A Weakest Pre–Expectation Semantics for Mixed–Sign Expectations

Benjamin Lucien Kaminski and Joost-Pieter Katoen
Software Modeling and Verification Group
RWTH Aachen University, Aachen, Germany

I. Introduction

We consider probabilistic programs of the form

$$C \quad \longrightarrow \quad x := \mathit{expr} \;\mid\; C;\, C \;\mid\; \texttt{if}\,(\xi)\,\{C\}\,\texttt{else}\,\{C\} \;\mid\; \texttt{while}\,(\xi)\,\{C\}\ ,$$

where ξ is a *probabilistic guard* which behaves as follows: Let Σ denote the set of program states, i.e. mappings from program variables to valuations. If the computation is currently in a state $\sigma \in \Sigma$ then ξ evaluates to true with probability $[\![\xi]\!](\sigma)$ and to false with probability $1 - [\![\xi]\!](\sigma) = [\![\neg\xi]\!](\sigma)$. For example, the probabilistic guard

$$[x \text{ is even}] \cdot \big(2/3\langle\mathsf{true}\rangle + 1/3\langle\mathsf{false}\rangle\big) + [x \text{ is odd}] \cdot \langle\mathsf{false}\rangle$$

evaluates to false with probability $1/3$ if in the current program state x is even and likewise with probability 1 if x is odd.

Given a program C, a random variable f mapping program states to reals, and an initial state σ, we are now interested in the following question: *What is the expected value of f after termination of C on input σ?* This expected value is referred to as the *pre–expectation* of C with respect to *post–expectation* f. For example, what is the pre–expectation of

$$C_{geo} \triangleright \quad \texttt{while}\,\big(1/2\langle\mathsf{true}\rangle + 1/2\langle\mathsf{false}\rangle\big)\,\{x := x+1\}$$

with respect to post–expectation $f = x$? The answer is $x+1$, since C_{geo} terminates with probability 1 and the execution of C_{geo} increases x on average by 1.

If we stay in the realm of *non–negative* expectations, i.e. random variables $f \in \mathbb{E}^{\infty}_{\geq 0} \coloneqq \big\{f \;\big|\; f\colon \Sigma \to \mathbb{R}_{\geq 0} \cup \{\infty\}\big\}$, the situation is fairly well understood, e.g. by means of the weakest pre–expectation calculus [1], [2], [3], [**?**]. It gives a meaning to each program C by means of a transformer $\mathsf{wp}[C]\colon \mathbb{E}^{\infty}_{\geq 0} \to \mathbb{E}^{\infty}_{\geq 0}$ that maps any post–expectation $f \in \mathbb{E}^{\infty}_{\geq 0}$ to a pre–expectation $\mathsf{wp}\,[C]\,(f) \in \mathbb{E}^{\infty}_{\geq 0}$, such that

$$\forall \sigma \in \Sigma\colon \quad \mathsf{wp}\,[C]\,(f)\,(\sigma) \;=\; \mathsf{E}_{[\![C]\!](\sigma)}\,(f)\ ,$$

where $\mathsf{E}_{\mu}\,(h)$ denotes the expected value of random variable h with respect to distribution μ and $[\![C]\!](\sigma)$ denotes the distribution obtained by executing program C on input σ. Hence $\mathsf{wp}\,[C]\,(f)\,(\sigma)$ is the expected value of f after termination of program C executed on input σ.

What happens, however, if we drop the requirement of f being non–negative? Suppose we want to reason about C_{geo} with respect to post–expectation $f = {(-2)^x}/{x}$. Is $\mathsf{wp}\,[x := 1;\, C_{geo}]\,(f)$ well–defined in that case? Intuitively, the pre–expectation is given by the series

$$-1 + \frac{1}{2} - \frac{1}{3} + \frac{1}{4} - \frac{1}{5} + \frac{1}{6} - \frac{1}{7} + \ldots \;=\; -\ln(2)\ .$$

The problem with this series is that—though it converges—it does not converge absolutely and thus—as a consequence of the well–known Riemann Series Theorem [4]—by reordering of the summands we can make the above series converge to *any real value* or even make it *tend to $+\infty$ or $-\infty$*. For representing expected values, however, the ordering of the summands should not matter as there is no natural ordering in which the mass of an expected value should be accumulated. For that reason, the expected value of a mixed–sign random variable f should exist if and only if f is integrable, i.e. if and only if the expected value of $|f|$ is finite. We therefore propose a weakest pre–expectation semantics that internally keeps track of the integrability of f, while still being well–defined for any program with respect to any mixed–sign post–expectation f.

II. Our Proposal

A. Integrability Witnessing Expectations

To keep track of the integrability of expectations, we accompany each mixed–sign expectation $f \in \mathbb{E}^{\star} \coloneqq \{f \mid f\colon \Sigma \to \mathbb{R}\}$ with a *non–negative* expectation $g \in \mathbb{E}^{\infty}_{\geq 0}$, such that $|f| \leq g$. We call such a pair $(f,\, g)$ an *integrability witnessing pair*.

The intuition behind an integrability witnessing pair $(f,\, g)$ is the following: If $\mathsf{wp}\,[C]\,(g)\,(\sigma) \;<\; \infty$, then the pre–expectation of C in σ with respect to $f \in \mathbb{E}^{\star}$ should exist as f is integrable with respect to distribution $[\![C]\!](\sigma)$. If, however, $\mathsf{wp}\,[C]\,(g)\,(\sigma) = \infty$ then we should not care about the pre–expectation of C in σ with respect to f since it should not be defined because in that case f is not integrable. This intuition leads to a quasi–order $\precsim$ on integrability witnessing expectations given by $(f,\, g) \precsim (f',\, g')$ iff for all $\sigma \in \Sigma$,

$$g'(\sigma) \neq \infty \quad \text{implies} \quad f(\sigma) \leq f'(\sigma) \text{ and } g(\sigma) \leq g'(\sigma)\ .$$

Notice that, indeed, $\precsim$ is not a partial order as it is *not antisymmetric*: we can have two integrability witnessing pairs $(f,\, g) \neq (f',\, g')$ with $(f,\, g) \precsim (f',\, g')$ and $(f,\, g) \succsim (f',\, g')$. This is the case if for some state $\sigma \in \Sigma$ we have $g(\sigma) = \infty = g'(\sigma)$, but $f(\sigma) \neq f'(\sigma)$.

On the other hand, two integrability witnessing pairs $(f,\, g)$ and $(f',\, g')$, for which $f(\sigma) \neq f'(\sigma)$ holds only for those states in which $g(\sigma) = \infty = g'(\sigma)$, should really be

considered *equivalent*, even though they are not equal. This is because for states σ in which $g(\sigma) = \infty = g'(\sigma)$, the evaluations of $f(\sigma)$ and $f'(\sigma)$ should be irrelevant since integrability is not ensured. Consequently, we need a notion of equivalence of integrability witnessing pairs, given by $\approx\, = \precsim \cap \succsim$. We denote the $\approx$–equivalence class of an integrability witnessing pair (f, g) by $\wr f, g \wr$ and call such an equivalence class an *integrability witnessing expectation*. We denote by $\mathbb{IE}$ the set of integrability witnessing expectations.

There is a canonical [**?**] partial order $\sqsubseteq$ on $\mathbb{IE}$ given by $\wr f_1, g_1 \wr \sqsubseteq \wr f_2, g_2 \wr$ iff $(f_1, g_1) \precsim (f_2, g_2)$. As for an intuitive interpretation of this partial order, we note that if $\wr f_1, g_1 \wr \sqsubseteq \wr f_2, g_2 \wr$ holds, then we have $f_1'(\sigma) = f_1(\sigma) \leq f_2(\sigma) = f_2'(\sigma)$ for all $(f_1', g_1') \in \wr f_1, g_1 \wr$, $(f_2', g_2') \in \wr f_2, g_2 \wr$, and all states in which $g_2(\sigma) \neq \infty$ holds. Thus if integrability in σ is ensured, the first components compare in σ, which is the comparison we are mainly interested in.

The partial order $\sqsubseteq$ on $\mathbb{IE}$ expectations is complete in the sense that every *non–empty* subset has a supremum. However, $\mathbb{IE}$ has *no least element*; in particular $\wr \mathbf{0}, \mathbf{0} \wr$ is not a least element of $\mathbb{IE}$. This fact prevents us from applying the Kleene Fixed Point Theorem to ensure existence of least fixed points for defining a wp–calculus acting on $\mathbb{IE}$.

B. Mixed–Sign Weakest Pre–Expectations

We now propose a weakest pre–expectation transformer $\widetilde{\mathsf{wp}}[C] \colon \mathbb{IE} \to \mathbb{IE}$ defined compositionally by induction on the structure of C, see Table I. Let us shortly go over these definitions: $\widetilde{\mathsf{wp}}\,[x := E]\,\wr f, g \wr$ takes a representative $(f, g) \in \wr f, g \wr$, performs the assignment $x := E$ on both components to obtain $(f\,[x/E],\, g\,[x/E])$ and then returns the according equivalence class $\wr f\,[x/E],\, g\,[x/E] \wr$. Notice that assignments preserve $\approx$–equivalence, so doing the update on the representative is a sound and sufficient course of action.

$\widetilde{\mathsf{wp}}\,[C_1\,;\, C_2]\,\wr f, g \wr$ obtains a pre–expectation for the program $C_1\,;\, C_2$ by applying $\widetilde{\mathsf{wp}}[C_1]$ to the intermediate integrability witnessing expectation obtained from $\widetilde{\mathsf{wp}}\,[C_2]\,\wr f, g \wr$.

TABLE I

DEFINITIONS FOR $\widetilde{\mathsf{wp}}$. $f\,[x/expr]$ DENOTES $\lambda\sigma\bullet\ f(\sigma[x \mapsto \sigma(expr)])$, WHERE $\sigma[x \mapsto \sigma(expr)]$ IS THE PROGRAM STATE OBTAINED BY UPDATING IN σ THE VALUE OF x TO $\sigma(expr)$. FOR THE DEFINITION OF `while`, ${}_{C'}{}^{\xi}F^{n}_{\wr f, g \wr}$ DENOTES APPLYING ${}_{C'}{}^{\xi}F_{\wr f, g \wr}$ n–FOLD TO ITS ARGUMENT.

C	$\widetilde{\mathsf{wp}}[C]\wr f, g \wr$
$x := expr$	$\wr f\,[x/expr],\, g\,[x/expr] \wr$
$C_1\,;\, C_2$	$\widetilde{\mathsf{wp}}[C_1](\widetilde{\mathsf{wp}}\,[C_2]\,\wr f, g \wr)$
$\mathtt{if}\,(\xi)\,\{C_1\}\,\mathtt{else}\,\{C_2\}$	$[\![\xi]\!] \cdot \widetilde{\mathsf{wp}}\,[C_1]\,\wr f, g \wr + [\![\neg\xi]\!] \cdot \widetilde{\mathsf{wp}}\,[C_2]\,\wr f, g \wr$
$\mathtt{while}\,(\xi)\,\{C'\}$	$\lim_{n\to\omega}\ {}_{C'}{}^{\xi}F^{n}_{\wr f, g \wr}\wr \mathbf{0}, \mathbf{0} \wr$

$${}_{C'}{}^{\xi}F_{\wr f, g \wr}\wr X, Y \wr \;=\; [\![\neg\xi]\!] \cdot \wr f, g \wr + [\![\xi]\!] \cdot \widetilde{\mathsf{wp}}\,[C]\,\wr X, Y \wr$$

$\widetilde{\mathsf{wp}}\,[\mathtt{if}\,(\xi)\,\{C_1\}\,\mathtt{else}\,\{C_2\}]\,\wr f, g \wr$ weights $\widetilde{\mathsf{wp}}\,[C_1]\,\wr f, g \wr$ and $\widetilde{\mathsf{wp}}\,[C_2]\,\wr f, g \wr$ according to the probability of the guard ξ evaluating to true and false. Here, $g' \cdot \wr f, g \wr \coloneqq \wr g' \cdot f, g' \cdot g \wr$ and $\wr f', g' \wr + \wr f, g \wr \coloneqq \wr f' + f, g' + g \wr$.

$\widetilde{\mathsf{wp}}$ of $\mathtt{while}\,(\xi)\,\{C'\}$ is defined as the limit of iteratively applying the characteristic functional

$${}_{C'}{}^{\xi}F_{\wr f, g \wr}\wr X, Y \wr \;=\; [\![\neg\xi]\!] \cdot \wr f, g \wr + [\![\xi]\!] \cdot \widetilde{\mathsf{wp}}\,[C']\,\wr X, Y \wr\,,$$

to $\wr \mathbf{0}, \mathbf{0} \wr$. This limit can be shown to be existent and unique. Recall that $\wr \mathbf{0}, \mathbf{0} \wr$ is not the least element of $\mathbb{IE}$ and thus the Kleene Fixed Point Theorem *cannot be applied* to deduct the existence of this limit. Instead, the core idea for proving this fact is adopted from a well–known proof proving that every absolutely convergent series is also convergent.

C. Soundness, Monotonicity, and Loop Invariants

Our mixed–sign weakest pre–expectation transformer is sound, meaning that if we can establish $\widetilde{\mathsf{wp}}\,[C]\,\wr f, |f| \wr = \wr f', g' \wr$ with $g'(\sigma) < \infty$, then $f'(\sigma)$ is in fact the expected value of f after termination of C on initial state σ.

Furthermore, our transformer is monotonic, meaning that

$$\wr f, g \wr \sqsubseteq \wr f', g' \wr \text{ implies } \widetilde{\mathsf{wp}}\,[C]\,\wr f, g \wr \sqsubseteq \widetilde{\mathsf{wp}}\,[C]\,\wr f', g' \wr\,.$$

Since monotonicity of a weakest pre–expectation transformer is as vital to reasoning about programs as the consequence rule is to Hoare logic, this is a key feature.

Lastly, we note that we can give a proof rule for loops based on loop invariants. Going into the details of this rule would go beyond the scope of this short abstract but suffice it to say that using our proof rule we can for instance prove that the pre–expectation of

$$C_{Op} \triangleright \quad \Phi := \Phi + 1;\ \mathtt{while}\ (1/2)\ \{\Phi := \Phi - 3\}$$

with respect to post–expectation Φ is *at most* $\Phi - 2$. In other words: C_{Op} *decreases* Φ at least by 2.

Notice that such an analysis would neither be possible using the deduction rules of PPDL [1] nor the invariant–based approach of McIver & Morgan's wp–calculus [2] off–the–shelf. Instead, a tailor made argument would be needed for reasoning about the mixed–sign post–expectation Φ.

ACKNOWLEDGMENT

This work was supported by the Excellence Initiative of the German federal and state government and by the CDZ project CAP (GZ 1023).

REFERENCES

[1] D. Kozen, "A probabilistic PDL," *J. Comput. Syst. Sci.*, vol. 30, no. 2, pp. 162–178, 1985.

[2] A. McIver and C. Morgan, *Abstraction, Refinement and Proof for Probabilistic Systems*. Springer, 2004.

[3] F. Gretz, J. Katoen, and A. McIver, "Operational versus Weakest Pre–Expectation Semantics for the Probabilistic Guarded Command Language," *Performance Evaluation*, vol. 73, pp. 110–132, 2014.

[4] B. Riemann, *Ueber die Darstellbarkeit einer Function durch eine trigonometrische Reihe*. Königliche Gesellschaft der Wissenschaften zu Göttingen, 1867.