing*, New York, 1983. ACM.

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

[16] A.K. McIver. Quantitative program logic and efficiency in probabilistic distributed algorithms. Technical report. See QLE98 at *http* [22].

[17] Annabelle McIver and Carroll Morgan. Probabilistic predicate transformers: part 2. Technical Report PRG-TR-5-96, Programming Research Group, March 1996. Available at [22].

[18] 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.

[19] 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 [22].

[20] Carroll Morgan, Annabelle McIver, and Karen Seidel. Probabilistic predicate transformers. *ACM Transactions on Programming Languages and Systems*, 18(3):325–353, May 1996.

[21] J. M. Morris. Temporal predicate transformers and fair termination. *Acta Informatica*, 27:287–313, 1990.

[22] PSG. Probabilistic Systems Group: Collected reports.
`http://www.comlab.ox.ac.uk/oucl/groups/probs/bibliography.html`.

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

[24] Roberto Segala and Nancy Lynch. Probabilistic simulations for probabilistic processes. In B. Jonsson and J. Parrow, editors, *CONCUR '94*, number 836 in LNCS.

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

[26] Colin Stirling. Local model checking games. In *CONCUR 95*, number 962 in LNCS, pages 1–11. Springer Verlag, 1995. Extended abstract.

[27] 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 Further lemmas for *eventually*

Lemma A.1 *probabilistic double eventually* For all expectations A we have

$$\Diamond\Diamond A \quad \equiv \quad \Diamond A \ .$$

Proof Replace $\subseteq$ by $\Rrightarrow$ in the proof of Lemma 2.4. ■

Lemma A.2 *data refinement* If for any monotonic transformer t we have

$$\circ(t.A) \ \Rrightarrow \ t.(\circ A)$$

for all expectations A, then also

$$\Diamond(t.A) \quad \Rrightarrow \quad t.(\Diamond A)$$

for all A.

Proof We reason

$$\begin{array}{lll}
 & \Diamond(t.A) \quad \Rrightarrow \quad t.(\Diamond A) & \\
\text{if} & t.A \ \sqcup \ \circ t.(\Diamond A) \quad \Rrightarrow \quad t.(\Diamond A) & \Diamond(t.A) \ \textit{least} \\
\text{if} & t.A \ \sqcup \ t.(\circ\Diamond A) \quad \Rrightarrow \quad t.(\Diamond A) & \text{assumption} \\
\text{if} & t.(A \sqcup \circ\Diamond A) \quad \Rrightarrow \quad t.(\Diamond A) & t \ \text{monotonic} \\
\text{iff} & t.(\Diamond A) \quad \Rrightarrow \quad t.(\Diamond A) \ . & \text{Definition 3.4}
\end{array}$$

■

Lemma A.3 $\Diamond$ *monotonicity* For all expectations A, B we have

$$A \ \Rrightarrow \ B \quad \text{implies} \quad \Diamond A \ \Rrightarrow \ \Diamond B \ .$$

Proof Again use $\Diamond A$ *least*, and check that

$$\begin{array}{lll}
 & A \ \sqcup \ \circ\Diamond B & \\
\Rrightarrow & B \ \sqcup \ \circ\Diamond B & A \Rrightarrow B \\
\equiv & \Diamond B \ , &
\end{array}$$

as required. ■

Lemma A.4 $\Diamond$ *excluded miracle* For all expectations A we have

$$\Diamond A \quad \Rrightarrow \quad \underline{\sqcup A}\ .$$

Proof Use $\Diamond A$ *least*, and check that

$$\begin{array}{lll}
 & A \ \sqcup\ \circ\underline{\sqcup A} & \\
\Rrightarrow & A \ \sqcup\ \underline{\sqcup\underline{\sqcup A}} & \circ\ \textit{excluded miracle} \\
\equiv & \underline{\sqcup A}\ . &
\end{array}$$

■

Lemma A.5 $\Diamond$ *scaling* For all expectations A and scalars p in $[0,1]$ we have

$$\Diamond(pA) \quad \equiv \quad p(\Diamond A)\ .$$

Proof We prove $\Diamond(pA) \Rrightarrow p(\Diamond A)$ first, using $\Diamond(pA)$ *least* and checking

$$\begin{array}{lll}
 & pA \ \sqcup\ \circ(p(\Diamond A)) & \\
\equiv & pA \ \sqcup\ p(\circ\Diamond A) & \circ\ \textit{scaling} \\
\equiv & p(A \ \sqcup\ \circ\Diamond A) & \\
\equiv & p(\Diamond A)\ . &
\end{array}$$

For $\Diamond(pA) \Lleftarrow p(\Diamond A)$ note first that it is trivial when $p = 0$. For $p > 0$ we prove equivalently $(\Diamond(pA))/p \Lleftarrow \Diamond A$, where Lemma A.4 guarantees well-definedness of the left-hand side:

$$(\Diamond(pA))/p \quad \Rrightarrow \quad \underline{\sqcup(pA)}/p \quad \Rrightarrow \quad \underline{p}/p \quad \equiv \quad \underline{1}\ .$$

Then using $\Diamond A$ *least*, we check

$$\begin{array}{lll}
 & A \ \sqcup\ \circ((\Diamond(pA))/p) & \\
\equiv & A \ \sqcup\ (p/p)(\circ((\Diamond(pA))/p)) & p \neq 0 \\
\equiv & A \ \sqcup\ (\circ(p(\Diamond(pA))/p))/p & \circ\ \textit{scaling} \\
\equiv & A \ \sqcup\ (\circ\Diamond(pA))/p & \\
\equiv & (pA \ \sqcup\ \circ\Diamond(pA))/p & p \neq 0 \\
\equiv & \Diamond(pA)/p\ . &
\end{array}$$

■