Programming Research Group

AN EXPECTATION-TRANSFORMER MODEL FOR PROBABILISTIC TEMPORAL LOGIC

Carroll Morgan and Annabelle McIver

PRG-TR-20-97

Oxford University Computing Laboratory
Wolfson Building, Parks Road, Oxford OX1 3QD

An expectation-transformer model for probabilistic temporal logic

Carroll Morgan and Annabelle McIver*

24 April 1997

Abstract

We reinterpret the modal μ-calculus [16] to act over expectations rather than predicates, where *expectations* generalise predicates by taking states into the interval $[0,1]$ rather than the two-point set $\{0,1\}$; our interest is in the idioms of the μ-calculus that correspond to operators of temporal logic, in particular in establishing reasoning principles for them.

Our model includes both probabilistic and demonic choice, and the interpretation exploits the characterisation [20] of probabilistic healthiness for expectation transformers to determine the algebraic properties of probabilistic *next*, and thence those of the other probabilistic temporal operators.

The results confirm that many nonprobabilistic temporal axioms have close probabilistic analogues, and that they can indeed be used for quantitative reasoning about probabilistic behaviour. Often the proofs are just generalisations of the original nonprobabilistic versions. In the μ-calculus more generally the new interpretation may be useful for describing 'gambling games' containing demonic, angelic and probabilistic choice.

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

1 Introduction

Since Pnueli [22] 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 allowed in the computation, and validity of formulae is 'with probability 1' [17, 10, 23]. The *0-1 law* of Sharir, Pnueli and Hart [26] shows that there are many systems in which such validity depends only on the transition probabilities' being nonzero, and not on their precise values.

Other approaches address explicit probabilities, but until recently only at the cost of disallowing demonic nondeterminism [7, 6].

*Both authors are members of the Programming Research Group at Oxford University: Wolfson Building, Parks Road, Oxford OX1 3QD, {*carroll, anabel*}@*comlab.ox.ac.uk*. McIver is supported by the EPSRC.

Recent work by Bianco and de Alfaro [3], based on the *pCTL* of Aziz *et. al.* [1] and ultimately ideas of Hansson and Jonsson [9], 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 properties that hold 'with probability at least (or at most) p'.

Our contribution is to propose a model and interpretation for a 'temporal logic of expectations' with the same scope — explicit probability and demonic nondeterminism — but of quite a different nature.[1] The model is the now-common 'sets of probability distributions' transition system [3, 25, 23], based in our case on an extension of Kozen's model [14] for probabilistic sequential computation: Jifeng He *et. al.* [11] add demonic choice in a way distinguished from others by its imposition of certain closure conditions[2] on the distribution sets. The conditions are important for reasoning and refinement in general (and determine the properties (Fig. 6) of the probabilistic *next* operator).

Our proposed interpretation is based on Kozen's 'expectation transformers' [15] (generalising predicate transformers [4]), as adapted by Morgan *et. al.* [20] to act over He's rather than Kozen's model. The closure conditions generate 'probabilistic healthiness conditions' [20, Fig. 4 p342, also Fig. 2 here], generalising Dijkstra's conditions [4].

We do not formally present a logic, preferring to concentrate on semantic issues at this stage.

To examine the special case of the temporal operators, we define $\circ$ (*next*) to act as an expectation transformer; the properties of $\circ$ in general are then exactly the probabilistic healthiness conditions, generalising the join-distribution of a modal algebra. The temporal operators $\diamond$ (*eventually*) and $\Box$ (*always*) are defined as least- and greatest fixed points, in the style of fixpoint logics [5, 16], and their properties are just the usual characterisation for those.

The novel properties of $\circ$ (together with the fixed-point properties of $\diamond$ and $\Box$) are what makes it possible in many cases to give very straightforward proofs of probabilistic temporal identities — often they are simply replayings of standard proofs in the new setting.

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; Sec. 4 examines properties of the model and investigates the identities it supports; and Sec. 5 treats the symmetric random walk, a simple situation in whose analysis explicit probabilities play a key role.

In Sec. 6 we examine the benefits and limitations of using expectations, and discuss how our proposal relates to other approaches, in particular to *pCTL* and *pCTL** [1, 3].

[1] The same proposal is made independently, for the deterministic case, by Huth and Kwiatkowska [13], who address model checking. We return to their work in the conclusion.

[2] They are *up-closure*, allowing refinement of divergence, and *probabilistic (convex) closure*, allowing demonic choice to be refined by probabilistic choice. Morgan *et. al.* [20] add *Cauchy closure*, representing bounded nondeterminism (equivalently continuity).

We write $f.x$ for function f applied to argument x, left-associative and binding more tightly than all except modal operators; and $this := that$ 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** $step.\emptyset = \emptyset$,
>
> **monotonicity** if $A \subseteq B$ then $step.A \subseteq step.B$ and
>
> **positive conjunctivity** $step.(A \cap B) = step.A \cap step.B$,

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.[3]

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] 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 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* 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. ∎

[3] 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 $step.S = S$.

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

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

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 note the correspondence with branching-time temporal logic, via the isomorphism [12] 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 terminates just from those state in 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.

A similar justification can be given for $\Box A$.

Axiomatically, we note that Definitions 3.3–3.5 have all the properties[4] listed in Fig. 1; as a further illustration we give a direct proof of the following familiar fact.

Lemma 2.4 *double eventually*

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

[4]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 only as examples of what is reasonable for a model.

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 [7] or to add probabilistic choice while retaining demonic nondeterminism [11, 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.

Expectation transformers are due to Kozen [15] 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 [14]:

> 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 [15] was extended to include nondeterminism by He [11], where programs are functions from initial state to *sets* of final distributions with certain closure conditions. Morgan [20] shows that model to correspond to the healthy expectation transformers.[5] 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

[5] Morgan [20] imposes an additional constraint of finiteness of S, which is weakened to continuity of *step* by McIver [18] when S is infinite. Neither constraint is needed here.

to post-expectation A is defined:

$$\mathrm{wp}.prog.A.s \quad := \quad (\sqcap D\colon prog.s \bullet \int_D A) \ . \tag{2}$$

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 $S \to \{0,1\}$, 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 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.

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 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

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

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

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

the probability 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

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

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

Figure 2: Probabilistic healthiness conditions [20].

allow the proof of many algebraic laws over programs — for example, *positive conjunctivity* shows that nondeterminism right-distributes over sequential composition.

For probabilistic programs the healthiness conditions serve the same purposes, and in particular lead directly to the characterisation of probabilistic *next* (Fig. 6 below). That in turn allows us to prove probabilistic analogues, for the other operators as well, of the standard properties in Fig. 1. (The probabilistic versions are given in Fig. 7.)

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

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

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

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

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

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.

A straightforward analogue of conjunction is minimum $\sqcap$, but 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.

It turns out that the generalisation of positive conjunctivity is subdistributivity of &.

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

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

■

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

$$step.(A \,\&\, B) \quad \Leftarrow \quad step.A \;\&\; step.B \ ,$$

for all expectations A, B.

Proof:

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

■

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

For 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 of* & because on standard expectations & and $\sqcap$ agree. Hence positive conjunctivity for standard transformers indeed follows from their probabilistic healthiness.

3.3 A probabilistic model

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 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

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

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. ■

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

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

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

At $*$ we have for example

$$
\begin{array}{lll}
 & \circ\{t,e\}.h & \\[0.5em]
= & \quad (\{t,e\}.h)/2 + (\{t,e\}.t)/2 & \text{Definition 3.3} \\
 & \sqcap \; (\{t,e\}.h)/3 + (\{t,e\}.t)/3 + (\{t,e\}.e)/3 & \\[0.5em]
= & (0/2 + 1/2) \;\sqcap\; (0/3 + 1/3 + 1/3) & \{t,e\}.h = 0 \; \mathit{etc.} \\
= & 1/2\ . &
\end{array}
$$

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

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

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

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

of which the least solution[6] is $\Diamond\Diamond\{t\}.e := 0$. Finally, we calculate

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

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 (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

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

[6]Here and below we will be calculating extremal solutions pointwise, which 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.

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

At $*$ we have for example

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

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

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

$$= \quad 1/2 \sqcap (\Box A.h + \Box A.t)/2 \;, \qquad \Box A.e = 1;\ \Box A.h, \Box A.t \le 1$$

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

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

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 them to share many temporal laws: indeed their axiomatisations should be similar. Although we do not attempt an 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, whoe structure is as follows. The healthiness conditions generate the properties for *next*, ensuring [20] the existence of a corresponding relational probabilistic computation [11] to whose single step *next* refers.[7] The pairs of properties for *eventually* and *always* are the usual for extremal fixed points, determining them uniquely.

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

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	$\circ(A \,\&\, B) \;\Lleftarrow\; \circ A \,\&\, \circ B$
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.

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

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

■

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 $**$.

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

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

	$\circ(A \Rrightarrow B) \Rrightarrow \circ A \Rrightarrow \circ B$	
iff	$\circ(A \Rrightarrow B) \,\&\, \circ A \Rrightarrow \circ B$	adjoint
if	$\circ((A \Rrightarrow B) \,\&\, A) \Rrightarrow \circ B$	$\circ$-subdistributivity of &
if	$\circ B \Rrightarrow \circ B$.	adjoint: $(A \Rrightarrow B) \,\&\, A \Rrightarrow B$

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

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

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

Proof:

	$\Box(A \Rrightarrow B) \,\&\, \Diamond A \Rrightarrow \Diamond B$	
iff	$\Diamond A \Rrightarrow \Box(A \Rrightarrow B) \Rrightarrow \Diamond B$	adjoint
if	$A \sqcup \circ(\Box(A \Rrightarrow B) \Rrightarrow \Diamond B)$ $\Rrightarrow \Box(A \Rrightarrow B) \Rrightarrow \Diamond B$	*least* property of $\Diamond A$
iff	$A \sqcup \circ(\Box(A \Rrightarrow B) \Rrightarrow \Diamond B)$ $\& \ \Box(A \Rrightarrow B)$ $\Rrightarrow \Diamond B$	adjoint
iff	$A \,\&\, \Box(A \Rrightarrow B)$ $\sqcup \ \circ(\Box(A \Rrightarrow B) \Rrightarrow \Diamond B) \,\&\, \Box(A \Rrightarrow B)$ $\Rrightarrow \Diamond B$	distribute $\sqcup$ through &
iff	$A \,\&\, \Box(A \Rrightarrow B)$ $\sqcup \ \circ(\Box(A \Rrightarrow B) \Rrightarrow \Diamond B) \,\&\, \Box(A \Rrightarrow B)$ $\Rrightarrow B \sqcup \circ\Diamond B$	*fixed point* property of $\Diamond B$
if	$\circ(\Box(A \Rrightarrow B) \Rrightarrow \Diamond B) \ \& \ \Box(A \Rrightarrow B)$ $\Rrightarrow \circ\Diamond B$	$A \,\&\, \Box(A \Rrightarrow B) \Rrightarrow A \,\&\, (A \Rrightarrow B) \Rrightarrow B$

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

$\blacksquare$

5 Examples

We conclude our presentation of the model with examples in which explicit probabilities are essential.

The *unbounded random walk* [8] treats a (Markov) process that moves up or down in discrete steps with certain fixed probabilities. If the probabilities are equal, both 1/2, then the random walk is *symmetric* — and it is a theorem of elementary probability that the symmetric random walker returns to its starting position with probability 1 eventually. Such a process is said to be *recurrent*.

If the random walk is *asymmetric* then the walker returns eventually to the starting position with probability strictly less than 1, and is *transient*.

We 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 specifying

$$
\circ A.s \quad := \quad (A.(s{-}1) + A.(s{+}1))/2 \;, \tag{4}
$$

so that the expected value of any expectation A after one step is the average of A at the adjacent positions. We prove for all s that

$$
\circ\Diamond\{s\}.s \quad = \quad 1 \;,
$$

asserting that from any starting state eventual return occurs with probability 1 — that the walk is recurrent.

From the form of *step* we see[8] that $\Diamond\{s{+}1\}.s$ is independent of s — let it be u (for *up*). We have

$$
\begin{array}{lll}
 & u & \\
= & \Diamond\{s{+}1\}.s & \text{definition } u \\
= & \{s{+}1\}.s \sqcup \circ\Diamond\{s{+}1\}.s & \text{Definition 3.4} \\
= & (\Diamond\{s{+}1\}.(s{-}1) + \Diamond\{s{+}1\}.(s{+}1))/2 & \{s{+}1\}.s = 0\text{; from (4)} \\
= & (\Diamond\{s{+}1\}.(s{-}1))/2 + 1/2 & \Diamond\{s{+}1\}.(s{+}1) = 1
\end{array}
$$

[8]It 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.

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

of which $u{:=}\ 1$ is the unique solution. 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 $\Diamond\{s{-}1\}.s = 1$; and we conclude with

$$\circ\Diamond\{s\}.s \quad = \quad (\Diamond\{s\}.(s{-}1) + \Diamond\{s\}.(s{+}1))/2 \quad = \quad 1/2 + 1/2 \quad = \quad 1\ ,$$

as required.

Now suppose that instead of (4) we have the weaker specification

$$\Diamond A.s \quad \geq \quad (A.(s{-}1) + A.(s{+}1))/2\ , \tag{5}$$

in which $\circ A$ is replaced by $\Diamond A$.[9] It is satisfied for example by a random *stumbler* who on each step with some probability remains where he is: when he eventually does move however, it is with probability at least $1/2$ in each direction. (Taking $A{:=}\ \{s{-}1\}$ and $A{:=}\ \{s{+}1\}$ in (5) implies that.)

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

$$
\begin{array}{lll}
 & \Diamond\{s{+}1\}.s & \\
= & \Diamond\Diamond\{s{+}1\}.s & \text{Lemma A.1} \\
\geq & (\Diamond\{s{+}1\}.(s{-}1) + \Diamond\{s{+}1\}.(s{+}1))/2\ . & \text{from (5)}
\end{array}
$$

We then reason as before to conclude that u is again 1.

An important difference between the walker and the stumbler is that the walker could have been specified as two statements separately, for all s that

$\circ\{s{+}1\}.s \ \geq\ 1/2$	the walker moves up with probability at least 1/2 and
$\circ\{s{-}1\}.s \ \geq\ 1/2$	the walker moves down with probability at least 1/2,

from which $u = 1$ can be shown to follow.[10]

Specifying the stumbler similarly,

$\Diamond\{s{+}1\}.s \ \geq\ 1/2$	the walker *eventually* moves up, with probability at least 1/2 and	(6)
$\Diamond\{s{-}1\}.s \ \geq\ 1/2$	the walker *eventually* moves down, with probability at least 1/2,	

[9] We are forced consequentialy to replace $=$ by $\geq$, since we show that in fact $\Diamond A.s$ is greater than the right-hand side; but that is not the main point.

[10] Use *scaling* and *weighted average* to establish (4) weakened to an inequality; that is still sufficient for the proof.

is not sufficient however: for example the '1/3 up 2/3 down' *asymmetric* random walker, for which u is only 1/2, satisfies (6) but is not recurrent.

Specification (5) excludes transient stumblers that nevertheless satisfy (6) by 'piggybacking' — for example, by reaching $s-1$ only after having visited $s+1$ on the way.

6 Conclusions

Our technical contribution is the reinterpretation of fixed-point logic — the modal μ-calculus — over expectation- rather than predicate transformers:

- Sec. 3.3 shows how the formulae can 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 reasoning principles analogous to those for standard temporal logic, when the operators are restricted to the usual modalities $\circ$, $\Diamond$ and $\Box$.[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* [26] 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.

Our emphasis has been on reasoning rather than (for example) on model checking. In independent work, Huth and Kwiatkowska [13] interpret 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 [27, 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

[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.

- replacing the propositional operators $\vee, \wedge, \neg$ by the arithmetic $\sqcup, \sqcap, (1-)$ respectively,
- leaving the modal operators as they are and
- replacing $\mathbb{P}_{\geq p}$ by $(\underline{p} \Rrightarrow)$, 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 $\underline{p} \Rrightarrow \Diamond A$ (where we interpret A as a characteristic function).

Huth and Kwiatkowska establish similar correspondences, but for different sets of formulae: in their Theorem 1 [13] 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

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

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

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

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.

Expectations go beyond $pCTL^*$ in the trivial sense that $[0,1]$ extends $\{0,1\}$; that increased power can be useful in expressing some specifications very succinctly and in a way that facilitates reasoning (as at (5) in Sec. 5).

Finally, our treatent of nondeterminism does not explicitly mention a scheduler [25, 3] because the (demonic) schedule is built into 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 [11]. In principle we could have both demonic and angelic nondeterminism in *step*, though we would adjust the healthiness conditions in that case [18].

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. A decidable propositional dynamic logic with explicit probabilities. *Information and Control*, 63:11–38, 1984.

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

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

[9] Hans Hansson and Bengt Jonsson. A logic for reasoning about time and reliability. *Formal Aspects of Computing*, 6:512–535, 1994.

[10] Sergiu Hart and Micha Sharir. Probabilistic propositional temporal logics. *Information and Control*, 70:97–155, 1986.

[11] Jifeng He, A. K. McIver, and K. Seidel. Probabilistic models for the guarded command language. To appear in FMTA'95 Special Issue of Science of Computer Programming. Also available via *http* [24], 1996.

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

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

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

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

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

[17] Daniel Lehmann and Saharon Shelah. Reasoning with time and chance. *Information and Control*, 53:165–198, 1982.

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

[19] Carroll Morgan and Annabelle McIver. A probabilistic temporal calculus based on expectations. Technical Report PRG-TR-13-97, Programming Research Group, April 1997. Also available via *http* [24].

[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] A. Pnueli. The temporal logic of programs. In *Proc. 8th IEEE Symp. on Foundations of Computer Science*, pages 46–57, 1977.

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

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

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

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

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

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

	$\Diamond(t.A) \quad\Rrightarrow\quad t.(\Diamond A)$	
if	$t.A\ \sqcup\ \circ t.(\Diamond A) \quad\Rrightarrow\quad t.(\Diamond A)$	$\Diamond(t.A)$ *least*
if	$t.A\ \sqcup\ t.(\circ\Diamond A) \quad\Rrightarrow\quad t.(\Diamond A)$	assumption
if	$t.(A \sqcup \circ\Diamond A) \quad\Rrightarrow\quad t.(\Diamond A)$	t monotonic
iff	$t.(\Diamond A) \quad\Rrightarrow\quad t.(\Diamond A)\ .$	Definition 3.4

■

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

	$A\ \sqcup\ \circ\Diamond B$	
$\Rrightarrow$	$B\ \sqcup\ \circ\Diamond B$	$A \Rrightarrow B$
$\equiv$	$\Diamond B\ ,$	

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

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

■

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

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

■