A Modular Cost Analysis for Probabilistic Programs

MARTIN AVANZINI, INRIA Sophia Antipolis
GEORG MOSER, University of Innsbruck
MICHAEL SCHAPER, University of Innsbruck

We present a novel methodology for the automated resource analysis of non-deterministic, probabilistic imperative programs, which gives rise to a unique *modular approach*. Program fragments are analysed in full independence. Further, the results established allow us to incorporate sampling from *dynamic distributions*, making our analysis applicable to realistic examples.

We have implemented our contributions in the tool `eco-imp`, exploiting a constraint-solver over iterative refineable cost functions facilitated by off-the-shelf SMT-solvers. We provide ample experimental evidence of the prototypes' algorithmic superiority. Our experiments show that our tool runs typically at least one *order of magnitude faster* than comparable tools. On realistic examples, it is even the case that execution times of seconds become milliseconds. At the same time we retain the precision of existing tools.

The extensions in applicability and the greater efficiency of our prototype, yield scalabilty of the tool. This effects into more realistic examples, whose expected cost analysis can be thus performed fully automatically. In particular, our tool is the first establishing an automated analysis of the *Coupon Collector's problem*.

Additional Key Words and Phrases: probabilistic programs, average complexity, automation, modularity

1 INTRODUCTION

Resource analysis is a subfield of static analysis, studying a non-functional property of programs, namely the use of *resources* (see [Cohen and Zuckerman 1974; Wegbreit 1975, 1976] for early references). Resources are broadly construed and encompass *runtime*, *memory usage*, *stack and heap sizes*, etc. Resource analysis impacts on the *correctness* or *safety* of programs. Programs that over-exceed available computing resources are most likely to fail, and hence cannot run correctly. See, for example Albert et al. [2019] for an application of resource analysis on the safety of *smart contracts*.

In the last decades there has been significant progress in the area of *fully automated* resource analysis, where no user interaction is required. This resulted in significant success stories showing that resource analysis can be practicable and scalable, cf. [Frohn and Giesl 2017; Gulwani et al. 2009; Hoffmann et al. 2017; Wilhelm et al. 2008; Wilhelm and Grund 2014]. *Modularity* of the analysis turned out as a key ingredient to the scalability of automated resource analysis, as modularity allows for code fragments to be analysed in full independence, that is, whole-program analyses can be overcome. This significantly speeds up the analysis without affecting the precision of the analysis. See for example [Avanzini et al. 2016; Brockschmidt et al. 2016; Frohn and Giesl 2017;

This work is supported by the French ANR: "Agence National de Recherche" under Grant "PPS: Probabilistic Program Semantics", No. ANR-19-CE48-0014.
Authors' addresses: Martin Avanzini, martin.avanzini@inria.fr, INRIA Sophia Antipolis, France; Georg Moser, georg.moser@uibk.ac.at, University of Innsbruck, Austria; Michael Schaper, michael.schaper@student.uibk.ac.at, University of Innsbruck, Austria.

XXXX-XXXX/2020/8-ART $15.00
https://doi.org/

Gulwani and Zuleger 2010; Moser and Schaper 2018; Sinn et al. 2016, 2017] for references to the literature on fully automated resource analysis methods of non-probabilistic imperative programs.

Apart from modularity, the study of *non-deterministic* programs has proven immensely useful. Non-determinism appears naturally through *program abstraction*. In particular, in the analysis of imperative programs, program abstractions form an integral part. It is due to program abstractions—sometimes also referred to as *program transformations*—that sophisticated, fully automated analyses of complex, pointer-based programs have become possible. (See Fiedor et al. [2018] also for further pointers to the literature.)

Interrelations between computer science and probability theory are well-studied. Indeed, probabilistic variations on well-known models like automata, Turing machines or the λ-calculus have been studied since the early days of theoretical computer science (see Kozen [1981] for an early reference). Generalising the model of computation further and allowing for *probabilistic, non-deterministic* programs, induces new challenges to an automated resource analysis.

First, *non-deterministic* probabilistic programs have not received much attention in the literature. The provided theoretical constructions, namely the resolution of non-determinism through dedicated scheduling complicates the principally beautiful foundation via *Markov chains*. A new foundation is essential. Second, automation, in particular automation of the push-button variety is not yet firmly established. Only few prototypes exist and the literature is lacking clear experimental comparisons. Further, intuitive textbook examples, like the *Coupon Collector's problem* (see Figure 1c) cannot be represented properly in existing tools. This is due to the lack of primitives for *dynamic distributions*, ie. for sampling from distributions whose support or value depends on the current environment. Third, and most crucially, *modularity* of the analysis is not provided for. Instead, the automated analysis in all existing prototypes degenerates to a whole-program analysis. The results established in this paper overcome all these issues.

We are concerned with an automated *average runtime analysis* of a prototypical *imperative language* pWhile in the spirit of Dijkstra's *Guarded Command Language*. This language is endowed with primitives for *sampling* and *non-deterministic choice* so that *randomised algorithms* can be expressed. Further, a dedicated command `consume`(e) allows for the representation of unbounded non-negative costs given by the expression e. Non-negativity is required so as to ensure that the expected cost of a program is well-defined. Thus our automated analysis provides an *expected cost analysis*. By instrumenting the program so that every program statement is attributed cost one, this analysis can be used to assess the mean-time to termination and, as such, assesses that a program is *(positive) almost-surely terminating* Bournez and Garnier [2005]. On the other hand, almost-sure termination is not a pre-condition to our analysis.

Contributions. We present a novel *modular* methodology for the *automated* resource analysis of non-deterministic, probabilistic programs. Precisely,

- we present a novel *structural operational semantics* in terms of *probabilistic abstract reduction systems* originally due to Bournez and Garnier—significantly simplifying the formal development;
- we generalise the *expected runtime transformer* of Kaminski et al. [2016] to a cost transformer and formally prove it sound wrt. our novel operational semantics;
- we establish a novel alternating *expected cost* and *expected value* analysis, which gives rise to the first *fully modular resource analysis* of non-deterministic, probabilistic programs;
- we demonstrate how sampling from *dynamic distributions* can be incorporated, making our analysis more realistic; specifically, we allow for uniform sampling from an interval dependent on program states;

```
1 while (p > min ≥ 0) {
2   b ≔ Bernoulli(1/4);
3   if (b) {p ≔ p + 1} {p ≔ p - 1};
4   n ≔ Uniform(0,10);
5   while (n > 0) {
6     consume(p); n ≔ n - 1 }
7 }
```

(a) Trader C_{trader}.

```
1 b ≔ 1;
2 x ≔ 1;
3 while (b = 1) {
4   consume(1);
5   x ≔ x * 2;
6   b ≔ Bernoulli(1/2)
7 }
```

(b) Geometric C_{geo}.

```
1 coupons ≔ 0;
2 while (0 ≤ coupons < n) {
3   consume(1);
4   draw ≔ Uniform(1,n);
5   if (draw > coupons) {
6     coupons ≔ coupons + 1 }
7 }
```

(c) Coupon Collector $C_{coupons}$.

Fig. 1. Motivating Examples.

- we have implemented our method in the tool `eco-imp` and show *efficiency* and *scalability* of this automation by comparison with existing prototypes in the literature; while `eco-imp` parallels other tools in precision, its analysis times are significantly faster;
- finally, we detail our resource analysis algorithm underlying our prototype `eco-imp`, together with an in-depth discussion on the employed constraint solving mechanism.

Our prototype facilitates off-the-shelf SMT-solvers for the iteratively refinable synthesis of cost expressions. In benchmarking, we focus on complex and realistic scenarios, thus emphasising the algorithmic prowess and scalability of our approach. We validate its effectiveness on a set of 66 challenging probabilistic programs taken from the literature. In particular, for programs with non-linear bounds and nested loop structure our analysis is upto *three orders of magnitude faster* than existing prototypes. At the same time we retain the precision.

Outline. We start with motivating our quest for a *modular* framework, later detailed in Section 6. Probabilistic abstract reduction systems, which form the theoretical underpinning, and our imperative language are presented in Section 3 and 4, respectively. Section 5 recalls a weakest precondition calculus due to Kaminski et al. [2018], which is generalised in Section 6 to serve our needs of a modular analysis. In Section 7, the actual implementation is described and ample experimental evidence is given. In this section, we also explain our dedicated constraint solver and highlight our methodology on a handful of interesting examples. Section 8 discusses related work and we conclude in Section 9. The Supplementary Material to this paper contains information on the mathematical background and full proofs of all our results.

2 AUTOMATED EXPECTED COST ANALYSIS AND MODULARITY

We motivate the central contribution of our work: an *automated* and *modular* expected cost analysis of non-deterministic, probabilistic programs. First, we present a classic analysis of an algorithm incorporating a one-dimensional random walk, cf. Figure 1a. Second, we highlight the need for a more refined analysis technique, when it comes to compositionality of the analysis. Third, we detail the challenges of automated verification techniques. Finally, we emphasise the need for *modularity* in this context.

Recurrence equations. A classical way to analyse the runtime of a program is to set up a set of recurrence equations, whose closed-form provides the sought runtime. Wegbreit [1975, 1976] was the first to automate this approach for deterministic programs. This idea generalises straight forward to probabilistic programs.

Consider the program C_{trader} due to Ngo et al. [2018] in Figure 1a, which illustrates the behaviour of a stock trader. While the stock price (p) is above the minimum (min), the trader decides to buy shares. The stock price is governed by a *one-dimensional random walk*. With probability $1/4$ the price increases (by one), and with probability $3/4$ the price decreases. After the change of the stock price takes effect, the trader decides to buy upto 10 shares, all with equal probability. The cost for

the trader is given as the total amount invested. Clearly, this cost is unbounded in some scenarios, namely, when the price p stays above the minimum price. However, the combined probability of all such scenarios is 0. Worst case bounds are thus not informative for such programs. A more informative measure, and the one we are interested in, is given by the *expected cost*, ie. the average cost emitted on all the computational branches, weighted by their probability. Simplifying the analysis by assuming $min = 0$ for now, the expected cost of $\mathsf{C}_{\mathsf{trader}}$ becomes expressible by the recurrence

$$\begin{aligned} T(price) &= {}^{1}\!/_{44} \cdot \textstyle\sum_{n=0}^{10} \big(n \cdot (price + 1) + T(price + 1)\big) + {}^{3}\!/_{44} \cdot \sum_{n=0}^{10} \big(n \cdot (price - 1) + T(price - 1)\big) \\ &= 5 \cdot price - {}^{5}\!/_{2} + {}^{1}\!/_{4} T(price + 1) + {}^{3}\!/_{4} T(price - 1) \ . \end{aligned}$$

This is a non-homogeneous linear second-order recurrence, whose closed-form can be computed as $5 \cdot price \cdot (price+1)$. While the general solution of the corresponding homogeneous recurrence can be derived directly (see Levitin [2007]), the manual computation of the closed-form of T requires some work. It is well-known that in general such a manual analysis—even for small and simple programs as in the case of $\mathsf{C}_{\mathsf{trader}}$—is tedious, error prone and fragile to small changes of the recurrence equations. On the other hand our prototype implementation computes the (asymptotically) optimal upper bound of $5 \cdot price \cdot (price + 2)$ in *milliseconds*.

Compositionality of the analysis. A central observation in the seminal work by Kaminski et al. [2018] is that an expected runtime analysis is inherently *non-compositional*, that is, from finite expected runtimes of program parts, we cannot conclude finite expected runtime of the whole program. A related issue has been encountered and overcome in the context of unbounded updates of non-deterministic (but non-probabilistic) programs, cf. [Ben-Amram 2011; Ben-Amram 2015; Ben-Amram and Hamilton 2019; Ben-Amram and Kristiansen 2012; Hirokawa and Moser 2008; Jones and Kristiansen 2009].

To illustrate, let us first consider the program $\mathsf{C}_{\mathsf{geo}}$ depicted in Figure 1b. While also this example potentially diverges, its expected cost—the number of loop iterations—is 2. Second, consider the composition of $\mathsf{C}_{\mathsf{geo}}$ with a program D, whose expected cost is given by $f(x)$. Then the expected cost of $\mathsf{C}_{\mathsf{geo}};\mathsf{D}$, that is, running the two programs in sequence, becomes

$$\textstyle\sum_{i=0}^{\infty} {}^{1}\!/_{2^i} \cdot f(2^{i+1}) \ . \tag{$\dagger$}$$

When f grows at least linearly, this sum is infinite. Conclusively, while the expected costs of $\mathsf{C}_{\mathsf{geo}}$ and D are finite, the expected cost of their composition is not. Generalising a weakest precondition calculus à la Dijkstra's to an *expected runtime transformer* ert, Kaminski et al. overcome this issue through the expression of the expected runtime in continuation passing style, cf. [Kaminski and Katoen 2017; Kaminski et al. 2016, 2018; Olmedo et al. 2016]. As observed by Kaminski et al., this transformer in turn generalises seamlessly to one for reasoning about expected costs. Wrt. a program D, whose expected cost is f, $\mathsf{ert}[\mathsf{C}](f)$ computes the time of first executing C and then D. In particular, $\mathsf{ert}[\mathsf{C}_{\mathsf{geo}}](f)$ is precisely ($\dagger$). The cost of two sequentially composed commands $\mathsf{C};\mathsf{D}$ thus becomes expressible via composition of the transformer: $\mathsf{ert}[\mathsf{C};\mathsf{D}](f) = (\mathsf{ert}[\mathsf{C}] \circ \mathsf{ert}[\mathsf{D}])(f)$. Similarly, consider the program $\mathsf{C}_{\mathsf{trader}}$. Composablity of the analysis allow us to describe the expected costs of the outer loop's body independently from the expected cost of the outer loop. Hence, the analysis becomes compositional in theory.

To sum up, the ert-calculus is a more refined technical tool for the analysis of probabilistic programs than the classical analysis through recurrence relations. The analysis becomes clean and is less fragile. Further, it allows an optimal analysis of a variety of interesting case studies, like eg. the aforementioned program $\mathsf{C}_{\mathsf{coupons}}$ from Figure 1c. However, Kaminski et al. [2018] do not

provide an automation and also only superficially concepts automation. So the method remains tedious.

Automation. The `Absynth` prototype provided by Ngo et al. [2018] has been the first *automated* expected resource analysis of probabilistic programs. For instance, `Absynth` infers the manual bound on the expected cost of $\mathsf{C}_{\mathsf{trader}}$ shown above, fully automatically. The tool provides a specialised automation of Kaminski's ert-calculus. The transformer is coached into a Hoare-style calculus and expected cost functions are formalised as *potential functions* [Ngo et al. 2018]. Automation is achieved by specialising these potential functions to linear combinations of *base functions*, abstracting stores as non-negative numbers. Recently, Wang et al. [2019] provides a resource analysis, based on martingale theory. Notably, their methodology is the first to also account for *negative costs*. The main challenge in accommodating negative costs lies in ensuring that the overall expected cost remains well-defined. Wang et al. ensures this by requiring that in the presence of negative costs, program updates are generally bounded. Here (almost-sure) termination is required. Moreover, their implementation yields a polytime algorithm.

Both tools provide a *whole-program analysis*. Conclusively, neither of these tools is modular and both tools have issues with scalability. To whit, consider a more realistic variant of $\mathsf{C}_{\mathsf{trader}}$, where the stock trader is choosing uniformly upto 100.000 shares. Due to the modular design of our prototype, the variant can be handled with ease in seconds. However, the `Absynth` tool is no longer able to compute a bound, while the prototype established by Wang et al. [2019] requires upto 30 seconds of runtime—additionally a significant amount of user guidance is required. Similar issues hold wrt. multiple nested loops (see Section 7). In contrast, we provide a novel modular and efficient automation, inspired by the continuation-passing style analysis method formalised in the ert-calculus, which however is free of the aforementioned scalability issues.

An Intuitive Textbook Example. Following the formulation of Mitzenmacher and Upfal [2005], the above mentioned *Coupon Collector's problem* states as follows. Given a box with n different coupons, one is interested in the expected number of *draws with replacement* that are needed before having drawn each coupon at least once. The corresponding code $\mathsf{C}_{\mathsf{coupons}}$ is depicted in Figure 1c. Here, *coupons* represents the number of unique coupons collected; *draw* samples uniformly from the interval $[1, n]$, with n an input parameter. The chosen cost model reflects the number of trials. Note, that the probability of collecting a new coupon drops in proportion of the collected coupons, that is, in proportion $1/\mathit{coupons}+1$. In particular, the expected cost is finite.

The full pen-and-paper analysis of $\mathsf{C}_{\mathsf{coupons}}$ given by Kaminski et al. [2018]—which provides the optimal expected time bound $\mathrm{O}(n \log n)$—spans several pages and requires non-trivial estimations. Thus, non surprisingly, automation poses significant challenges. So far, to the best of our knowledge, the Coupon Collector's problem has been elusive to any automated analysis. As already mentioned, no existing tool can even *represent* the corresponding code $\mathsf{C}_{\mathsf{coupons}}$. To date support for *dynamic probabilistic branching* is lacking. Our prototype `eco-imp` admits dynamic distribution and provides the bound $n + 1/2 \cdot n^2$ fully automatically in *a fraction of a second*. This automated analysis of the expected cost of $\mathsf{C}_{\mathsf{coupons}}$ is achieved via a constraint solver that allows for the iterative refinement of cost expressions; thus generic enough to handle the example.

If the distribution is set statically, eg. to a uniform distribution of 10 coupons, the example becomes expressible by existing tools. Alas, only the `Absynth` tool can provide a (non-optimal) bound (see Section 7). Still the employed potential functions are not amenable to express the subtle dependency of the expected cost of $\mathsf{C}_{\mathsf{coupons}}$ on the (now) static distribution governing the draw. Ie. the generated constraint again grows linearly to the number of coupons. On the other hand, the constraints generated by our tool are succinct. Wrt. tool execution time this implies that our prototype `eco-imp` handles a uniform distribution of upto 100 coupons in seconds. On the other

hand the Absynth tool cannot provide bounds for larger numbers, even after several minutes of runtime.

Achieving Modularity of the Analysis. The main novel aspect of our work lies in providing a modular (and thus scalable) analysis of probabilistic and non-deterministic programs. Of course, in a probabilistic setting this is not too straight forward, because running a command results in a distribution of possible end states, cf. Fioriti and Hermanns [2015].

We emphasise that composability of the *analysis* of the expected cost of sequential commands, as provided by the ert-calculus, does not induce composability of the *synthesis* of the corresponding bounding functions. We illustrate the difference, wrt. $\mathsf{C}_{\mathsf{trader}}$. To find closed-forms of the expected cost of loops, one searches for *upper invariants* (see Section 5.2). Concretely, as $\mathsf{C}_{\mathsf{trader}}$ features a nested loop, its expected cost wrt. the cost $f(n, p, min)$ of a continuation is driven by the following inter-dependent constraints (see Section 6).

$$\begin{aligned} p > min \geq 0 &\Rightarrow O(n,p,min) \geq {}^{1}\!/_{44} \cdot \textstyle\sum_{n=1}^{10} I(n,p+1,min) + {}^{3}\!/_{44} \cdot \sum_{n=1}^{10} I(n,p-1,min) \\ \neg(p > min \geq 0) &\Rightarrow O(n,p,min) \geq f(n,p,min) \\ n \geq 0 &\Rightarrow I(n,p,min) \geq p + I(n-1,p,min) \\ \neg(n \geq 0) &\Rightarrow I(n,p,min) \geq O(n,p,min)\ . \end{aligned}$$

Here, $O(n, p, min)$ and $I(n, p, min)$ stands for the cost before entering the inner and outer loop, respectively. Due to their inter-dependent nature, invariants I and O cannot be considered in isolation and their synthesis degenerates to a whole-program analysis. We refer to the composability of the synthesis of upper invariants as *modularity* of the (expected) cost analysis. Modularity requests that the cost analysis for a program can be broken into an independent cost analysis of program parts. This establishes a crucial stepping stone for the *scalability* of the analysis.

The idea, underlying the gist of the methods achieving modularity for the analysis of deterministic programs can be summarised as follows, cf. [Avanzini et al. 2016; Brockschmidt et al. 2016; Frohn and Giesl 2017; Gulwani and Zuleger 2010; Moser and Schaper 2018; Sinn et al. 2016, 2017]. Consider functions f and g measuring the costs of deterministic programs C and D, respectively. These cost functions f, g are dependent on the program state σ before program execution, that is, f and g depend on the variable assignments at the beginning of C and D, respectively. Then $f(\sigma)+g(\sigma')$ gives the resource usage of the sequential command C; D, whenever σ' denotes the variable assignment after the execution of C. Estimating σ' in terms of C and σ, gives rise to a modular analysis, where runtime and size analysis is alternated. The observation, while conceptually simple, is nevertheless immensely useful. We suit it to probabilistic, non-deterministic programs. For that, we focus on *expected cost* and *expected value* analysis as substitution for the aforementioned runtime and value analysis. Similarly to the above sketch, we alternate between expected cost and value analysis. Here, we crucially exploit that *concave* cost functions, eg. multi-linear polynomials, distribute over expectations. In this setting, the above mentioned inter-dependent constraints become decomposeable, as the synthesis of the bounding functions for the inner loop (I) and the outer loop (O), respectively, can be performed independently. This gives rise to a modular methodology for the automated expected cost analysis of non-deterministic, probabilistic programs.

Our modular analysis is particularly effective in the analysis of nested loops, which has direct consequences for the scalability and speed of the analysis. For example, in comparison to the Absynth prototype—which can be considered among the most efficient implementations of such an analysis to date—we achieve a speed-up of upto three orders of magnitude on such examples. At the same time we retain the precision of the Absynth tool.

3 PROBABILISTIC REDUCTION SYSTEMS

In this section we quickly recap notions and notations of (weighted) probabilistic abstract reduction systems. Probabilistic abstract reduction systems are due to Bournez and Garnier [2005] and form a generalisation of *abstract reduction systems*, accounting for probabilistic choice. Avanzini and Yamada [2020] extend probabilistic abstract reduction systems with *weights*, allowing for the formulation of a suitable *cost model*. For brevity, we refer to the weighted variant again as *probabilistic abstract reduction systems* (*PARSs*). In the sequel, *costs* $\mathbb{C}$ are represented as non-negative real numbers extended with ∞, ie. $\mathbb{C} \triangleq \mathbb{R}^{\infty}_{\geq 0}$, where $\mathbb{R}^{\infty}_{\geq 0} = \mathbb{R}_{\geq 0} \cup \{\infty\}$. Note that costs are positive, but unbounded. Otherwise, the below defined expected cost function would be ill-defined.

A (discrete) *subdistribution* over A is a function $\delta \colon A \to \mathbb{R}_{\geq 0}$ such that $\sum_{a \in A} \delta(a) \leq 1$, and a *distribution* if $\sum_{a \in A} \delta(a) = 1$. We may write subdistributions δ as $\{\!\{\delta(a) : a\}\!\}_{a \in A}$. The set of all subdistributions over A is denoted by $\mathcal{D}(A)$. We restrict ourselves to distributions over countable sets A. The *expectation of* a function $f \colon A \to \mathbb{R}^{\infty}_{\geq 0}$ wrt. a distribution δ is given by $\mathbb{E}_{\delta}(f) \triangleq \sum_{a \in A} \delta(a) \cdot f(a)$.

Probabilistic abstract reduction systems. A PARS over A is a set of *rules* $a \to \delta$ indicating that $a \in A$ reduces to $b \in A$ with probability $\delta(b)$ if $\delta(b) \neq 0$. Operationally, a reduction step on a involves first picking a rule $a \to \delta$ (among possibly many) and then sampling the reduct from δ. To allow for non-uniform costs, we endow each rule with a *weight* $w \in \mathbb{R}_{\geq 0}$, accounting for the cost of the corresponding reduction step, cf. [Avanzini and Yamada 2020]. Thus formally, a PARS on A is given by ternary relation $\cdot \dot{\to} \cdot \subseteq A \times \mathbb{R}_{\geq 0} \times \mathcal{D}(A)$, where in a rule $a \xrightarrow{w} \delta$, the weight w indicates the cost of the rule application. Objects $a \in A$ with no rule $a \xrightarrow{w} \delta$ are called *terminal*, in notation $a{\downarrow}$. The program $\mathsf{C}_{\mathsf{geo}}$ from Figure 1b, for instance, is modelled by the PARS $\xrightarrow[\mathsf{geo}]{}$, defined by

$$\mathrm{geo}(x) \xrightarrow[\mathsf{geo}]{1} \{\!\{1/2 : 2 \cdot x, 1/2 : \mathrm{geo}(2 \cdot x)\}\!\} \quad \text{for all } x \in \mathbb{Z}.$$

Following [Avanzini et al. 2019b; Avanzini and Yamada 2020], we define the dynamics of a PARS $\to$ in terms of a *(weight-indexed) reduction relation* $\cdot \dot{\twoheadrightarrow} \cdot \subseteq \mathcal{M}(A) \times \mathbb{R}_{\geq 0} \times \mathcal{M}(A)$ over *multidistributions* $\mathcal{M}(A)$. These are countable *multisets* $\{\!\{p_i : a_i\}\!\}_{i \in I}$ over pairs $p_i : a_i$ of *probabilities* $0 < p_i \leq 1$ and *objects* $a_i \in A$ with $\sum_{i \in I} p_i \leq 1$. Multidistributions are denoted by $\mu, \nu, \ldots$. The notion of *expectation* is extended to multidistributions in the natural way by $\mathbb{E}_{\mu}(f) \triangleq \sum_{(p:a) \in \mu} p \cdot f(a)$. Finally, the reduction relation is inductively find by

$$\frac{}{\mu \xrightarrow{0}\!\!\!\!\twoheadrightarrow \mu} \qquad \frac{a \xrightarrow{w} \delta}{\{\!\{1 : a\}\!\} \xrightarrow{w}\!\!\!\!\twoheadrightarrow \delta} \qquad \frac{\mu_i \xrightarrow{w_i}\!\!\!\!\twoheadrightarrow \nu_i}{\biguplus_{i \in I} p_i \cdot \mu_i \xrightarrow{w}\!\!\!\!\twoheadrightarrow \biguplus_{i \in I} p_i \cdot \nu_i} \ .$$

In the second rule, distributions are lifted to multidistributions in the obvious way. In the last rule, $w = \sum_{i \in I} p_i \cdot w_i$ and $p_i > 0$ are probabilities with $\sum_{i \in I} p_i \leq 1$. Scalar multiplication is performed component-wise on probabilities, $\biguplus$ refers to the usual notion of multiset union. Put differently, $\mu \xrightarrow{w}\!\!\!\!\twoheadrightarrow \nu$ indicates that some elements a_i with associated probability p_i are replaced by δ_i, re-weighted with probability p_i, according to rules $a_i \xrightarrow{w_i} \delta_i$. The overall cost w is given by the sum $\sum p_i \cdot w_i$, corresponding to the expected cost of the single reduction step $\mu \xrightarrow{w}\!\!\!\!\twoheadrightarrow \nu$. For instance, the PARS $\xrightarrow[\mathsf{geo}]{}$ gives rise to the reduction

$$\{\!\{1 : \mathrm{geo}(1)\}\!\} \xrightarrow[\mathsf{geo}]{1}\!\!\!\!\twoheadrightarrow \{\!\{1/2 : 2, 1/2 : \mathrm{geo}(2)\}\!\} \xrightarrow[\mathsf{geo}]{1/2}\!\!\!\!\twoheadrightarrow \{\!\{1/2 : 2, 1/4 : 4, 1/4 : \mathrm{geo}(4)\}\!\} \xrightarrow[\mathsf{geo}]{1/4}\!\!\!\!\twoheadrightarrow \cdots \ .$$

We write $\mu \xrightarrow{w}\!\!\!\!\twoheadrightarrow^{n} \nu$ if $\mu \xrightarrow{w_1}\!\!\!\!\twoheadrightarrow \cdots \xrightarrow{w_n}\!\!\!\!\twoheadrightarrow \nu$ for $w = \sum_{i=1}^{n} w_i$.

Expected cost. A reduction from $a \in A$ is a, generally infinite, sequence $\Delta : \{\!\{1 : a\}\!\} \xrightarrow{w_0}\!\!\!\!\twoheadrightarrow \mu_1 \xrightarrow{w_1}\!\!\!\!\twoheadrightarrow \mu_2 \xrightarrow{w_2}\!\!\!\!\twoheadrightarrow \cdots$. The infinite sum $w = \sum_{i \in \mathbb{N}} w_i \in \mathbb{C}$ gives the *expected cost of this specific reduction*. Due to the presence of non-determinism, expected costs are in general not unique. Taking a demonic

view on non-determinism, we define the *expected cost function*, denoted as $\mathrm{ecost}[\to] : A \to \mathbb{C}$, as the function that associates each $a \in A$ with the maximal expected cost of reductions starting from $\{\!\{1 : a\}\!\}$. Concisely, via the monotone convergence theorem of real numbers this can be defined as

$$\mathrm{ecost}[\to](a) \triangleq \sup\{w \mid \{\!\{1 : a\}\!\} \xrightarrow{w}\!\!\!\!\to^{n} \mu\} \,.$$

For instance, we have $\mathrm{ecost}[\xrightarrow[\mathrm{geo}]{}](\mathrm{geo}(x)) = \sup\{\sum_{i=0}^{n} 1/2^i \mid n \in \mathbb{N}\} = \sum_{i=0}^{\infty} 1/2^i = 2$.

Remark. In the literature, the operational semantics of *purely probabilistic programs*, are usually modelled as Markov chains over program states. Here, the i-th random variable in this chain gives the probability of being in a state after i reduction steps. On the other hand, the operational semantics of languages with non-deterministic choice are modelled in terms of *Markov Decision Processes* (*MDPs*) (see, eg. [Agrawal et al. 2018; Chakarov and Sankaranarayanan 2013; Kaminski et al. 2018; Olmedo et al. 2016]). Schedulers (aka policies) resolve non-deterministic choices based on the current history of states, thereby breaking down reductions again to Markov chains. Such MDPs M are naturally modelled as PARSs $\to_M$, so that the Markov chains induced by the schedulers are in one-to-one correspondence with reductions wrt. $\to_M$. The use of multidistributions, rather than distributions, eliminates the need for schedulers, intuitively, because multidistributions within a reduction implicitly encode histories, cf. Avanzini et al. [2019b]. Particularly, Avanzini et al. [2019b] proves the following correspondence.

Proposition 3.1 ([Avanzini et al. 2019b; Avanzini and Yamada 2020]). *Suppose each rule in the PARS $\to$ is attributed weight one. Then* $\mathrm{ecost}[\to]$ *coincides with the expected time to termination under the standard MDP semantics of Bournez and Garnier [2005].*

While the proposition assumes a unitary cost model, where each reduction step is attributed cost one, the proposition generalises to arbitrary (non-negative) costs as employed in the definition of $\mathrm{ecost}[\to]$.

3.1 Expected Cost Transformers for PARSs

In this section we define an *expected cost transformer* $\mathrm{ect}[\to]$ for arbitrary PARSs $\to$. This transformer, generalising the expected cost function, serves as a technical tool to prove soundness and completeness of our methods.

To this end, we quickly recap notions from program semantics, cf. Winskel [1993]. A poset $(A, \sqsubseteq)$ is called an *ω-CPO*, if every *ω-chain* $a_0 \sqsubseteq a_1 \sqsubseteq \cdots$ has a supremum $\sup\{a_n \mid n \in \mathbb{N}\} \in A$. A function $f : A \to B$ between two ω-CPOs is called *(Scott)-continuous* if $f(\sup_{n\in\mathbb{N}} a_n) = \sup_{n\in\mathbb{N}} f(a_n)$ holds for all ω-chains $(a_n)_{n\in\mathbb{N}}$. Recall that a continuous function is monotone, wrt. the underlying orders of the poset. Kleene's Fixed-Point Theorem asserts that, if $f : A \to A$ is continuous and A features a least element $\bot$, the *least fixed-point* $\mathrm{lfp}(f)$ of f is given $\mathrm{lfp}(f) \triangleq \sup_{n\in\mathbb{N}} f^n(\bot)$ for f^n the n-fold composition of f. Let $\mathbb{C}^A \triangleq \{f \mid f : A \to \mathbb{C}\}$ denote the set of *cost functions* over A. We endow this set with the order $\preceq$ defined by $f \preceq g$ if $f(a) \le g(a)$ for all $a \in A$. We also extend functions over $\mathbb{C}$ point-wise to cost functions and denote these extensions in **bold face** font, as we already did above, eg., $f + g \triangleq \lambda a.f(a) + g(a)$ for $f, g \in \mathbb{C}^A$ etc. In particular, $\mathbf{0} = \lambda a.0$ and $\boldsymbol{\infty} = \lambda a.\infty$. The proof of the following is standard.

Proposition 3.2 (Cost functions form an ω-CPO). *For any A, $(\mathbb{C}^A, \preceq)$ is an ω-CPO, with least and greatest element $\mathbf{0}$ and $\boldsymbol{\infty}$, respectively. The supremum of ω-chains $(f_n)_{n\in\mathbb{N}}$ is given point-wise:* $\sup_{n\in\mathbb{N}} f_n \triangleq \lambda a.\, \sup_{n\in\mathbb{N}} f_n(a)$.

The following definition introduces the expected cost transformer of a PARS $\to$. Informally, this transformer associates each $a \in A$ with its expected cost, plus the expected value of a given cost function f on terminal objects.

Definition 3.3 (Expected Cost Transformer for PARSs). The *expected cost transformer* $\mathrm{ect}[\rightarrow]\colon \mathbb{C}^A \to \mathbb{C}^A$ *for a PARS* $\rightarrow$ is given by $\mathrm{ect}[\rightarrow](f) \triangleq \mathrm{lfp}(\chi_f)$, where the functional $\chi_f\colon \mathbb{C}^A \to \mathbb{C}^A$ is defined as

$$\chi_f(g)(a) \triangleq \begin{cases} f(a) & \text{if } a\!\downarrow, \\ \sup\{w + \mathbb{E}_\mu(g) \mid a \xrightarrow{w} \mu\} & \text{else.} \end{cases}$$

It can be shown that for any f, $\chi_f(g)$ is a continuous functional. Hence $\mathrm{ect}[\rightarrow](f)$ is well-defined. Moreover, it is *continuous* and hence *monotone*.

Lemma 3.4 (Central Properties of $\mathrm{ect}[\rightarrow]$).

(1) continuity*:* $\mathrm{ect}[\rightarrow](\sup_{n\in\mathbb{N}} f_n) = \sup_{n\in\mathbb{N}} \mathrm{ect}[\rightarrow](f_n)$ *for all* ω*-chains* $(f_n)_{n\in\mathbb{N}}$*;*
(2) monotonicity*:* $f \preceq g \implies \mathrm{ect}[\rightarrow](f) \preceq \mathrm{ect}[\rightarrow](g)$.

A standard induction reveals that $\chi_f^n(\mathbf{0})(a) = \sup\{w \mid a \xrightarrow{w}\!\!\!\!\rightarrow^{n} \mu\}$, where χ_f^n denotes the n-fold composition of χ_f. Consequently, the next result follows by Kleene's Fixed-Point Theorem.

Theorem 3.5 (Expected Cost via Cost Transformer).

$$\mathrm{ecost}[\rightarrow] = \mathrm{ect}[\rightarrow](\mathbf{0})\ .$$

4 A PROBABILISTIC LANGUAGE

We consider an *imperative language* pWhile in the spirit of Dijkstra's *Guarded Command Language*, endowed with a non-deterministic choice operator <> and where the assignment statement is generalised to one that can sample from a distribution. A command `consume`(e) signals the consumption of $e \geq 0$ resource units.

We fix a finite set of integer-valued *variables* Var. *Stores* are denoted by $\sigma \in \Sigma \triangleq \mathsf{Var} \to \mathbb{Z}$. With $\phi \in \mathsf{BExp} \triangleq \Sigma \to \mathbb{B}$, $e \in \mathsf{Exp} \triangleq \Sigma \to \mathbb{Z}$, and $d \in \mathsf{DExp} \triangleq \Sigma \to \mathcal{D}(\mathbb{Z})$ we denote, *Boolean*, *Integer*, and *Integer-valued distribution expression* over Var, respectively. The syntax of *program commands* Cmd is given as follows.

$$\mathtt{C}, \mathtt{D} ::= x \coloneqq d \mid \mathtt{skip} \mid \mathtt{abort} \mid \mathtt{consume}(e) \mid \mathtt{C};\mathtt{D} \mid \mathtt{if}\ (\phi)\ \{\mathtt{C}\}\ \{\mathtt{D}\} \mid \mathtt{while}\ (\phi)\ \{\mathtt{C}\} \mid \{\mathtt{C}\}\ \mathtt{<>}\ \{\mathtt{D}\}\ .$$

Commands are fairly standard. The assignment statement $x \coloneqq d$ samples a value from d, ie. an expression that evaluates to a distribution over integers. This command generalises the usual non-probabilistic assignment $x \coloneqq e$. The command `consume`(e) consumes e resource units but acts as a no-op otherwise. Here e is a non-negative but otherwise arbitrary integer-valued expression. Particularly, the incurred cost can depend on the programs state rather than being constant. The non-deterministic choice operator {C} <> {D} executes either C or D. For brevity, we omit a probabilistic choice command and probabilistic guards as by Kaminski et al. [2016], since they do not add to the expressiveness of our language.

Semantics. We model reduction semantics of our language as a PARS over *configurations* $\mathsf{Conf} \triangleq (\mathsf{Cmd} \times \Sigma) \cup \Sigma$. Elements $(\mathtt{C}, \sigma) \in \mathsf{Conf}$ are denoted by $\sigma \triangleright \mathtt{C}$ and signal that the command C is to be executed under the current store σ, whereas $\sigma \in \mathsf{Conf}$ indicates that the computation has halted with final store σ. The (infinite) PARS is depicted in Figure 2. Rules $\sigma \triangleright \mathtt{C} \xrightarrow{w} \{\!\{1 : \gamma\}\!\}$ without probabilistic effect are written as $\sigma \triangleright \mathtt{C} \xrightarrow{w} \gamma$ for brevity. For $\phi \in \mathsf{BExp}$ and $\sigma \in \Sigma$ we denote by $\sigma \vDash \phi$ that ϕ evaluates on σ to true. Note that only in Rule (Consume) resources are consumed. Here, $\langle z \rangle \triangleq \max(0, z)$ denotes *Macaulay brackets*. As we had for PARSs, incurred costs are thus always non-negative.

$$\frac{}{\sigma \triangleright x \coloneqq d \xrightarrow{0} \{\!\{p_i : \sigma[x/i] \mid p_i = d(\sigma)(i) > 0\}\!\}_{i\in\mathbb{Z}}}\ [\textsc{Assign}]$$

$$\frac{}{\sigma \triangleright \mathtt{skip} \xrightarrow{0} \sigma}\ [\textsc{Skip}] \qquad \frac{}{\sigma \triangleright \mathtt{abort} \xrightarrow{0} \varnothing}\ [\textsc{Abort}] \qquad \frac{}{\sigma \triangleright \mathtt{consume}(e) \xrightarrow{\langle e(\sigma)\rangle} \sigma}\ [\textsc{Consume}]$$

$$\frac{\sigma \vDash \phi}{\sigma \triangleright \mathtt{if}\ (\phi)\ \{\mathtt{C}\}\ \{\mathtt{D}\} \xrightarrow{0} \sigma \triangleright \mathtt{C}}\ [\textsc{IfT}] \qquad \frac{\sigma \nvDash \phi}{\sigma \triangleright \mathtt{if}\ (\phi)\ \{\mathtt{C}\}\ \{\mathtt{D}\} \xrightarrow{0} \sigma \triangleright \mathtt{D}}\ [\textsc{IfF}]$$

$$\frac{\sigma \vDash \phi}{\sigma \triangleright \mathtt{while}\ (\phi)\ \{\mathtt{C}\} \xrightarrow{0} \sigma \triangleright \mathtt{C};\mathtt{while}\ (\phi)\ \{\mathtt{C}\}}\ [\textsc{WhileT}] \qquad \frac{\sigma \nvDash \phi}{\sigma \triangleright \mathtt{while}\ (\phi)\ \{\mathtt{C}\} \xrightarrow{0} \sigma}\ [\textsc{WhileF}]$$

$$\frac{i \in \{1,2\}}{\sigma \triangleright \{\mathtt{C}_1\} <> \{\mathtt{C}_2\} \xrightarrow{0} \sigma \triangleright \mathtt{C}_i}\ [\textsc{Choice}] \qquad \frac{\sigma \triangleright \mathtt{C} \xrightarrow{r} \{\!\{p_i : \sigma_i \triangleright \mathtt{C}_i\}\!\}_{i\in I} \uplus \{\!\{q_j : \sigma_j\}\!\}_{j\in J}}{\sigma \triangleright \mathtt{C};\mathtt{D} \xrightarrow{r} \{\!\{p_i : \sigma_i \triangleright \mathtt{C}_i;\mathtt{D}\}\!\}_{i\in I} \uplus \{\!\{q_j : \sigma_j \triangleright \mathtt{D}\}\!\}_{j\in J}}\ [\textsc{Compose}]$$

Fig. 2. Small-step operational semantics as a PARS.

C	ect[C](f)	evalue[C](f)
consume(e)	$\langle e\rangle + f$	f
skip	f	f
abort	$\mathbf{0}$	$\mathbf{0}$
$x \coloneqq d$	$\lambda\sigma.\mathbb{E}_{d(\sigma)}(\lambda v.f[x/v](\sigma))$	$\lambda\sigma.\mathbb{E}_{d(\sigma)}(\lambda v.f[x/v](\sigma))$
C;D	ect[C](ect[D](f))	evalue[C](evalue[D](f))
if (ϕ) {C} {D}	$[\phi]\cdot \mathrm{ect}[\mathtt{C}](f) + [\neg\phi]\cdot \mathrm{ect}[\mathtt{D}](f)$	$[\phi]\cdot \mathrm{evalue}[\mathtt{C}](f) + [\neg\phi]\cdot \mathrm{evalue}[\mathtt{D}](f)$
while (ϕ) {C}	$\mathrm{lfp}(\lambda F.[\phi]\cdot \mathrm{ect}[\mathtt{C}](F) + [\neg\phi]\cdot f)$	$\mathrm{lfp}(\lambda F.[\phi]\cdot \mathrm{evalue}[\mathtt{C}](F) + [\neg\phi]\cdot f)$
{C} <> {D}	$\mathbf{max}(\mathrm{ect}[\mathtt{C}](f), \mathrm{ect}[\mathtt{D}](f))$	$\mathbf{max}(\mathrm{evalue}[\mathtt{C}](f), \mathrm{evalue}[\mathtt{D}](f))$

Fig. 3. Definition of expected cost transformer ect[C] and expected value function evalue[C]. Notice that their definition coincides up to the case C = consume(e).

5 EXPECTED COST AND EXPECTED VALUE TRANSFORMERS

We now suite the ert-transformer of Kaminski et al. [2016] to an *expected cost transformer*. To this end, for $\phi \in \mathrm{BExp}$, we lift *Iverson brackets* $[\cdot]$ to stores, resulting in the cost function $[\phi](\sigma) \triangleq 1$ if $\sigma \vDash \phi$, and $[\phi](\sigma) \triangleq 0$ otherwise. In particular, $[\phi]\cdot f + [\neg\phi]\cdot g$ evaluates to $f(\sigma)$ on stores $\sigma \vDash \phi$, and to $g(\sigma)$ if $\sigma \vDash \neg\phi$. We denote by $f[x/v]$ the cost function that applies f on the modified store where x takes value v.

Our *expected cost transformer* $\mathrm{ect}[\cdot](\cdot)\colon \mathrm{Cmd} \to \mathbb{C}^\Sigma \to \mathbb{C}^\Sigma$ operates on cost functions over stores, that is, elements of $\mathbb{C}^\Sigma$. In the literature $f \in \mathbb{C}^\Sigma$ are also referred to as *expectations* [Kaminski et al. 2016]. The cost $\mathrm{ect}[\mathtt{C}](f)$ should be seen as the cost of evaluating C wrt. to a continuation of expected cost f.

Definition 5.1 (Expected Cost Transformer). The *expected cost transformer* $\mathrm{ect}[\cdot](\cdot)\colon \mathrm{Cmd} \to \mathbb{C}^\Sigma \to \mathbb{C}^\Sigma$ for *commands* C is defined through the rules given in the second column in Figure 3. For $\mathtt{C} \in \mathrm{Cmd}$, we set $\mathrm{ecost}[\mathtt{C}] \triangleq \mathrm{ect}[\mathtt{C}](\mathbf{0})$ and call $\mathrm{ecost}[\mathtt{C}]$ the expected cost of C.

Remark. The earlier defined expected cost transformer $\mathrm{ect}[\to]$ *wrt. PARS* $\to$ (see Section 3) abstracts the above definition of the expected cost transformer *wrt. programs* C. As we see in equation (‡), these are in correspondence. Hence, we take the liberty to employ the same notations.

With the above intuition in mind, most of the cases are straight forward to derive from the operational semantics given in Figure 2. In the case of a statement consume(e), a cost of e is

incurred (provided $e(\sigma) \geq 0$) in addition to the cost of the continuation. While `skip` is a no-op, consequently $\mathrm{ect}[\mathtt{skip}](f) = f$, the command `abort` immediately aborts the computation and thus $\mathrm{ect}[\mathtt{abort}](f) = \mathbf{0}$. Running an assignment $x \coloneqq d$ followed by a continuation amounts to first sampling a value v for x according to d, say with probability p_v, updating x in the given store σ to v, and then running the continuation on the updated store. The overall expected resource consumption is thus given by the sum of expected costs $f[x/v]$ of all such runs, weighted by their probability p_v. If $\mathtt{Bernoulli}(p)$ denotes the Bernoulli distribution with parameter p, (yielding 1 with probability p and 0 with probability $p-1$), then

$$\mathrm{ect}[x \coloneqq \mathtt{Bernoulli}(1/3)](f) = \mathbf{1/3} \cdot f[x/\mathbf{1}] + \mathbf{2/3} \cdot f[x/\mathbf{0}] \ .$$

For sequential commands `C`; `D`, $\mathrm{ect}[\mathtt{C};\mathtt{D}]$ is given by the composition $\mathrm{ect}[\mathtt{C}] \circ \mathrm{ect}[\mathtt{D}]$, transforming the cost f of a continuation to that of running `C`, then `D` followed by the continuation. For conditionals $\mathtt{if}\ (\phi)\ \{\mathtt{C}\}\ \{\mathtt{D}\}$, the transformer perform a case analysis on the guard. Considering loops $\mathtt{while}\ (\phi)\ \{\mathtt{C}\}$, the expected cost transformer is defined as the least fixed-point of the functional

$$\lambda F.[\phi] \cdot \mathrm{ect}[\mathtt{C}](F) + [\neg\phi] \cdot f \ . \tag{1}$$

We will see below that this fixed-point is always defined. The transformer $\mathrm{ect}[\mathtt{while}\ (\phi)\ \{\mathtt{C}\}]$ thus in particular enjoys

$$\begin{aligned} \mathrm{ect}[\mathtt{while}\ (\phi)\ \{\mathtt{C}\}](f) &= [\phi] \cdot \mathrm{ect}[\mathtt{C}](\mathrm{ect}[\mathtt{while}\ (\phi)\ \{\mathtt{C}\}](f)) + [\neg\phi] \cdot f \\ &= [\phi] \cdot \mathrm{ect}[\mathtt{C};\mathtt{while}\ (\phi)\ \{\mathtt{C}\}](f) + [\neg\phi] \cdot f \ , \end{aligned}$$

that is, it evaluates to the cost of unfolding the loop when the loop's guard ϕ is satisfied, and otherwise returns the cost f, in correspondence to the semantics. Finally, the transformer on non-deterministic choices maximises over expected costs along the two branches.

5.1 Well-definedness and Soundness

Before we prove soundness, let us mention that as for the expected cost transformer on PARSs, $\mathrm{ect}[\mathtt{C}]$ is continuous, and consequently also monotone, in the following sense:

Lemma 5.2 (Central Properties of $\mathrm{ect}[\mathtt{while}\ (\phi)\ \{\mathtt{C}\}]$).

(1) continuity*:* $\mathrm{ect}[\mathtt{C}](\sup_{n\in\mathbb{N}} f_n) = \sup_{n\in\mathbb{N}} \mathrm{ect}[\mathtt{C}](f_n)$ *for all* ω*-chains* $(f_n)_{n\in\mathbb{N}}$*;*
(2) monotonicity*:* $f \preceq g \implies \mathrm{ect}[\mathtt{C}](f) \preceq \mathrm{ect}[\mathtt{C}](g)$.

In particular, continuity ensures that in the case for loop $\mathtt{C} = \mathtt{while}\ (\phi)\ \{\mathtt{D}\}$, the least fixed point underlying $\mathrm{ect}[\mathtt{C}]$ is well-defined. Now that we have established that $\mathrm{ect}[\mathtt{C}](f)$, and hence $\mathrm{ecost}[\mathtt{C}]$, is well-defined, the remaining objective of this section is to prove that $\mathrm{ecost}[\mathtt{C}](\sigma)$ indeed gives the expected cost of running `C` on store σ. To this end, we show that $\mathrm{ect}[\mathtt{C}](f)(\sigma)$ coincides with $\mathrm{ect}[\to](f)(\sigma \triangleright \mathtt{C})$ defined in terms of the underlying PARS in Section 3.

Let us denote by $\mathrm{ect}[\to](f)(\bullet \triangleright \mathtt{C})$ the function $\lambda\sigma.\mathrm{ect}[\to](f)(\sigma \triangleright \mathtt{C})$. The correspondence thus becomes

$$\mathrm{ect}[\mathtt{C}](f) = \mathrm{ect}[\to](f)(\bullet \triangleright \mathtt{C}) \ . \tag{‡}$$

Since the definition of $\mathrm{ect}[\mathtt{C}](f)$ is guided by the semantics, for most commands `C` this equality is immediate. The only non-trivial cases are that of composition and loops. The following lemma links the corresponding cases.

Lemma 5.3 (Composition and Loop Lemma).

(1) $\mathrm{ect}[\to](f)(\bullet \triangleright \mathtt{C};\mathtt{D}) = \mathrm{ect}[\to](\mathrm{ect}[\to](f)(\bullet \triangleright \mathtt{D}))(\bullet \triangleright \mathtt{C})$*;*
(2) $\mathrm{ect}[\to](f)(\bullet \triangleright \mathtt{while}\ (\phi)\ \{\mathtt{C}\}) = \mathsf{lfp}(g.[\phi] \cdot \mathrm{ect}[\to](g)(\bullet \triangleright \mathtt{C}) + [\neg\phi] \cdot f)$.

Note that the right-hand side in (2) is well-defined by Lemma 3.4(1). Relying on this auxiliary lemma, our central soundness result follows by a standard induction on $\mathtt{C}$.

Theorem 5.4 (Soundness & Completeness). *For every command* $\mathtt{C} \in \mathsf{Cmd}$, *we have*
(1) $\mathsf{ect}[\to](f)(\bullet \triangleright \mathtt{C}) = \mathsf{ect}[\mathtt{C}](f)$*; and consequently*
(2) $\mathsf{ecost}[\to](\bullet \triangleright \mathtt{C}) = \mathsf{ecost}[\mathtt{C}]$.

The theorem thus witnesses that the expected cost transformer of this section gives a sound and complete method for reasoning about the expected cost of programs $\mathtt{C}$.

5.2 Upper Invariants

To find closed-forms for the runtime of loops, Kaminski et al. [2016] propose to search for *upper invariants*, ie. prefix points of the loops characteristic function. The following constitutes a straight forward generalisation of Kaminski et al. [2016, Theorem 3]. For a Boolean expression $\phi \in \mathsf{BExp}$, and two cost functions $f, g \in \mathbb{C}^{\Sigma}$, let us denote by $\phi \vDash f \preceq g$ that $f(\sigma) \leq g(\sigma)$ holds for all stores σ with $\phi \vDash \sigma$.

Theorem 5.5 (Upper Invariant). *Let* $I \in \mathbb{C}^{\Sigma}$. *If* $\phi \vDash \mathsf{ect}[\mathtt{C}](I) \preceq I$ *and* $\neg\phi \vDash f \preceq I$, *then*

$$\mathsf{ect}[\mathtt{while}\ (\phi)\ \{\mathtt{C}\}](f) \preceq I\ .$$

Observe that the two premises are equivalent to $[\phi] \cdot \mathsf{ect}[\mathtt{C}](I) + [\neg\phi] \cdot f \preceq I$, that is, I is a pre-fixed point of the functional $\lambda F.[\phi] \cdot \mathsf{ect}[\mathtt{C}](F) + [\neg\phi] \cdot f$. The theorem is thus a reformulation of the fact that the least fixed-point is the least among all its pre-fixed points. Via this theorem, the problem of computing $\mathsf{ecost}[\mathtt{C}]$ can be reduced to a set of inequalities whose solution gives an *upper bound* on the expected cost of $\mathtt{C}$. Let us illustrate this on a simple example.

Example 5.6. Reconsider the program $\mathtt{C}_{\mathrm{geo}}$ from Figure 1b and let $\mathtt{D}$ denote the body of the loop in $\mathtt{C}_{\mathrm{geo}}$. A cost expression I is an upper invariant for this loop wrt. f if (i) $b = 1 \vDash \mathsf{ect}[\mathtt{D}](I) \preceq I$; (ii) $b \neq 1 \vDash f \preceq I$ holds. Unfolding the definition of $\mathsf{ect}[\mathtt{D}](I)$ yields

$$\mathsf{ect}[\mathtt{D}](I) = 1 + (I[b/1, x/2 \cdot x] + I[b/0, x/2 \cdot x])/2\ .$$

Define now $I \triangleq [b = 1] \cdot 2 + f$, that is, I evaluates to $2 + f(\sigma)$ on stores σ with $b = 1$ and behaves like f otherwise. In particular, $I[b/1, x/2 \cdot x] = 2 + f$ and $I[b/0, x/2 \cdot x] = f$. The upper invariant condition thus simplifies to $b = 1 \vDash 2 + f \preceq [b = 1] \cdot 2 + f$ and $b \neq 1 \vDash f \preceq [b = 1] \cdot 2 + f$. A case analysis on $b = 1$ then shows that left- and right-hand sides are actually equal. Since in $\mathtt{C}_{\mathrm{geo}}$, the variable b and x are initially set to one, we obtain $\mathsf{ecost}[\mathtt{C}_{\mathrm{geo}}] = I[b/1, x/1] = 2$ as a consequence of Theorem 5.4 and Theorem 5.5.

Theorem 5.5 suggests the following two stage approach towards an automated cost analysis of a program $\mathtt{C}$ via Theorem 5.4. (i) evaluate $\mathsf{ecost}[\mathtt{C}] = \mathsf{ect}[\mathtt{C}](\mathbf{0})$ symbolically and generating a constraint corresponding to the the upper invariant condition; and (ii) synthesise concrete upper invariants via the collection of generated constraints.

This is akin to the common approach, where cost functions are specified as linear combination over an (arbitrary but fixed) finite vector of *base functions* $(b_1, \ldots, b_k)$, itself cost functions, abstracting stores as non-negative numbers. Such cost expressions take the form $\boldsymbol{\kappa}(b_1, \ldots, b_k)$, where $\kappa(r_1, \ldots, r_k) = \sum_i q_i \cdot r_i$ for rational (in particular real) numbers q_i. Upper invariants then take the form $\phi \vDash \mathsf{ect}[\mathtt{C}](\boldsymbol{\kappa_I}(b_1, \ldots, b_k)) \preceq \boldsymbol{\kappa_I}(b_1, \ldots, b_k)$ and $\neg\phi \vDash \boldsymbol{\kappa_f}(b_1, \ldots, b_k) \preceq \boldsymbol{\kappa_I}(b_1, \ldots, b_k)$.

By treating κ_I and κ_f as undetermined, these constraints can be reduced to inequalities over expressions on coefficients in such a way that the resulting set of constraints is e.g. amenable to Linear Programming. A solution to these constraints, viz, particularly concrete values for the

coefficients q_i occurring in κ_I, then yields a concrete upper invariant. Consequently, an upper bound to the expected cost of `while` (ϕ) {C} in terms of the base functions $\vec{b}$ is inferred.

6 ALTERNATING EXPECTED COST AND VALUE ANALYSIS

While the calculus developed in the previous section is indeed compositional, the cost analysis via Theorem 5.5, as described above, is not. This is most apparent in the case of nested loops, abstractly represented as follows:

$$\texttt{while}\ (\phi)\ \{\texttt{while}\ (\psi)\ \{\texttt{C}\}\}\ .$$

The synthesis of upper invariants I and O for the inner and outer loops, respectively, wrt. a cost function f, is driven by the following inter-dependent constraints, compare the exposition of the trader example in Section 2.

$$\phi \vDash I \preceq O \quad \wedge \quad \neg\phi \vDash f \preceq O \quad \wedge \quad \psi \vDash \mathrm{ect}[\texttt{C}](I) \preceq I \quad \wedge \quad \neg\psi \vDash O \preceq I\ .$$

These constraints cannot be considered in isolation. In particular, if we express I and O in terms of linear combinations $\boldsymbol{\kappa}_I(b_1,\ldots,b_k)$ and $\boldsymbol{\kappa}_O(b_1,\ldots,b_k)$ of base functions b_i, the undetermined combinators κ_I and κ_O cannot be synthesised separately. Thus, the analysis degenerates to a *whole-program analysis*.

As emphasised in Section 2, in the *non-probabilistic* setting modularity of a cost analysis is facilitated through combining cost analysis with an analysis on how stores evolve through the execution of program parts. In the following, we suit this conceptual simple idea to an expected cost analysis.

The result of a program C, run on an initial store σ, is conceivable as a subdistribution μ over stores (many, in the case C is also non-deterministic). Then $\mathrm{ect}[\texttt{C}](f)(\sigma)$ yields the expected cost of C plus the *expected value* $\mathbb{E}_\mu(f)$ of the cost function f on the distribution of states μ. When f coincides with the cost of a continuation, we re-obtain the initial intuition that $\mathrm{ect}[\texttt{C}](f)$ yields the cost of running C followed by the corresponding continuation. We make this correspondence precise. First, we define the expected value transformer $\mathrm{evalue}[\texttt{C}]$ of a command C in correspondence to $\mathrm{ect}[\texttt{C}]$, while ignoring costs.

Definition 6.1 (Expected Value Transformer). The *expected value transformer* $\mathrm{evalue}[\texttt{C}] \colon \mathbb{C}^\Sigma \to \mathbb{C}^\Sigma$ for *commands* C is defined through the rules given in the third column in Figure 3.

Note that $\mathrm{evalue}[\texttt{C}](f) = \mathrm{ect}[\mathrm{costFree}(\texttt{C})](f)$ holds, where the *cost-free program* $\mathrm{costFree}(\texttt{C})$ is obtained from C by dropping all cost annotations $\texttt{consume}(e)$. Particularly, Theorem 5.5 remains intact if we substitute $\mathrm{evalue}[\cdot]$ for $\mathrm{ect}[\cdot]$. The next lemma establishes a separation of the expected cost and value computation, which underlies the expected cost transformer $\mathrm{ect}[\texttt{C}]$.

Lemma 6.2 (Separating Expected Cost and Value).

$$\mathrm{ect}[\texttt{C}](f) \preceq \mathrm{ecost}[\texttt{C}] + \mathrm{evalue}[\texttt{C}](f)\ .$$

If C features non-determinism, the right-hand side may over-approximate $\mathrm{ect}[\texttt{C}](f)$. Whereas in $\mathrm{ect}[\texttt{C}](f)$ cost and expected values are kept in sync across branches, this property is lost when considering $\mathrm{ecost}[\texttt{C}]$ and $\mathrm{evalue}[\texttt{C}](f)$ independently. A similar result, albeit restricted to purely probabilistic programs, has been observed by Kaminski et al. [2018, Thm 8.1].

Consider a while loop, `while` (ϕ) {C}. As above, we express the upper invariant I as the combination $\boldsymbol{\kappa}(b_1,\ldots,b_k)$ of base functions b_i. Reconsider the first premise of Theorem 5.5: $\phi \vDash \mathrm{ect}[\texttt{C}](\boldsymbol{\kappa}(b_1,\ldots,b_k)) \preceq \boldsymbol{\kappa}(b_1,\ldots,b_k)$. By Lemma 6.2, this constraint is entailed by

$$\phi \vDash \mathrm{ecost}[\texttt{C}] + \mathrm{evalue}[\texttt{C}](\boldsymbol{\kappa}(b_1,\ldots,b_k)) \preceq \boldsymbol{\kappa}(b_1,\ldots,b_k)\ , \tag{2}$$

Moreover, when the upper invariant κ is linear in all its arguments, it distributes over expectations and hence over the expected value transformer evalue[C]. Consequently (2) becomes

$$\phi \vDash \mathrm{ecost}[\mathtt{C}] + \boldsymbol{\kappa}(\mathrm{evalue}[\mathtt{C}](b_1), \ldots, \mathrm{evalue}[\mathtt{C}](b_k)) \preceq \boldsymbol{\kappa}(b_1, \ldots, b_k) \; . \tag{3}$$

First, this decomposes the analysis of the cost of the loop's body C from the analysis of how $\boldsymbol{\kappa}(b_1, \ldots, b_k)$ changes in expectation during one iteration. Second, none of the calls to evalue[C] do reference the combinator κ. These can be determined in independence of the analysis of $\mathtt{while}\ (\phi)\ \{\mathtt{C}\}$. We generalise this observation. As usual, we call κ *concave* if $p \cdot \kappa(\vec{r}) + (1-p) \cdot \kappa(\vec{s}) \leq \kappa(p \cdot \vec{r} + (1-p) \cdot \vec{s})$ (where $0 \leq p \leq 1$) and (weakly) *monotone* if $\vec{r} \leq \vec{s}$ implies $\kappa(\vec{r}) \leq \kappa(\vec{s})$. Together, the two conditions yield the following sufficient criterion to distribute κ over expectations.

Lemma 6.3 (Distribute over Expected Values). *Suppose* $\kappa \colon \mathbb{C}^k \to \mathbb{C}$ *is monotone. Furthermore, suppose* κ *is concave if the command* C *is probabilistic. Then* $\mathrm{evalue}[\mathtt{C}](\boldsymbol{\kappa}(b_1, \ldots, b_k)) \preceq \boldsymbol{\kappa}(\mathrm{evalue}[\mathtt{C}](b_1), \ldots, \mathrm{evalue}[\mathtt{C}](b_k))$.

Note that concavity is only needed to distribute κ over the expected value given by *probabilistic* statements, that is, probabilistic assignments from non-dirac distributions. On the other hand, it is not difficult to design an example showing the necessity of the restriction to concavity in this case.

The above lemmas in conjunction with Theorem 5.5 yields the main result of this section.

Theorem 6.4 (Modular Upper-Invariants). *Let* C *and* κ *be as in Lemma 6.3. Then*

1. $\phi \vDash \mathrm{ecost}[\mathtt{C}] + \boldsymbol{\kappa}(\mathrm{evalue}[\mathtt{C}](b_1), \ldots, \mathrm{evalue}[\mathtt{C}](b_k)) \preceq I \Rightarrow \mathrm{ecost}[\mathtt{while}\ (\phi)\ \{\mathtt{C}\}] \preceq I$;
2. $\phi \vDash \boldsymbol{\kappa}(\mathrm{evalue}[\mathtt{C}](b_1), \ldots, \mathrm{evalue}[\mathtt{C}](b_k)) \preceq I \wedge \neg\phi \vDash f \preceq I \Rightarrow \mathrm{evalue}[\mathtt{while}\ (\phi)\ \{\mathtt{C}\}](f) \preceq I$.

Note that in the first point, we discharge the pre-condition $f = \mathbf{0} \preceq I$ in Theorem 5.5. Concerning the second point, we exploit $\mathrm{evalue}[\mathtt{while}\ (\phi)\ \{\mathtt{C}\}](f) = \mathrm{ect}[\mathtt{while}\ (\phi)\ \{\mathrm{costFree}(\mathtt{C})\}](f)$ and $\mathrm{ecost}[\mathrm{costFree}(\mathtt{C})] = \mathbf{0}$. The theorem gives a *modular recursive procedure* to infer upper bounds on costs of loops, as follows, cf. Section 7. (i) Estimate the cost of one iteration of the body C. (ii) Analyse how the expected value of the base functions b_i is changed by one iteration of the body changes, as formalises in the expected value transformer. (iii) Solve the recurrence, given by the implication, where $\boldsymbol{\kappa}$ is to be determined. Crucially the loop's body C becomes treatable in complete independence of the loop itself. Via Lemma 6.2 and Lemma 6.3, sequential composition can be treated similarly to Theorem 6.4.

Theorem 6.5 (Modular Sequential Analysis). *Let* C *and* κ *be as in Lemma 6.3. Then*

1. $\mathrm{ecost}[\mathtt{D}](f) \preceq \boldsymbol{\kappa}(b_1, \ldots, b_k) \Rightarrow \mathrm{ecost}[\mathtt{C};\mathtt{D}] \preceq \mathrm{ecost}[\mathtt{C}] + \boldsymbol{\kappa}(\mathrm{evalue}[\mathtt{C}](b_1), \ldots, \mathrm{evalue}[\mathtt{C}](b_k))$;
2. $\mathrm{evalue}[\mathtt{D}](f) \preceq \boldsymbol{\kappa}(b_1, \ldots, b_k) \Rightarrow \mathrm{evalue}[\mathtt{C};\mathtt{D}](f) \preceq \boldsymbol{\kappa}(\mathrm{evalue}[\mathtt{C}](b_1), \ldots, \mathrm{evalue}[\mathtt{C}](b_k))$.

6.1 Analysis of Examples

We conclude the section, by discussing the analysis of the running examples of Section 2 using our methodology. Further, we briefly comment on an interesting example by Wang et al. [2019] modelling a *fork-join queues*. Noteworthy, all displayed bounds are derived via our implementation `eco-imp` as detailed in the following section.

Geo. Reconsider the program $\mathtt{C}_{\mathrm{geo}}$ (Figure 1b), where the cost is given by the number of loop iterations. Since loop-iterations depend on the value of b, we choose the base function $\langle b \rangle$. This is sufficient to handle $\mathtt{C}_{\mathrm{geo}}$ via Theorem 6.4(1). The body D of the loop changes $\langle b \rangle$ to $\mathbf{1/2} \cdot \langle \mathbf{0} \rangle + \mathbf{1/2} \cdot \langle \mathbf{1} \rangle = \mathbf{1/2}$ in expectation. Moreover, the cost of a single loop iteration ecost[D] is one, which follows by unfolding the definition. By Theorem 6.4(1), $\boldsymbol{\kappa}(\langle b \rangle)$ is an upper bound to the cost of the loop if

$$b = 1 \vDash \mathrm{ecost}[\mathtt{D}] + \boldsymbol{\kappa}(\mathrm{evalue}[\mathtt{D}](\langle b \rangle)) \preceq \boldsymbol{\kappa}(\langle b \rangle) \quad \Leftrightarrow \quad b = 1 \vDash \mathbf{1} + \boldsymbol{\kappa}(\mathbf{1/2}) \preceq \boldsymbol{\kappa}(\langle b \rangle) \; .$$

A case analysis on $b = 1$ shows that the constraint is satisfied with $\kappa(x) \triangleq 2 \cdot x$. Finally, since $b \coloneqq 1$ before entering the loop we derive the optimal bound $\kappa(\langle \mathbf{1} \rangle) = \mathbf{2}$ for $\mathsf{C}_{\mathsf{geo}}$.

Trader. Recall program $\mathsf{C}_{\mathsf{trader}}$ from Figure 1a. It is not difficult to see that the cost of the inner loop is given by $\langle n \rangle \cdot \langle price \rangle$. This then yields

$$\mathrm{ecost}[\mathtt{D}] = \mathbf{1/44} \cdot \textstyle\sum_{n=0}^{10} n \cdot \langle price + \mathbf{1} \rangle + \mathbf{3/44} \cdot \sum_{n=0}^{10} n \cdot \langle price - \mathbf{1} \rangle \ ,$$

as bound the cost of the body $\mathtt{D}$ of the outer loop. Wrt. the outer loop itself, consider the base functions $b_1 \triangleq \langle min + \mathbf{1} \rangle \cdot \langle price - min \rangle$ and $b_2 \triangleq \langle price - min \rangle^2$. Applying Theorem 6.4(1), the cost of $\mathsf{C}_{\mathsf{trader}}$ is given by $\boldsymbol{\kappa}(b_1, b_2)$ subject to the constraint

$$\mathbf{0} \leq min \leq price - \mathbf{1} \vDash \mathrm{ecost}[\mathtt{D}] + \boldsymbol{\kappa}(\mathrm{evalue}[\mathtt{D}](b_1), \mathrm{evalue}[\mathtt{D}](b_2)) \leq \boldsymbol{\kappa}(b_1, b_2) \ .$$

Note that the loop body $\mathtt{D}$ increments and decrements the price with probabilities $1/4$ and $3/4$, respectively, whereas *min* remains unchanged. Formally,

$$\mathrm{evalue}[\mathtt{D}](b_1) = 1/4 \cdot \langle min + \mathbf{1} \rangle \cdot \langle price + 1 - min \rangle + 3/4 \cdot \langle min + \mathbf{1} \rangle \cdot \langle price - 1 - min \rangle \ ,$$
$$\mathrm{evalue}[\mathtt{D}](b_2) = 1/4 \cdot \langle price + 1 - min \rangle^2 + 3/4 \cdot \langle price - 1 - min \rangle^2 \ ,$$

which can be derived by unfolding evalue[D] and applying Theorem 6.4(2). In turn, the above constraint holds with $\kappa(x, y) \triangleq 10 \cdot x + 5 \cdot y$, yielding an upper bound

$$\boldsymbol{\kappa}(b_1, b_2) = \mathbf{10} \cdot \langle min + \mathbf{1} \rangle \cdot \langle price - min \rangle + \mathbf{5} \cdot \langle price - min \rangle^2 \ ,$$

on the cost of $\mathsf{C}_{\mathsf{trader}}$. Note that this upper bound can be derived with our implementation in 25s.

Coupon Collector. Recall program $\mathsf{C}_{\mathsf{coupons}}$ of Figure 1c, and let $\mathtt{D}$ denote the main loop's body. While $\mathrm{ecost}[\mathtt{D}] = 1$ is straight forward to derive, the challenge of this example lies in calculating the expected value of base functions, due to the sampling instruction. Particularly, for a base function b, $\mathrm{evalue}[\mathtt{D}](b)$ is given by

$$[\mathbf{1} \leq n] \cdot \textstyle\sum_{draw=1}^{n} \big([coupons < draw] \cdot b[coupons/coupons + \mathbf{1}] + [draw \leq coupons] \cdot b \big) / n \ .$$

Our implementation selects, among others, the base functions $b_1 \triangleq \langle n - coupons \rangle^2$ and $b_2 \triangleq \langle n - coupons \rangle \cdot \langle coupons + 1 \rangle$ from the loop guard, for which it derives bounds

$$b_1' \triangleq \langle n - coupons \rangle \cdot (\langle n - coupons - 1 \rangle^2 + \langle n - coupons \rangle \cdot \langle coupons \rangle) / \langle n \rangle$$
$$b_2' \triangleq \langle n - coupons \rangle \cdot (\langle n - coupons - 1 \rangle \cdot \langle coupons + \mathbf{2} \rangle + \langle coupons + \mathbf{1} \rangle \cdot \langle coupons \rangle) / \langle n \rangle \ ,$$

for $\mathrm{ect}[\mathtt{D}](b_i)$. The constraint $\mathbf{0} \leq i \leq n - \mathbf{1} \vDash \mathbf{1} + \boldsymbol{\kappa}(b_1', b_2') \leq \boldsymbol{\kappa}(b_1, b_2)$, describing the cost of the loop, is then shown satisfiable by taking $\kappa(x, y) \triangleq x + 1/2 \cdot y$. Substituting $\mathbf{0}$ for *coupons* in the bound $\boldsymbol{\kappa}(b_1, b_2)$ due to the initial assignments yields the overall estimate $\langle n \rangle + \mathbf{1/2} \cdot \langle n \rangle^2$ for the expected cost of $\mathsf{C}_{\mathsf{coupons}}$. This analysis was performed in 195ms with our tool.

Queuing Network. Wang et al. [2019] represent fork-join queues (see Kim and Agrawala [1989]) for 2 servers as a probabilistic program with a unitary cost model, that measures progress of the sub-jobs in the respective queues. A fixed probability is employed to model the arrival of new jobs, while n jobs are processes. With probability $\frac{1}{5}$ the job is handled by the first server and with probability $\frac{1}{2}$ by the second server. In the default, the job is passed to both servers. Server 1 takes 3 units for completion, while Server 2 takes 2 time units. If the job is split on the servers, the Server 1 and 2 require 2 and 1 time units, respectively. The cost for the fork-join queue is given by the expected time of completion of each job. Our prototype computes the (asymptotically) optimal bound $113/741\langle n + 1 \rangle + 125/243 + 125/244$ in 2.215s. Our bound is more precise than the bound obtained in [Wang et al. 2019] and the execution time of `eco-imp` is 35-times faster.

function ecost[C]
  switch C **do**
    case D;E **where** D contains a loop:
      $\boldsymbol{\kappa}(\vec{b}) \leftarrow$ ecost[E]
      $\vec{b'} \leftarrow$ **foreach** $b \in \vec{b}$**:** evalue[D](b)
      return ecost[D] $+ \boldsymbol{\kappa}(\vec{b'})$
    case while (ϕ) {D}:
      $g \leftarrow$ ecost[D]
      $\vec{b} \leftarrow$ SelectBases(ϕ, g)
      $\vec{b'} \leftarrow$ **foreach** $b \in \vec{b}$**:** evalue[D](b)
      $\kappa \leftarrow$ LinearTemplate(length$(\vec{b})$)
      $\theta \leftarrow$ Solve$(\phi \vDash g + \boldsymbol{\kappa}(\vec{b'}) \trianglelefteq \boldsymbol{\kappa}(\vec{b}))$
      return $\theta(\boldsymbol{\kappa})(\vec{b})$
    default: return SymbolicCost(C)

function evalue[C](f)
  switch C **do**
    case D;E **where** D contains a loop:
      $\boldsymbol{\kappa}(\vec{b}) \leftarrow$ evalue[E]
      $\vec{b'} \leftarrow$ **foreach** $b \in \vec{b}$**:** evalue[D](b)
      return $\boldsymbol{\kappa}(\vec{b'})$
    case while (ϕ) {D}:
      $\vec{b} \leftarrow$ SelectBases(ϕ, f)
      $\vec{b'} \leftarrow$ **foreach** $b \in \vec{b}$**:** evalue[D](b)
      $\kappa \leftarrow$ LinearTemplate(length$(\vec{b})$)
      $\theta \leftarrow$ Solve$(\phi \vDash \boldsymbol{\kappa}(\vec{b'}) \trianglelefteq \boldsymbol{\kappa}(\vec{b}) \wedge \neg\phi \vDash f \trianglelefteq \boldsymbol{\kappa}(\vec{b}))$
      return $\theta(\boldsymbol{\kappa})(\vec{b})$
    case $x \coloneqq d$**: return** Expectation$(d, \lambda v.f[x/v])$
    default: return SymbolicValue(C, f)

Fig. 4. Pseudocode detailing cost-inference.

7 IMPLEMENTATION

In this section, we give an overview of the implementation of our methodology within our tool `eco-imp`. The core of our tool is given by the algorithms ecost[C] and evalue[C] outlined in Figure 4, computing for a given program C and cost function f, an upper bound to ecost[C] and evalue[C](f), respectively. As for the transformers, the two algorithms are structurally similar. In the majority of cases, the default branch of the algorithm is executed and the implementation symbolically executes the corresponding transformer from Figure 3. Conclusively, a precise bounds is computed in these cases. Exceptions to this are the cases of loops and assignments, detailed below. Here, possibly imprecise upper bounds are derived. Due to monotonicity (Lemma 3.4(2)) soundness of the overall algorithm remains intact.

Sequential composition. For a command C = D;E, our implementation relies on Theorem 6.4, except when D does not contain a loop. In this case, the algorithms proceed by unfolding according to the rules in Figure 4 and (recursion on D). Here, modularity is not necessary; the straight-line program D can be analysed directly.

While loops. The main novel aspect from which our implementation derives its strength lies in the treatments of loops, providing an almost literal implementation of Theorem 6.4, following to recipe given on page 14. The subprocedure SelectBases, outlined below, selects a vector of base functions $\vec{b}$ from the loops guard ϕ, and the recursively computed cost g of the loop's body or the cost function f. For each such base function b, an upper bound b' to its expectation evalue[C](b) is computed and a linear template $\kappa(\vec{x}) = \sum_i q_i \cdot x_i$ with undetermined coefficients $q_i \in \mathbb{R}_{\geq 0}$ is prepared. Based on these ingredients, the subprocedure Solve is applied to the constraint dictated by Theorem 6.4. Should this procedure establish a solution θ, ie. an assignment to the undetermined coefficients q_i underlying κ that validates the supplied constraint, the instantiated cost function $\theta(\boldsymbol{\kappa})(\vec{b}) = \sum_i \theta(q_i) \cdot \vec{b_i}$ is returned. The dedicated constraint solver underlying the procedure Solve is detailed below in Section 7.1.

Selection of base functions. Our implementation selects a set of candidate base functions $\vec{b}$ as a *linear* or *non-linear* combination of base functions $\vec{b}_\phi$, $\vec{b}_g$ and $\vec{b}_f$ extracted from the loop guard ϕ, the expected cost of the loop body g and the continuation f, loosely following the heuristics of Sinn et al. [2016]. Specifically, for a loop guard containing $e_1 \trianglelefteq e_2$ we take $\langle e_2 - e_1 + \mathbf{1} \rangle \in \vec{b}_\phi$.

Since base functions can be extracted from a given context rather than the whole program, the number of base functions is usually low. This is one crucial aspect to the efficiency of our algorithm. The prototype implements caching and backtracking to test different base functions. In particular, non-linear base functions are employed only if the linear ones fail. This is another crucial aspect to efficiency, in contrast to a monolithic procedure. Constraint solving over linear arithmetical expressions is significantly more efficient; non-linear expressions are employed only in the analysis of those program fragments where necessary.

Assignments. Our implementation supports, on the one hand, assignments with sampling from *finite*, *discrete* distributions, of the form $d(\sigma) = \{\!\{ p_i(\sigma) : e_i(\sigma) \}\!\}_{0 \le i \le k}$ for a fixed constant k and $p_i = e_i/f_i$, such as $\{\!\{ {}^{i+1}/_{10} : x + 2i \}\!\}_{0 \le i \le 9}$. Noteworthy, probabilities of probabilistic branches are not necessarily constant. The expected cost of a probabilistic assignment $x \coloneqq d$ is given by

$$\mathrm{ect}[x \coloneqq d](f)(\sigma) = \textstyle\sum_{1 \le i \le k} p_i(\sigma) \cdot f[x/e_i(\sigma)] \ .$$

Thus our system encompasses a variety of standard distributions where probabilistic branching is *static*, in the sense that the degree does not depend on program variables. Our implementation supports this way a variety of standard distributions, noteworthy sampling from *uniform distributions with bounded support*, *Bernoulli*, *binomial* and *hypergeometric* distributions. A distinct feature of our overall methodology is that we are able to natively support *dynamic probabilistic branching*, facilitated by our constraint solver for Upper Invariants. In particular, we have added support for sampling uniform distributions $\mathtt{Uniform}(e_1, e_2)$ for $e_1 \le e_2$. This, for example, is crucial to represent the Coupon Collector's problem properly. Note, that in this case

$$\mathrm{ect}[x \coloneqq d](f) = [e_1 \le e_2] \cdot \big(\textstyle\sum_{i=e_1}^{e_2} f[x/i]\big)/(e_2 - e_1 + 1) \ .$$

To find a closed form for the bounded sum $\sum_{i=e_1}^{e_2} f[x/i]$, our implementation seeks for an upper bound $\boldsymbol{\kappa}(\vec{b})$ subject to the constraint $e_1 \le \boldsymbol{i} \wedge \boldsymbol{i} \le e_2 \vDash f[x/i] + \boldsymbol{\kappa}(\vec{b}[i/i+1]) \le \boldsymbol{\kappa}(\vec{b})$.

7.1 Constraint Solving Mechanism

In this section, we highlight the constraint solving mechanism as implemented in our prototype `eco-imp`, consisting of two stages: the first translates constraints over costs (with undetermined coefficients) to tests of non-negativity over polynomials; the second stage then treats this syntactically simpler form of constraints.

First, we fix two syntactic categories of (non-linear) integer expressions Exp and *cost expressions* CExp as follows.

$$\mathsf{Exp} \ni e, f ::= \boldsymbol{i} \mid x \mid e + f \mid e - f \mid e \cdot f \quad \mathsf{CExp} \ni c, d ::= e/f \mid [\phi] \cdot c \mid c + d \mid \mathbf{max}(c, d) \ .$$

In Exp, we use integer variables $x \in \mathsf{Var}$ to denote cost functions $\lambda\sigma.\sigma(x)$. Cost expressions denote fractions over integer expressions, closed under guards, sum and maximum. Furthermore, we restrict BExp to Boolean formulas over atoms $e \ge f$, in disjunctive normal form. This still permits the usual comparison operators over integer expressions, e.g., $e > f$ can be represented as $e \ge f + 1$ or $e = f$ as $e \ge f \wedge f \ge e$. We tacitly employ such equalities below. When denoting cost expressions, we usually write e instead of $e/1$. Base functions are given as a combination of expressions $\langle e \rangle \triangleq [0 \le e] \cdot e$. Not every cost expression is an expectation in $\mathbb{C}^{\Sigma}$ though, as cost expression need not be well-formed.

We say $c \in \mathsf{CExp}$ is *well-formed* wrt. store $\sigma \in \Sigma$ if (i) $c = e/f$ such that $e(\sigma) \ge 0$ and $f(\sigma) > 0$; (ii) $c = [\phi] \cdot d$ such that $\sigma \vDash \phi$ and d is well-formed wrt. σ; (iii) $c = c_1 + c_2$ or $c = \mathbf{max}(c_1, c_2)$ such that both c_1 and c_2 are well-formed wrt. σ. Well-formedness of c under σ guarantees that $c(\sigma)$ is defined and non-negative. We call c well-formed wrt. a Boolean expression ϕ, if c is well-formed

Simplification Rules

$$\frac{\phi \wedge \psi \vDash c_1 + c_2 \preceq d \quad \phi \wedge \neg\psi \vDash c_2 \preceq d}{\phi \vDash [\psi] \cdot c_1 + c_2 \preceq d}\,[\textsc{condL}] \qquad \frac{\phi \wedge \psi \vDash c \preceq d_1 + d_2 \quad \phi \wedge \neg\psi \vDash c \preceq d_2}{\phi \vDash c \preceq [\psi] \cdot d_1 + d_2}\,[\textsc{condR}]$$

$$\frac{\phi \vDash e + c \star f \preceq d \star f}{\phi \vDash e/f + c \preceq d}\,[\textsc{divL}] \qquad \frac{\phi \vDash c \star f \preceq e + d \star f}{\phi \vDash c \preceq e/f + d}\,[\textsc{divR}] \qquad \frac{\phi \vDash c_1 + c_3 \preceq d \quad \phi \vDash c_2 + c_3 \preceq d}{\phi \vDash \mathbf{max}(c_1, c_2) + c_3 \preceq d}\,[\textsc{maxL}]$$

Logical Rules

$$\frac{}{\phi \vDash 0 \preceq d}\,[\textsc{triv}] \qquad \frac{\phi \vDash \bot}{\phi \vDash c \preceq d}\,[\textsc{contr}] \qquad \frac{\forall i.(\phi_i \vDash c \preceq d)}{(\bigvee_i \phi_i) \vDash c \preceq d}\,[\textsc{conj}]$$

Fig. 5. Constraint simplification rules.

for all stores σ such that $\sigma \vDash \phi$. Apart from the lack of fixed points, the syntax of cost expression is rich enough to express our expectation transformers. Division is included to express the build in distributions outlined above. Cost expressions form a commutative semigroup under $\mathbf{+}$, with $\mathbf{0}$ the unit element. Thus, it is justified to consider cost expressions equal up to associativity and commutativity of $\mathbf{+}$, as well as the unit law $\mathbf{0} + c = c + \mathbf{0} = c$.

For $c \in \mathsf{CExp}$ and $e \in \mathsf{CExp}$, we define *multiplication* $c \star (e_1/e_2)$ with a fraction $q = e_1/e_2$ by recursion on c in the natural way as follows:

$$(f_1/f_2) \star (e_1/e_2) \triangleq (f_1 \cdot e_1)/(f_2 \cdot e_2) \qquad ([\phi] \cdot c) \star q \triangleq [\phi] \cdot (c \star q)$$
$$(c_1 + c_2) \star q \triangleq c_1 \star q + c_2 \star q \qquad \mathbf{max}(c_1, c_2) \star q \triangleq \mathbf{max}(c_1 \star q, c_2 \star q)\ .$$

Note that this operation preserves well-formedness. Due to the last clause, $c \star (e_1/e_2)$ does in general not equal $c \cdot (e_1/e_2)$, namely, on stores σ where the fraction is negative. However, for well-formed cost expression e_1/e_2, the equality holds.

Constraint simplification. In Figure 5, we present an inference system over *constraints* $\phi \vDash c \preceq d$, where $c, f \in \mathsf{CExp}$ and $\phi, \psi \in \mathsf{BExp}$. This system eliminates max, guards and disjunctions by case analysis. We elide a rule for $\mathbf{max}$ occurring in right-hand sides, as this can be easily prevented in the constraint solving setup. We say a constraint $\phi \vDash c \preceq d$ is *well-formed*, if c, d are well-formed under ϕ. It is *valid* if for all stores $\sigma \in \Sigma$ with $\sigma \vDash \phi$, we have $c(\sigma) \leq d(\sigma)$. It is easy to see that the rules preserve well-formedness. The system is sound and complete in the following sense.

Theorem 7.1. *Let Δ be a derivation of a well-formed constraint $\phi \vDash c \preceq d$. Then this constraint is valid if and only if all premises in Δ are.*

This statement is proven by induction on the derivation Δ. The rules concerning division, rule (divL) and (divR), are sound because the divisor f is positive on all stores σ satisfying ϕ, due to the well-formedness assumption.

Example 7.2. Recall that the analysis of program $\mathsf{C}_{\mathsf{geo}}$ in Section 6.1 required solving the constraint $b = 1 \vDash \mathbf{1} + \boldsymbol{\kappa}(\mathbf{1/2}) \preceq \boldsymbol{\kappa}(\langle b \rangle)$. Fix $\kappa(x) \triangleq q \cdot x$ for undetermined $q \in \mathbb{R}_{\geq 0}$ and note that $\langle b \rangle = [\mathbf{0} \preceq b] \cdot b$. By unfolding κ, the cost of the loop in $\mathsf{C}_{\mathsf{geo}}$ is given by $\boldsymbol{\kappa}(\langle b \rangle)$ if $b = \mathbf{1} \vDash \mathbf{1} + \boldsymbol{q/2} \preceq [\mathbf{0} \preceq b] \cdot \boldsymbol{q} \cdot b$, is valid for some $q \in \mathbb{R}_{\geq 0}$. Eliminating guards yield several constraints, but only the constraint $b = \mathbf{1} \wedge \mathbf{0} \preceq b \vDash \mathbf{1} + \boldsymbol{q/2} \preceq \boldsymbol{q} \cdot b$, is not subject to rule (triv) or rule (contr). Rule (divL) then yields $b = \mathbf{1} \wedge \mathbf{0} \preceq b \vDash \mathbf{2} + \boldsymbol{q} \preceq \mathbf{2} \cdot \boldsymbol{q} \cdot b$. By Theorem 7.1, this constraint is equi-satisfiable with the initial one above, in the sense that any value for q for the latter makes also the former valid.

Constraint solving. Given a constraint $\phi \vDash c \preceq d$, the simplification rules of Figure 5 can be seen as a way to eliminate max, guards, division and disjunctions. Thus, they translate constraints over cost-expressions to a set of equivalent constraints over integer-valued expressions. Wlog., these

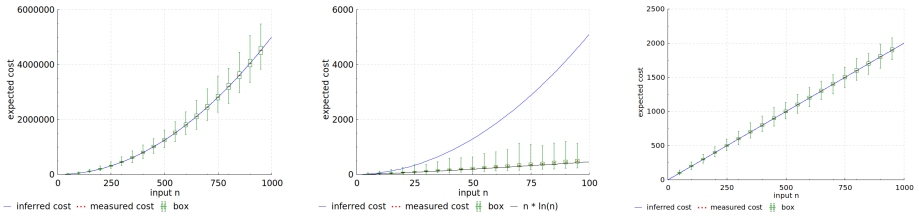

Fig. 6. Comparison of inferred expected cost and measured expected cost using a sample size of 10000, for (from left to right) examples (a) `trader` 2, (b) coupons and (c) `rejection_sampling`. The box plot depicts the minimum, lower- and upper quartile, and maximum cost measured. For `trader` we fix *min* to 100.

constraints are of the form

$$\bigwedge_i e_i \geq \mathbf{0} \vDash e \geq \mathbf{0} \,,$$

by employing additionally the identity $f \geq g \Leftrightarrow f - g \geq \mathbf{0}$. Any expression e can be understood as a polynomial $p(\vec{x})$ in the program variables $\vec{x}$. Validity of constraints of the above form becomes representable as a test of non-negativity. To this end, we make use of known approximations for certifying non-negativity of polynomial expressions, cf. [Chatterjee et al. 2016; Fuhs et al. 2007; Wang et al. 2019].

Proposition 7.3. *Let $I = (i_1, \ldots, i_m) \in \mathbb{N}^m$ denote a multi-index such that $p, p_{1 \leqslant i \leqslant m} \colon \mathbb{Z}^n \to \mathbb{R}$. Further, let $p_I(\vec{x}) = p_1^{i_1}(\vec{x}) \cdots p_m^{i_m}(\vec{x})$. If $p(\vec{x}) = \sum_{I \in \mathbb{N}^m} c_I \cdot p_I(\vec{x})$ for some $c_I \in \mathbb{R}_{\geq 0}$, then $\bigwedge_{i=1}^m p_i(\vec{x}) \geq 0$ implies $p(\vec{x}) \geq 0$.*

Incidentally, Proposition 7.3 expresses a (gross) simplification of Handelman's theorem [Handelman 1988], which turns out to be quite effective in our context. Recall that overall, we are concerned with synthesising concrete values for the undetermined $q_i \in \mathbb{R}_{\geq 0}$ stemming from templates $\kappa(\vec{b}) \triangleq \sum q_i \cdot b_i$, so that all the generated constraints become valid. By reducing inequalities over polynomials to inequalities of the constituting coefficients and fixing indices I, via Proposition 7.3 this synthesis can be formulated as a satisfiability problem over arithmetical expressions over variables $q_i \geq 0$. In turn, this problem can be solved with an off-the-shelf SMT-solver supporting `QF_NRA`. We illustrate this with our running example.

Example 7.4 (Example 7.2 continued). The final remaining constraint from the running example simplifies to

$$b - 1 \geq 0 \wedge 1 - b \geq 0 \wedge b \geq 0 \implies 2 \cdot q \cdot b - q - 2 \geq 0 \,.$$

We restrict to the multi-indices $(1,0,0)$, $(0,1,0)$ and $(0,0,1)$, that is, we intend to express $2 \cdot q \cdot b - q - 2$ as a linear combination of the three functions $b - 1$, $1 - b$ and b, representing the conjuncts in the assumption. Proposition 7.3 yields the following obligation

$$2 \cdot q \cdot b - q - 2 = c_{(1,0,0)} \cdot (b - 1) + c_{(0,1,0)} \cdot (1 - b) + c_{(0,0,1)} \cdot b \,,$$

which, subject to the side-condition $q \geq 0$, holds with $q = 2$, $c_{(1,0,0)} = 4$ and $c_{(0,1,0)} = c_{(0,0,1)} = 0$. Theorem 7.1 now translates this solution to a solution $\kappa(x) \triangleq 2 \cdot x$ for the initial constraint in Example 7.2. The constraint solving mechanism established this way thus derives the (optimal) bound given by hand in Section 6.1.

7.2 Experimental Evaluation

To assess our implementation, we have conducted an experimental evaluation of `eco-imp` on the benchmarks of [Ngo et al. 2018; Wang et al. 2019]. We have elided example `recursive` from [Ngo

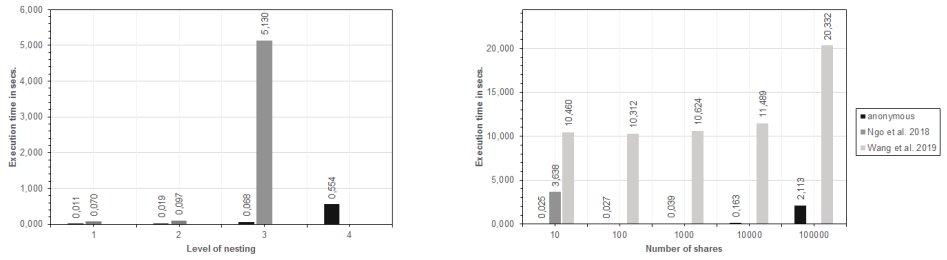

Fig. 7. Execution times of the three analysers on parametric examples (a) `nest-i` consisting of i nested loops, each performing a biased random walk and (b) `trader-n` from Figure 1a with number of shares fixed to n.

et al. 2018] as we have not yet incorporated support for recursive definitions into `eco-imp`. This is planned for a future release of the prototype. The prototype of Wang et al. [2019] can also deal with some programs featuring negative costs, corresponding examples have been also removed from our testbed. We have extended the resulting testbed with the various examples from this work: In Table 2 we list the program C_{coupons} from Figure 1c as `coupons-n` and also instantiate n to constants 10, 50 and 100. Similar, the trader example C_{trader} from Figure 1a has been parameterised in the number of shares, denoted as `trader-n`, respectively. Examples `nest-i` perform i nested random walks. The example `bridge` performs an unbiased random walk within an interval $[a, b]$.

In Tables 1 and 2, we compare our implementation (column **A**) to the prototypes of Ngo et al. [2018] (column **B**) and Wang et al. [2019] (column **C**). On some of the examples, the tool `Absynth` does not provide an upper bound in a reasonable amount of time; as timeout we have use 5 minutes; corresponding examples have been marked with —. Wrt. to tool by Wang et al. [2019], we were able to slightly extend the results given in their work. However, the tool requires extensive manual invariant annotations. Conclusively, various examples were not amendable to an experimental evaluation and corresponding rows have been left blank. Execution times are obtained on an Intel i7-7600U CPU with 2.8GHz and 16GB RAM.

Precision. The upper bounds reported in Table 1 and 2 are to a great extent overlapping with those inferred by the `Absynth` tool from Ngo et al. [2018] and, where available, inferred by the prototype of Wang et al. [2019]. In particular, the bounds for all but one example are on the same order of magnitude. In example `prnes`, `eco-imp` infers a quadratic rather than a linear bound. Vice versa, for example `C4B_t30` our tool infers an asymptotic optimal linear bound, whereas `Absynth` yields a quadratic one. These results are remarkable, as the precision of `Absynth` is outstanding. It is well-understood that a modular analysis, like ours, often comes with the drawback of less precision. Noteworthy is our analysis of `rejection_sampling` due to Kaminski et al. [2016], where `eco-imp`'s precision equals the measured expected cost, cf. Figure 6.

Speed. Across the benchmark, `eco-imp` outperforms the other tools. The only exception to this assessment are the examples `queueing-network` and `prnes`. While our tool achieves already significant speedups in the linear benchmark from [Ngo et al. 2018] (annotated in parenthesis besides execution times), the gains are most pronounced in examples with nested loops and non-linear bounds. This assessment remains intact when comparing to the implementation of Wang et al. on the subset of examples treated by Wang et al. [2019].

Scalability. In Figure 7, we show the results of `eco-imp` on parametric examples in comparison to the prototypes of Ngo et al. [2018] and Wang et al. [2019]. The left figure plots execution times in relation to the number of nested loops, comparing `eco-imp` and the tool `Absynth`. Similarly, the

figure on the right depicts the effects on extending the number of shares in C_{trader}, comparing all tools. Our results are competitive and highlight sharply the prime benefit of our implementation, viz, its modularity.

8 RELATED WORKS

We restrict our focus on related work concerned with the analysis of *bounded expected resource usage* of (non-deterministic) probabilistic imperative programs.

Very briefly, we refer to the extensive literature of analysis methods for (*bounded*) or *almost-sure termination* for (non-deterministic) probabilistic programs that have been introduced in the last years. These have been provided in the form of *abstract interpretations* [Chakarov and Sankaranarayanan 2014; Monniaux 2001]; *martingales*, eg., ranking super-martingales [Agrawal et al. 2018; Brázdil et al. 2015; Chakarov and Sankaranarayanan 2013; Chatterjee et al. 2016, 2017a,b; Esparza et al. 2005; Takisaka et al. 2018; Wang et al. 2019]; or equivalently *Lyapunov ranking functions* [Bournez and Garnier 2005]; *model checking* [Katoen 2016]; *program logics* [Kaminski et al. 2018; McIver et al. 2018; Ngo et al. 2018; Wang et al. 2018]; *proof assistants* [Barthe et al. 2009]; *recurrence relations* [Sedgewick and Flajolet 1996]; methods based on *program analysis* [Celiku and McIver 2005; Katoen et al. 2010; Kozen 1985]; or *symbolic inference* [Gehr et al. 2016]; and finally *type systems* [Avanzini et al. 2019a; Breuvart and Dal Lago 2018].

Probabilistic resource analysis. Kaminski et al. generalises Dijkstra's wp-calculus to an expected runtime transformer ert. The obtained resource analysis expresses is smoothly applicable in a variety of case studies, in particular to the program C_{coupons}. Our expected cost transformer constitutes a generalisation of the ert-calculus. In particular, note that evalue[C] coincides with the weakest precondition transformer wp[C] by Kaminski et al. [2018] on *fully probabilistic programs*, ie. those without non-deterministic choice. In the presence of mixed-sign, unbounded updates, the ert-calculus has been extended by exploiting an absolute convergence criterion, cf. Kaminski and Katoen [2017]. A bulk of research in the literature concentrates on specific forms of martingales or Lyapunov ranking functions. Central to our work is the observation, that these approaches can be suited to a variety of quantitative program properties, see Takisaka et al. [2018] for an overview. We also mention Chatterjee et al. [2017a] where inference procedures to solve recurrences stemming from probabilistic programs are proposed.

Automation. Notably, the `Absynth` prototype by Ngo et al. [2018], implements a weakest precondition calculus for reasoning about expected costs. Our tool `eco-imp` generalises this implementation and provides a modular and thus a more efficient and scalable alternative. Also martingale based techniques have been implemented, eg., by Chatterjee et al. [2016] and more recently by Wang et al. [2019]. A novelty of Wang et al. [2019] is the established polynomial-time analysis and incorporation of a cost model which allows for unbounded *negative* and *positive* costs, as long as the variable updated are bounded, while demands (almost-sure) termination as prerequisite. Exploiting the approach by Kaminski and Katoen [2017], we expect the extensibility of our approach to negative costs as well. Our work overcomes the whole-program analysis established by these tools and provides a modular and scalable framework. Further, dynamic distributions are supported. As vindicated by the above provided experimental assessment, modularity significantly speeds up the analysis (see Section 7).

9 CONCLUSION

We established an automated expected resource analysis of non-deterministic, probabilistic imperative programs. As indicated by the formal hardness of this problem by Kaminski and Katoen [2015], this is challenging. While previous approaches only feature a whole-program analysis to synthesis

precise cost functions, we present a novel modular framework for the automated analysis. Our prototype `eco-imp` is more efficient and scales better than existing tools. Its algorithmic prowess is eg. attested by the fact that the motivating example by Ngo et al. [2018] can be handled *three orders of magnitudes* faster. To establish these highlights, (i) we exploit a novel operational semantics in terms of *weighted probabilistic abstract reduction systems* Avanzini et al. [2019b]; Avanzini and Yamada [2020]; (ii) we establish modularity by generalising a weakest precondition calculus pioneered by Kaminski et al. [2018] to an *alternating expected cost and value analysis*; and (iii) painstaking attention to detail in the implementation with a focus on efficiency.

Future theoretical advances are needed to incorporate the treatment of presence of mixed-sign, unbounded updates, in order to properly deal with negative costs. Practical goals are the extension of the synthesis capabilities of our prototype towards *lower bounds* (following Ngo et al. [2017]) and further real-world examples.

Table 1. Automatically derived bounds on the expected cost via eco-imp (columns **A**), the Absynth prototype from [Ngo et al. 2018] (columns **B**) and the prototype of [Wang et al. 2019] (columns **C**). Integer factor annotated besides execution time give the relative speedup of our implementation.

	Inferred Bound			Execution times in secs. (factor)		
Program	**A**	**B**	**C**	**A**	**B**	**C**
linear benchmark from [Ngo et al. 2018]						
2drwalk	$2\langle n-d+1\rangle$	$2\langle n-d+1\rangle$		0.026s	0.286s (11)	
bayesian_network	$5\langle n\rangle$	$5\langle n\rangle$	$0.91n-0.91x-0.91$	0.002s	0.127s (63)	6.303s (3151)
ber	$2\langle n-x\rangle$	$2\langle n-x\rangle$	$n-x$	0.001s	0.014s (14)	6.685s (6685)
bin	$^{1.024}/_{1.023}\langle n-x\rangle$	$0.2\langle 9+n\rangle$		0.006s	0.152s (25)	
C4B_t09	$41\langle x\rangle$	$8.27\langle x\rangle$		0.006s	0.079s (13)	
C4B_t13	$^{5}/_{4}\langle x\rangle+\langle y\rangle$	$1.25\langle x\rangle+\langle y\rangle$	$1.25x+y-1.25$	0.005s	0.025s (5)	8.527s (1705)
C4B_t15	$2\langle x+1\rangle$	$\langle x-1\rangle+\langle x\rangle$		0.006s	0.026s (4)	
C4B_t19	$2\langle i-100\rangle+\langle i+k+51\rangle$	$2\langle i\rangle+\langle i+k+51\rangle$		0.005s	0.022s (4)	
C4B_t30	$\langle y+2\rangle+\langle x\rangle$	$0.33\langle x+2\rangle+0.167\langle 2+x\rangle\langle 2+y\rangle$		0.003s	0.240s (80)	
C4B_t61	$7+^{160}/_{19}\langle l-7\rangle$	$0.06\langle l-1\rangle+\langle l\rangle$		0.005s	0.036s (7)	
condand	$2\langle m\rangle$	$2\langle m\rangle$	$m+n-1$	0.002s	0.019s (9)	8.037s (4018)
cooling	$^{21}/_{10}\langle 1+t\rangle+\langle mt-st\rangle$	$0.42\langle 5+t\rangle+\langle mt-st\rangle$		0.015s	0.083s (6)	
coupon	25	15		0.003s	0.045s (15)	
cowboy_duel	$^{6}/_{5}$	1.2		0.001s	0.033s (33)	
cowboy_duel_3way	$^{83}/_{24}$	2.083		0.004s	0.149s (37)	
fcall	$2\langle n-x\rangle$	$2\langle n-x\rangle$		0.001s	0.021s (21)	
filling_vol	$^{3}/_{5}\langle 1+vTF\rangle+^{3}/_{5}\langle vTF\rangle$	$0.33\langle 10+vTF\rangle+0.33\langle vTF\rangle$		0.006s	0.230s (38)	
geo	1	5		0.001s	0.018s (18)	
hyper	$^{145}/_{28}\langle n-x-1\rangle$	$5\langle n-x\rangle$		0.002s	0.034s (17)	
linear01	$\langle x-1\rangle$	$0.6\langle x\rangle$	$0.6x$	0.001s	0.011s (11)	6.392s (6392)
no_loop	5	5		0.001s	0.010s (10)	
prdwalk	$^{8}/_{3}\langle n-x\rangle$	$1.14\langle 4+n-x\rangle$	$1.16n-1.18x-1.16$	0.002s	0.027s (13)	6.650s (3325)
prnes	$^{50}/_{9}\langle y-99\rangle\langle -n\rangle+^{250.000}/_{81}\langle -n\rangle^2$	$68.48\langle -n\rangle+0.05\langle y\rangle$	$0.05y-68.48n$	0.126s	0.034s (0)	7.789s (62)
prseq	$6\langle x-y-2\rangle+3\langle y-9\rangle$	$1.65\langle x-y\rangle+0.15\langle y\rangle$		0.010s	0.030s (3)	
prseq_bin	$^{32}/_{5}\langle x-y-2\rangle+3\langle y-9\rangle$	$1.65\langle 1+x-y\rangle+0.15\langle y\rangle$		0.016s	0.038s (2)	
prspeed	$^{4}/_{3}\langle n-x-2\rangle+2\langle m-y\rangle$	$0.067\langle n-x\rangle+2\langle m-y\rangle$		0.013s	0.033s (3)	
race	$^{11}/_{6}\langle t-h+3\rangle$	$0.67\langle t-h+9\rangle$	$0.571t-0.571h$	0.010s	0.048s (5)	6.936s (694)
rdseql	$^{9}/_{4}\langle x\rangle+\langle y\rangle$	$2.25\langle x\rangle+\langle y\rangle$	$2.25x+y$	0.007s	0.032s (5)	7.396s (1057)
rdspeed	$^{4}/_{3}\langle n-x-2\rangle+2\langle m-y\rangle$	$0.67\langle n-x\rangle+2\langle m-y\rangle$		0.012s	0.096s (8)	
rdwalk	$2\langle n-x+1\rangle$	$2\langle n-x+1\rangle$	$2n-2x-2$	0.003s	0.058s (19)	6.497s (2166)
rejection_sampling	$2\langle n\rangle$	$2\langle n\rangle$		0.002s	1.221s (610)	
rfind_lv	2	2		0.001s	0.015s (15)	
rfind_mc	$\langle k\rangle$	$\langle k\rangle$		0.002s	0.019s (9)	
robot	$^{5}/_{4}\langle n\rangle$	$0.38\langle 6+n\rangle$		0.006s	1.546s (258)	
roulette	$^{74}/_{15}\langle 10.011-n\rangle$	$4.933\langle 10.010-n\rangle$		0.049s	0.139s (3)	

Table 2. Automatically derived bounds on the expected cost via `eco-imp` (columns **A**), the `Absynth` prototype from [Ngo et al. 2018] (columns **B**) and the prototype of [Wang et al. 2019] (columns **C**). Integer factor annotated besides execution time give the relative speedup of our implementation.

Program	Inferred Bound A	Inferred Bound B	Inferred Bound C	Execution times in secs. (factor) A	Execution times in secs. (factor) B	Execution times in secs. (factor) C
linear benchmark from [Ngo et al. 2018] (continued)						
`simple_game`	$2\langle x+1\rangle$	$2\langle x+1\rangle$		0.006s	0.045s (7)	
`sprdwalk`	$2\langle n-x\rangle$	$2\langle n-x\rangle$	$2n-2x$	0.001s	0.019s (19)	6.155s (6155)
`trapped_miner`	$^{15}/_{2}\langle n\rangle$	$7.5\langle n\rangle$		0.002s	0.052s (26)	
Non-linear benchmark from [Ngo et al. 2018]						
`complex`	$\langle w\rangle + 18\langle M\cdot N+N\rangle\langle N\rangle + 3\langle y\rangle$	$\langle w\rangle + 18\langle M\rangle\langle N\rangle + 9\langle N\rangle + 3\langle y\rangle$		0.029s	0.809s (28)	
`multirace`	$\langle m+1\rangle\langle n\rangle$	$2\langle m\rangle\langle n\rangle + 4\langle n\rangle$		0.013s	2.190s (168)	
`pol04`	$^{15}/_{2}\langle x\rangle + {}^{9}/_{2}\langle x\rangle^2$	$7.5\langle x\rangle + 4.5\langle x\rangle^2$	$3.125x^2 + 5.31x$	0.007s	0.261s (37)	8.626s (1232)
`pol05`	$^{3}/_{4}\langle x\rangle + {}^{3}/_{2}\langle x\rangle^2$	$\langle x\rangle + \langle x\rangle^2$	$0.5x^2 + 2.5x$	0.007s	0.150s (21)	8.480s (1211)
`pol06`	$\langle 1+m\rangle\langle 1+p\rangle + \langle p-m\rangle\langle 1+p\rangle$	$0.5\langle p-m\rangle + \langle p-m\rangle\langle p\rangle + \langle p-m\rangle^2$		0.040s	1.567s (39)	
`pol07`	$^{3}/_{2}\langle n-1\rangle^2$	$1.5\langle n-1\rangle\langle n-2\rangle$		0.015s	0.561s (37)	
`rdbub`	$3\langle n\rangle^2$	$3\langle n\rangle^2$	n^2+n	0.006s	0.092s (15)	9.374s (1562)
`trader(-20)`	$20\langle 1+m\rangle\langle p-m\rangle + 10\langle p-m\rangle^2$	$20\langle m\rangle\langle p-m\rangle + 10\langle p-m\rangle + 10\langle p-m\rangle^2$	$10(p^2-m^2) - 20p + 40m + 10$	0.030s	119.464s (3982)	10.420s (347)
additional examples from [Wang et al. 2019]						
`2drobot`	$^{1}/_{2}\langle 1+a-b\rangle\langle a-b\rangle + 2\langle 1+a-b\rangle^2 + {}^{1267}/_{18}\langle 6+a-b\rangle$	–	$1.73a^2 - 3.46ab + 31.45a + 1.73b^2 - 31.45a + 126.52$	1.760s		11.621s (7)
`queueing-network`	$^{1.132.981}/_{7.411.500}\langle n+1\rangle + {}^{125}/_{243} + {}^{125}/_{244}$	$0.05\langle n+1\rangle + 0.014\langle n+1\rangle^2$	$0.01l_1^2 + 0.003l_2^3 + 0.007l_2^2 - 0.049(n+i+1)$	2.215s	1.286s (1)	78.191s (35)
examples from this work						
`bridge`	$\langle x-a\rangle\langle b-x\rangle$	–	$ax+bx+a-x^2-b-ab+1$	0.005s		8.173s (1635)
`nest-1`	$4\langle n\rangle$	$2\langle n+1\rangle$		0.011s	0.070s (6)	
`nest-2`	$4\langle n\rangle + 16\langle n\rangle^2$	$2\langle 1+n\rangle + 4\langle 1+n\rangle^2$		0.019s	0.097s (5)	
`nest-3`	$2\langle 2+n\rangle + 16\langle n\rangle^2 + 64\langle n\rangle^3$	$2\langle 1+n\rangle + 4\langle 1+n\rangle^2 + 8\langle 1+n\rangle^3$		0.068s	5.130s (75)	
`nest-4`	$144\langle 2+n\rangle\langle n\rangle + 10\langle 2+n\rangle + 254n^4$	–		0.554s		
`trader-10`	$10\langle 1+m\rangle\langle p-m\rangle + 5\langle p-m\rangle^2$	$10(\langle m\rangle\langle p-m\rangle + \langle p-m\rangle^2) + 5\langle p-m\rangle$	$5(p^2-m^2+p+m-2)$	0.025s	3.638s (146)	10.460s (418)
`trader-100`	$100\langle 1+m\rangle\langle p-m\rangle + 50\langle p-m\rangle^2$	–	$50(p^2-m^2+4m-2p+1)$	0.027s		10.312s (382)
`trader-1000`	$1.000\langle 1+m\rangle\langle p-m\rangle + 500\langle p-m\rangle^2$	–	$500(p^2-m^2+4m-2p+1))$	0.039s		10.624s (272)
`trader-10000`	$10.000\langle 1+m\rangle\langle p-m\rangle + 5.000\langle p-m\rangle^2$	–	$5.000(p^2-m^2-2p+4m+1)$	0.163s		11.489s (70)
`trader-100000`	$100.000\langle 1+m\rangle\langle p-m\rangle + 50.000\langle p-m\rangle^2$	–	$50.000(p^2-m^2-2p+4m+1)$	2.113s		20.332s (10)
`coupons-10`	110	1550		0.015s	27.011s (1801)	
`coupons-50`	2250	–		0.304s		
`coupons-100`	10100	–		1.141s		
`coupons-n`	$\langle n\rangle + {}^{1}/_{2}\langle n\rangle^2$	not supported	not supported	0.195s		

REFERENCES

S. Agrawal, K. Chatterjee, and P. Novotný. 2018. Lexicographic Ranking Supermartingales: An Efficient Approach to Termination of Probabilistic Programs. *PACMPL* 2, POPL (2018), 34:1–34:32.

E. Albert, P. Gordillo, A. Rubio, and I. Sergey. 2019. Running on Fumes - Preventing Out-of-Gas Vulnerabilities in Ethereum Smart Contracts Using Static Resource Analysis. In *Proc. 13th International Conference of Verification and Evaluation of Computer and Communication Systems (LNCS)*, Vol. 11847. 63–78. https://doi.org/10.1007/978-3-030-35092-5_5

M. Avanzini, U. Dal Lago, and A. Ghyselen. 2019a. Type-Based Complexity Analysis of Probabilistic Functional Programs. In *Proc. of 34th LICS*. IEEE, 1–13.

M. Avanzini, U. Dal Lago, and A. Yamada. 2019b. On Probabilistic Term Rewriting. *SCP* 185 (2019), 102338.

Martin Avanzini, Ugo Dal Lago, and Akihisa Yamada. 2018. On Probabilistic Term Rewriting. In *Proc. of 14th FLOPS (LNCS)*, Vol. 10818. Springer, 132–148.

M. Avanzini, G. Moser, and M. Schaper. 2016. TcT: Tyrolean Complexity Tool. In *Proc. of the 22nd International Conference on Tools and Algorithms for the Construction and Analysis of Systems (LNCS)*, Vol. 9636. 407–423.

M. Avanzini and A. Yamada. 2020. *Weighted Rewriting*. Technical Report. NII and INRIA.

G. Barthe, B. Grégoire, and S. Z. Béguelin. 2009. Formal certification of code-based cryptographic proofs. In *Proc. of 36th POPL*. 90–101. https://doi.org/10.1145/1480881.1480894

A. Ben-Amram. 2011. Monotonicity Constraints for Termination in the Integer Domain. *LMCS* 7, 3 (2011).

A. Ben-Amram. 2015. Mortality of iterated piecewise affine functions over the integers: Decidability and complexity. *Computability* 4, 1 (2015), 19–56. https://doi.org/10.3233/COM-150032

A. Ben-Amram and G. Hamilton. 2019. Tight Worst-Case Bounds for Polynomial Loop Programs. In *Proc. of 22th FOSSACS*. 80–97. https://doi.org/10.1007/978-3-030-17127-8_5

A. M. Ben-Amram and L. Kristiansen. 2012. On the Edge of Decidability in Complexity Analysis of Loop Programs. *JFCS* 23, 7 (2012), 1451–1464.

O. Bournez and F. Garnier. 2005. Proving Positive Almost-Sure Termination. In *Proc. of 16th RTA (LNCS)*, Vol. 3467. Springer, 323–337.

T. Brázdil, S. Kiefer, A. Kucera, and I.H. Vareková. 2015. Runtime analysis of probabilistic programs with unbounded recursion. *J. Comput. Syst. Sci.* 81, 1 (2015), 288–310. https://doi.org/10.1016/j.jcss.2014.06.005

F. Breuvart and U. Dal Lago. 2018. On Intersection Types and Probabilistic Lambda Calculi. In *Proc. of 20th PPDP*. ACM, 8:1–8:13.

M. Brockschmidt, F. Emmes, S. Falke, C. Fuhs, and J. Giesl. 2016. Analyzing Runtime and Size Complexity of Integer Programs. *TOPLAS* 38, 4 (2016), 13:1–13:50.

O. Celiku and A. McIver. 2005. Compositional Specification and Analysis of Cost-Based Properties in Probabilistic Programs. In *Proc. International Symposium of Formal Methods Europe (LNCS)*, Vol. 3582. Springer, 107–122.

A. Chakarov and S. Sankaranarayanan. 2013. Probabilistic Program Analysis with Martingales. In *Proc. of 25th CAV (LNCS)*, Vol. 8044. Springer, 511–526.

A. Chakarov and S. Sankaranarayanan. 2014. Expectation Invariants for Probabilistic Program Loops as Fixed Points. In *Proc. of 21th SAS*. 85–100. https://doi.org/10.1007/978-3-319-10936-7_6

K. Chatterjee, H. Fu, and A. K. Goharshady. 2016. Termination Analysis of Probabilistic Programs Through Positivstellensatz's. In *Proc. of 28th CAV (LNCS)*, Vol. 9779. Springer, 3–22.

K. Chatterjee, H. Fu, and A. Murhekar. 2017a. Automated Recurrence Analysis for Almost-Linear Expected-Runtime Bounds. In *Proc. of 29th CAV (LNCS)*, Vol. 10426. Springer, 118–139.

K. Chatterjee, P. Novotný, and D. Zikelic. 2017b. Stochastic Invariants for Probabilistic Termination. In *Proc. of 44th POPL*. ACM, 145–160.

C. Choppy, S. Kaplan, and M. Soria. 1989. Complexity Analysis of Term-Rewriting Systems. *TCS* 67, 2–3 (1989), 261–282.

J. Cohen and C. Zuckerman. 1974. Two Languages for Estimating Program Efficiency. *Comm. ACM* 17, 6 (1974), 301–308. https://doi.org/10.1145/355616.361015

J. Esparza, A. Kucera, and R. Mayr. 2005. Quantitative Analysis of Probabilistic Pushdown Automata: Expectations and Variances. In *Proc. of 20th LICS*. 117–126. https://doi.org/10.1109/LICS.2005.39

Tomás Fiedor, Lukás Holík, Adam Rogalewicz, Moritz Sinn, Tomás Vojnar, and Florian Zuleger. 2018. From Shapes to Amortized Complexity. In *Proc. of the 19th International Conference on Verification, Model Checking, and Abstract Interpretation (LNCS)*, Vol. 10747. 205–225. https://doi.org/10.1007/978-3-319-73721-8_10

L. M. Ferrer Fioriti and H. Hermanns. 2015. Probabilistic Termination: Soundness, Completeness, and Compositionality. In *Proc. of 42nd POPL*. ACM, 489–501.

P. Flajolet. 1992. Analytic Analysis of Algorithms. In *Proc. of 19th ICALP*. 186–210. https://doi.org/10.1007/3-540-55719-9_74

P. Flajolet, B. Salvy, and P. Zimmermann. 1991. Automatic Average-Case Analysis of Algorithm. *TCS* 79, 1 (1991), 37–109. https://doi.org/10.1016/0304-3975(91)90145-R

Florian Frohn and Jürgen Giesl. 2017. Complexity Analysis for Java with AProVE. In *Proc. of the 13th International Conference on Integrated Formal Methods (LNCS)*, Vol. 10510. 85–101. https://doi.org/10.1007/978-3-319-66845-1_6

C. Fuhs, J. Giesl, A. Middeldorp, P. Schneider-Kamp, R. Thiemann, and H. Zankl. 2007. SAT Solving for Termination Analysis with Polynomial Interpretations. In *Proc. of 10th SAT (LNCS)*, Vol. 4501. Springer, 340–354.

T. Gehr, S. Misailovic, and M. Vechev. 2016. PSI: Exact Symbolic Inference for Probabilistic Programs. In *Proc. of 28th CAV*. 62–83. https://doi.org/10.1007/978-3-319-41528-4_4

S. Gulwani, K.K. Mehra, and T.M. Chilimbi. 2009. SPEED: Precise and Efficient Static Estimation of Program Computational Complexity. In *Proc. of 36th POPL*. ACM, 127–139.

S. Gulwani and F. Zuleger. 2010. The Reachability-Bound Problem. In *Proc. of PLDI'10*. ACM, 292–304.

D. Handelman. 1988. Representing Polynomials by Positive Linear Functions on Compact Convex Polyhedra. *PJM* 132, 1 (1988), 35–62.

N. Hirokawa and G. Moser. 2008. Automated Complexity Analysis Based on the Dependency Pair Method. In *Proc. of 4th IJCAR (LNAI)*, Vol. 5195. Springer, 364–380.

J. Hoffmann, A. Das, and S.-C. Weng. 2017. Towards Automatic Resource Bound Analysis for OCaml. In *Proc. of 44th POPL*. ACM, New York, NY, 359–373.

N. D. Jones and L. Kristiansen. 2009. A Flow Calculus of *mwp*-Bounds for Complexity Analysis. *TOCL* 10, 4 (2009).

B. L. Kaminski and J.-P. Katoen. 2017. A Weakest Pre-expectation Semantics for Mixed-sign Expectations. In *Proc. of 32nd LICS*. IEEE, 1–12.

B. Lucien Kaminski, J.-P. Katoen, C. Matheja, and F. Olmedo. 2016. Weakest Precondition Reasoning for Expected Run-Times of Probabilistic Programs. In *Proc. of 25th ESOP (LNCS)*, Vol. 9632. Springer, 364–389.

B. L. Kaminski, J.-P. Katoen, C. Matheja, and F. Olmedo. 2018. Weakest Precondition Reasoning for Expected Runtimes of Randomized Algorithms. *JACM* 65, 5 (2018), 30:1–30:68.

B. L. Kaminski and J.-P. Katoen. 2015. On the Hardness of Almost-Sure Termination. In *MFCS 2015, Part I*. 307–318.

J.-P. Katoen. 2016. The Probabilistic Model Checking Landscape. In *Proc. of 31nd LICS*. 31–45. https://doi.org/10.1145/2933575.2934574

J.-P. Katoen, A. McIver, L. Meinicke, and C.C. Morgan. 2010. Linear-Invariant Generation for Probabilistic Programs: - Automated Support for Proof-Based Methods. In *Proc. of 17th SAS*. 390–406. https://doi.org/10.1007/978-3-642-15769-1_24

C. Kim and A. K. Agrawala. 1989. Analysis of the fork-join queue. *IEEE Trans. Comput.* 38, 2 (1989), 250–255.

D. Kozen. 1981. Semantics of Probabilistic Programs. *J. Comput. Syst. Sci.* 22, 3 (1981), 328–350.

D. Kozen. 1985. A Probabilistic PDL. *JCSC* 30, 2 (1985), 162 – 178. https://doi.org/10.1016/0022-0000(85)90012-1

U. Dal Lago and C. Grellois. 2017. Probabilistic Termination by Monadic Affine Sized Typing. In *Proc. of 26th ESOP (LNCS)*. Springer, 393–419.

A. Levitin. 2007. *The Design and Analysis of Algorithms*. Pearson.

A. McIver, C. Morgan, B. L. Kaminski, and J-P Katoen. 2018. A New Proof Rule for Almost-sure Termination. *PACMPL* 2, POPL (2018), 33:1–33:28.

M. Mitzenmacher and E. Upfal. 2005. *Probability and Computing: Randomized Algorithms and Probabilistic Analysis*. Cambridge University Press.

David Monniaux. 2001. An Abstract Analysis of the Probabilistic Termination of Programs. In *Proc. of 8th SAS (LNCS)*, Vol. 2126. Springer, 111–126.

G. Moser and M. Schaper. 2018. From Jinja Bytecode to Term Rewriting: A Complexity Reflecting Transformation. *IC* 261, Part (2018), 116–143. https://doi.org/10.1016/j.ic.2018.05.007

N. C. Ngo, Q. Carbonneaux, and J. Hoffmann. 2018. Bounded Expectations: Resource Analysis for Probabilistic Programs. In *Proc. of 39th PLDI*. ACM, 496–512.

V. Chan Ngo, M. Dehesa-Azuara, M. Fredrikson, and J. Hoffmann. 2017. Verifying and Synthesizing Constant-Resource Implementations with Types. In *Proc. of the IEEE Symposium on Security & Privacy*. 710–728.

F. Olmedo, B. L. Kaminski, J.-P. Katoen, and C. Matheja. 2016. Reasoning about Recursive Probabilistic Programs. In *Proc. of 31nd LICS*. 672–681.

E. Schlechter. 1996. *Handbook of Analysis and Its Foundations*. Elsevier.

R. Sedgewick and P. Flajolet. 1996. *An introduction to the analysis of algorithms*. Addison-Wesley-Longman.

M. Sinn, F. Zuleger, and H. Veith. 2016. A simple and scalable static analysis for bound analysis and amortized complexity analysis. In *Software Engineering (LNI)*, Vol. 252. 101–102.

M. Sinn, F. Zuleger, and H. Veith. 2017. Complexity and Resource Bound Analysis of Imperative Programs Using Difference Constraints. *JAR* 59, 1 (2017), 3–45. https://doi.org/10.1007/s10817-016-9402-4

T. Takisaka, Y. Oyabu, N. Urabe, and I. Hasuo. 2018. Ranking and Repulsing Supermartingales for Reachability in Probabilistic Programs. In *Proc. of 16th ATVA (LNCS)*, Vol. 11138. Springer, 476–493.

D. Wang, J. Hoffmann, and T. W. Reps. 2018. PMAF: an algebraic framework for static analysis of probabilistic programs. In *Proc. of 39th PLDI*. 513–528. https://doi.org/10.1145/3192366.3192408

P. Wang, H. Fu, A. K. Goharshady, K. Chatterjee, X. Qin, and W. Shi. 2019. Cost Analysis of Nondeterministic Probabilistic Programs. In *Proc. of 40th PLDI*. ACM, 204–220.

B. Wegbreit. 1975. Mechanical Program Analysis. *Comm. ACM* 18, 9 (1975), 528–539.

B. Wegbreit. 1976. Verifying Program Performance. *JACM* 23, 4 (1976), 691–699. https://doi.org/10.1145/321978.321987

R. Wilhelm, J. Engblom, A. Ermedahl, N. Holsti, S. Thesing, D. Whalley, G. Bernat, C. Ferdinand, R. Heckmann, T. Mitra, F. Mueller, I. Puaut, P. Puschner, J. Staschulat, and P. Stenstrom. 2008. The Worst Case Execution Time Problem - Overview of Methods and Survey of Tools. *TECS* 7, 3 (2008), 1–53.

R. Wilhelm and D. Grund. 2014. Computation takes time, but how much? *Comm. ACM* 57, 2 (2014), 94–103. https://doi.org/10.1145/2500886

G. Winskel. 1993. *The Formal Semantics of Programming Languages*. MIT Press.

A MATHEMATICAL BACKGROUND

Proposition A.1 (Function Lifting of ω-CPOs [Winskel 1993, Section 8.3.3]). *Let $(D, \sqsubseteq)$ be an ω-CPO. Then $(A \to D, \sqsubseteq\!\!\!\sqsubseteq)$ where $\sqsubseteq\!\!\!\sqsubseteq$ extends $\sqsubseteq$ point-wise forms an ω-CPO, with the supremum on $A \to D$ given point-wise. If $\sqsubseteq$ has least and greatest elements $\bot$ and $\top$, then $\bot\!\!\!\bot$ and $\top\!\!\!\top$ are the least and greatest elements of $\sqsubseteq\!\!\!\sqsubseteq$, respectively.*

Theorem A.2 (Kleene's Fixed-Point Theorem for ω-CPOs, [Winskel 1993, Theorem 5.11]). *Let $(D, \sqsubseteq)$ be a ω-CPO with least element $\bot$. Let $\chi \colon D \to D$ be continuous (thus monotone). Then χ has a least fixed-point given by*

$$\mathsf{lfp}(\chi) = \sup_{n \in \mathbb{N}} \chi^n(\bot) \ .$$

Lemma A.3 (Continuity of Expectation). $\mathbb{E}_\mu(\sup_{n\in\mathbb{N}} f_n) = \sup_{n\in\mathbb{N}} \mathbb{E}_\mu(f_n)$ *for all ω-chains $(f_n)_{n\in\mathbb{N}}$.*

Proof. This is the discrete version of Lebesgue's Monotone Convergence Theorem [Schlechter 1996, Theorem 21.38]. □

B MISSING PROOFS

Proofs of Section 3

Proposition 3.2 (Cost functions form an ω-CPO). *For any A, $(\mathbb{C}^A, \preceq)$ is an ω-CPO, with least and greatest element $\mathbf{0}$ and ∞, respectively. The supremum of ω-chains $(f_n)_{n\in\mathbb{N}}$ is given point-wise:* $\sup_{n\in\mathbb{N}} f_n \triangleq \lambda a.\, \sup_{n\in\mathbb{N}} f_n(a)$.

Proof. Since $(\mathbb{C}, \leq)$ form an ω-CPO with least element 0 and greatest element ∞, the proposition follows by Proposition A.1. □

In the remainder of this section, we prove Lemma 3.4 and Theorem 3.5. Recall that

$$\chi_f(g) = \lambda a. \begin{cases} f(a) & \text{if } a\!\downarrow, \\ \sup\{w + \mathbb{E}_\mu(g) \mid a \xrightarrow{w} \mu\} & \text{else.} \end{cases}$$

Lemma B.1 (Well-definedness of $\mathsf{ect}[\to]$). *The stepping function $\chi_f(g)$ is continues in f and g, that is,*

(1) $\chi_{\sup_{n\in\mathbb{N}} f_n}(g) = \sup_{n\in\mathbb{N}} \chi_{f_n}(g)$ for all ω-chains $(f_n)_{n\in\mathbb{N}}$; and
(2) $\chi_f(\sup_{n\in\mathbb{N}} g) = \sup_{n\in\mathbb{N}} \chi_f(g_n)$ for all ω-chains $(g_n)_{n\in\mathbb{N}}$.

Proof. Point 1 follows by a simple case analysis on arguments a.
Concerning Point 2 we have to prove that

$$\chi_f(\sup_{n\in\mathbb{N}} g_n)(a) = \sup_{n\in\mathbb{N}} \chi_f(g_n)(a) \ ,$$

for every chain $g_1 \preceq g_2 \preceq \cdots$ and all $a \in A$. If $a\!\downarrow$ the claim is trivial. As a consequence of Lemma A.3, the cost transformer

$$h_{\mu,w} \triangleq \lambda f.\, w + \mathbb{E}_\mu(f) \ ,$$

is continuous. Now observe that for any doubly indexed sequence $(r_{i,j})_{i\in I, j\in J}$ of extended reals,

$$\sup_{i\in I} \sup_{j\in J} r_{i,j} = \sup_{j\in J} \sup_{i\in I} r_{i,j} \ .$$

We thus obtain

$$\begin{aligned}
\chi_f(\sup_{n\in\mathbb{N}} g_n)(a) &= \sup_{a \xrightarrow{w}_\mu} h_{\mu,w}(\sup_{n\in\mathbb{N}} g_n) && \text{(by definition)}\\
&= \sup_{a \xrightarrow{w}_\mu} \sup_{n\in\mathbb{N}} h_{\mu,w}(g_n) && \text{(continuity of } h_{\mu,w}\text{)}\\
&= \sup_{n\in\mathbb{N}} \sup_{a \xrightarrow{w}_\mu} h_{\mu,w}(g_n) && \text{(observation)}\\
&= \sup_{n\in\mathbb{N}} \chi_{g_n}(a) && \text{(by definition) .}
\end{aligned}$$

□

Lemma B.2 (Continuity of ect[→]). *The expected cost transformer* ect[→] *is continuous, ie.*

$$\mathrm{ect}[\to](\sup_{n\in\mathbb{N}} f_n) = \sup_{n\in\mathbb{N}} \mathrm{ect}[\to](f_n) \ ,$$

for all ω-chains $(f_n)_{n\in\mathbb{N}}$.

Proof. It is well known that the least fixed point operator is continuous on continues functions [Winskel 1993, Chapter 8], particularly, by Lemma B.1(2) this implies

$$\mathrm{lfp}(\sup_{n\in\mathbb{N}} \chi_{f_n}) = \sup_{n\in\mathbb{N}} \mathrm{lfp}(\chi_{f_n}) \ .$$

Thus

$$\begin{aligned}
\mathrm{ect}[\to](\sup_{n\in\mathbb{N}}(f_n)) &= \mathrm{lfp}(\chi_{\sup_{n\in\mathbb{N}} f_n}) && \text{(by definition)}\\
&= \mathrm{lfp}(\sup_{n\in\mathbb{N}} \chi_{f_n}) && \text{(Lemma B.1(1))}\\
&= \sup_{n\in\mathbb{N}} \mathrm{lfp}(\chi_{f_n}) && \text{(above observation)}\\
&= \sup_{n\in\mathbb{N}} \mathrm{ect}[\to](f_n) \ .
\end{aligned}$$

□

Theorem 3.5 (Expected Cost via Cost Transformer).

$$\mathrm{ecost}[\to] = \mathrm{ect}[\to](\mathbf{0}) \ .$$

Proof. A standard induction reveals that $\chi_f^n(\mathbf{0}) = \sup\{w \mid a \xrightarrow{w}\!\!\!\!\!\rightarrow^n \mu\}$. Consequently, by Kleene's Fixed-Point Theorem

$$\begin{aligned}
\mathrm{ect}[\to](f) &= \sup_{n\in\mathbb{N}} \chi_f^n(\mathbf{0})\\
&\quad \text{(above observation)}\\
&= \sup_{n\in\mathbb{N}} \sup\{w \mid a \xrightarrow{w}\!\!\!\!\!\rightarrow^n \mu\}\\
&\quad (\{w \mid a \xrightarrow{w}\!\!\!\!\!\rightarrow^* \mu\} = \bigcup_{n\in\mathbb{N}} \{w \mid a \xrightarrow{w}\!\!\!\!\!\rightarrow^n \mu\})\\
&= \sup\{w \mid a \xrightarrow{w}\!\!\!\!\!\rightarrow^* \mu\}\\
&\quad \text{(by definition)}\\
&= \mathrm{ect}[\to](\mathbf{0})
\end{aligned}$$

□

Proofs of Section 5

Lemma B.3 (Continuity of Expectation Transformers). *For every ω-chain $(f_n)_{n\in\mathbb{N}}$,*

$$\mathrm{ect}[\mathtt{C}](\sup_{n\in\mathbb{N}} f_n) = \sup_{n\in\mathbb{N}} \mathrm{ect}[\mathtt{C}](f_n)\ .$$

Proof. The proof is by induction on the command C.

- Case $\mathtt{consume}(e)$. We have

$$\begin{aligned}
&\mathrm{ect}[\mathtt{consume}(e)](\sup_{n\in\mathbb{N}} f_n)\\
&\quad= \langle e\rangle + \sup_{n\in\mathbb{N}} f_n && (\textit{by definition})\\
&\quad= \sup_{n\in\mathbb{N}} (\langle e\rangle + f_n) && (\langle e\rangle \textit{ is constant wrt. } n\in\mathbb{N})\\
&\quad= \sup_{n\in\mathbb{N}} \mathrm{ect}[\mathtt{consume}(e)](f_n) && (\textit{by definition})\ .
\end{aligned}$$

- Case skip. As above, we have

$$\mathrm{ect}[\mathtt{skip}](\sup_{n\in\mathbb{N}} f_n) = \sup_{n\in\mathbb{N}} f_n = \sup_{n\in\mathbb{N}} \mathrm{ect}[\mathtt{skip}](f_n)\ .$$

- Case abort. By definition,

$$\mathrm{ect}[\mathtt{abort}](\sup_{n\in\mathbb{N}} f_n) = \mathbf{0} = \sup_{n\in\mathbb{N}} \mathrm{ect}[\mathtt{abort}](f_n)\ .$$

- Case $x \coloneqq d$. As a consequence of Lemma A.3, we have

$$\mathbb{E}_\delta(\sup_{n\in\mathbb{N}} g_n) = \sup_{n\in\mathbb{N}} \mathbb{E}_\delta(g_n)\ ,$$

for all distribution $\delta \in \mathcal{D}(\mathbb{Z})$ and $g_i\colon \mathbb{Z} \to \mathbb{R}^\infty_{\geq 0}$, where $\sup_{n\in\mathbb{N}} g_n \triangleq \lambda i.\, \sup_{n\in\mathbb{N}} g_n(i)$. Thus we have

$$\begin{aligned}
&\mathrm{ect}[x \coloneqq d](\sup_{n\in\mathbb{N}} f_n)\\
&\quad= \lambda\sigma.\mathbb{E}_{d(\sigma)}(\lambda i.(\sup_{n\in\mathbb{N}} f_n)(\sigma[x/i])) && (\textit{definition})\\
&\quad= \lambda\sigma.\mathbb{E}_{d(\sigma)}(\sup_{n\in\mathbb{N}} \lambda i.f_n(\sigma[x/i])) && (\textit{def. } \sup)\\
&\quad= \lambda\sigma.\sup_{n\in\mathbb{N}} \mathbb{E}_{d(\sigma)}(\lambda i.f_n(\sigma[x/i])) && (\textit{MCT})\\
&\quad= \sup_{n\in\mathbb{N}} \lambda\sigma.\mathbb{E}_{d(\sigma)}(\lambda i.f_n(\sigma[x/i])) && (\textit{def. } \sup)\\
&\quad= \sup_{n\in\mathbb{N}} \mathrm{ect}[x \coloneqq d](f_n) && (\textit{definition})\ .
\end{aligned}$$

- Case C;D. We have

$$\begin{aligned}
&\mathrm{ect}[\mathtt{C};\mathtt{D}](\sup_{n\in\mathbb{N}} f_n)\\
&\quad= \mathrm{ect}[\mathtt{C}](\mathrm{ect}[\mathtt{D}](\sup_{n\in\mathbb{N}} f_n)) && (\textit{definition})\\
&\quad= \mathrm{ect}[\mathtt{C}](\sup_{n\in\mathbb{N}} \mathrm{ect}[\mathtt{D}](f_n)) && (\textit{IH on } \mathtt{D})\\
&\quad= \sup_{n\in\mathbb{N}} \mathrm{ect}[\mathtt{C}](\mathrm{ect}[\mathtt{D}](f_n)) && (\textit{IH on } \mathtt{C})\\
&\quad= \sup_{n\in\mathbb{N}} \mathrm{ect}[\mathtt{C};\mathtt{D}](f_n) && (\textit{definition})\ .
\end{aligned}$$

- Case `if` (ϕ) {C} {D}. We have

$$\begin{aligned}
&\mathrm{ect}[\texttt{if } (\phi) \ \{\texttt{C}\} \ \{\texttt{D}\}](\sup_{n\in\mathbb{N}} f_n)\\
&\quad (\textit{definition})\\
&= [\phi] \cdot \mathrm{ect}[\texttt{C}](\sup_{n\in\mathbb{N}} f_n) + [\neg\phi] \cdot \mathrm{ect}[\texttt{D}](\sup_{n\in\mathbb{N}} f_n)\\
&\quad (\textit{IH on } \texttt{C} \textit{ and } \texttt{D})\\
&= [\phi] \cdot (\sup_{n\in\mathbb{N}} \mathrm{ect}[\texttt{C}](f_n)) + [\neg\phi] \cdot (\sup_{n\in\mathbb{N}} \mathrm{ect}[\texttt{D}](f_n))\\
&\quad ([\phi] \textit{ constant wrt. } n \in \mathbb{N})\\
&= (\sup_{n\in\mathbb{N}} [\phi] \cdot \mathrm{ect}[\texttt{C}](f_n)) + (\sup_{n\in\mathbb{N}} [\neg\phi] \cdot \mathrm{ect}[\texttt{D}](f_n))\\
&= \sup_{n\in\mathbb{N}} [\phi] \cdot \mathrm{ect}[\texttt{C}](f_n) + [\neg\phi] \cdot \mathrm{ect}[\texttt{D}](f_n)\\
&\quad (\textit{definition})\\
&= \sup_{n\in\mathbb{N}} \mathrm{ect}[\texttt{if } (\phi) \ \{\texttt{C}\} \ \{\texttt{D}\}](f_n)\ .
\end{aligned}$$

- Case `while` (ϕ) {C}. Reconsider the characteristic function of `while` (ϕ) {C} wrt. expectation f:

$$\chi_f^{\langle\phi,\texttt{C}\rangle} = \lambda F.[\phi] \cdot \mathrm{ect}[\texttt{C}](F) + [\neg\phi] \cdot f\ .$$

Observe that (i) $\chi^{\langle\phi,\texttt{C}\rangle}_{\sup_{n\in\mathbb{N}} f_n} = \sup_{n\in\mathbb{N}} \chi^{\langle\phi,\texttt{C}\rangle}_{f_n}$, and moreover, from induction hypothesis it follows that all $\chi^{\langle\phi,\texttt{C}\rangle}_{f_n}$ are continuous. The least fixed-point operator is continues on continuous functions, particularly (ii) $\mathrm{lfp}(\sup_{n\in\mathbb{N}} \chi^{\langle\phi,\texttt{C}\rangle}_{f_n}) = \sup_{n\in\mathbb{N}} \mathrm{lfp}(\chi^{\langle\phi,\texttt{C}\rangle}_{f_n})$. Thus we get

$$\begin{aligned}
&\mathrm{ect}[\texttt{while } (\phi) \ \{\texttt{C}\}](\sup_{n\in\mathbb{N}} f_n)\\
&= \mathrm{lfp}(\chi^{\langle\phi,\texttt{C}\rangle}_{\sup_{n\in\mathbb{N}} f_n}) && (\textit{definition})\\
&= \mathrm{lfp}(\sup_{n\in\mathbb{N}} \chi^{\langle\phi,\texttt{C}\rangle}_{f_n}) && (\textit{observation (i)})\\
&= \sup_{n\in\mathbb{N}} \mathrm{lfp}(\chi^{\langle\phi,\texttt{C}\rangle}_{f_n}) && (\textit{observation (ii)})\\
&= \sup_{n\in\mathbb{N}} \mathrm{ect}[\texttt{while } (\phi) \ \{\texttt{C}\}](f_n) && (\textit{definition})\ .
\end{aligned}$$

- Case {C} <> {D}. For the case of non-deterministic choice, observe that for expectations g_n and h_n $(n \in \mathbb{N})$ we have

$$\mathbf{max}(\sup_{n\in\mathbb{N}} g_n, \sup_{n\in\mathbb{N}} h_n) = \sup_{n\in\mathbb{N}} \mathbf{max}(g_n, h_n)\ .$$

Consequently,

$$\begin{aligned}
&\mathrm{ect}[\{\texttt{C}\} <> \{\texttt{D}\}](\sup_{n\in\mathbb{N}} f_n)\\
&= \mathbf{max}(\mathrm{ect}[\texttt{C}](\sup_{n\in\mathbb{N}} f_n), \mathrm{ect}[\texttt{D}](\sup_{n\in\mathbb{N}} f_n)) && (\textit{definition})\\
&= \mathbf{max}(\sup_{n\in\mathbb{N}} \mathrm{ect}[\texttt{C}](f_n), \sup_{n\in\mathbb{N}} \mathrm{ect}[\texttt{D}](f_n)) && (\textit{IH on } \texttt{C} \textit{ and } \texttt{D})\\
&= \sup_{n\in\mathbb{N}} \mathbf{max}(\mathrm{ect}[\texttt{C}](f_n), \mathrm{ect}[\texttt{D}](f_n)) && (\textit{observation})\\
&= \sup_{n\in\mathbb{N}} \mathrm{ect}[\{\texttt{C}\} <> \{\texttt{D}\}](f_n) && (\textit{definition})\ .
\end{aligned}$$

□

Lemma B.4 (Monotonicity of Transformers).

$$f \preceq g \implies \mathrm{ect}[\mathtt{C}](f) \preceq \mathrm{ect}[\mathtt{C}](g) \ .$$

Proof. This is an immediate consequence of Lemma B.3. □

Lemma 5.2 (Central Properties of ect[while (ϕ) {C}]).

(1) continuity*:* $\mathrm{ect}[\mathtt{C}](\sup_{n\in\mathbb{N}} f_n) = \sup_{n\in\mathbb{N}} \mathrm{ect}[\mathtt{C}](f_n)$ *for all* ω*-chains* $(f_n)_{n\in\mathbb{N}}$*;*
(2) monotonicity*:* $f \preceq g \implies \mathrm{ect}[\mathtt{C}](f) \preceq \mathrm{ect}[\mathtt{C}](g)$*.*

Proof. By Lemma B.3 and Lemma B.4. □

Proofs of Section 5.2

To ease readability of the proofs that follow, let us define recursively

$$\begin{aligned}
\mathrm{ect}[\to]^{(0)}(f)(\gamma) &\triangleq 0 \\
\mathrm{ect}[\to]^{(n+1)}(f)(\sigma) &\triangleq f(\sigma) \\
\mathrm{ect}[\to]^{(n+1)}(f)(\sigma \triangleright \mathtt{C}) &\triangleq \\
&\quad \sup\{w + \mathbb{E}_\mu(\mathrm{ect}[\to]^{(n)}(f)) \mid \sigma \triangleright \mathtt{C} \xrightarrow{w} \mu\} \ .
\end{aligned}$$

Then $\mathrm{ect}[\to]^{(n)}$ give us finite approximations of $\mathrm{ect}[\to](f)$ in the following sense.

Lemma B.5.

$$\mathrm{ect}[\to](f) = \sup_{n\in\mathbb{N}} \mathrm{ect}[\to]^{(n)}(f) \ .$$

Proof. Recall that $\mathrm{ect}[\to](f) = \mathsf{lfp}(\chi_f) = \chi_f^n(\mathbf{0})$, since terminal objects are precisely the stores σ we get

$$\chi_f(g) = \lambda\gamma. \begin{cases} f(\sigma) & \text{if } \gamma = \sigma \in \Sigma, \\ \sup\{w + \mathbb{E}_\mu(g) \mid \gamma \xrightarrow{w} \mu\} & \text{else.} \end{cases}$$

It is thus sufficient to show that $\mathrm{ect}[\to]^{(n)}(f) = \chi_f^n(\mathbf{0})$. This follows by a standard induction on n. □

Observe that $\mathrm{ect}[\to]^{(n)}(f)$ is monotone in f and m, ie. $\mathrm{ect}[\to]^{(n)}(f) \preceq \mathrm{ect}[\to]^{(m)}(g)$ if $f \preceq g$ and $n \leq m$.

Lemma B.6.

$$\mathrm{ect}[\to]^{(n)}(f)(\bullet \triangleright \mathtt{C};\mathtt{D}) \preceq \mathrm{ect}[\to]^{(n)}(\mathrm{ect}[\to]^{(n)}(f)(\bullet \triangleright \mathtt{D}))(\bullet \triangleright \mathtt{C}) \ .$$

Proof. The proof is by induction on n. It is sufficient to consider the inductive step. Fix $\sigma \in \Sigma$, and suppose $\sigma \triangleright \mathtt{C};\mathtt{D} \xrightarrow{w} \mu$, hence $\sigma \triangleright \mathtt{C} \xrightarrow{w} \nu$ where

$$\begin{aligned}
\mu &= \{\!\{p_i : \sigma_i \triangleright \mathtt{D}\}\!\}_{i\in I} \uplus \{\!\{q_j : \tau_j \triangleright \mathtt{C}_j;\mathtt{D}\}\!\}_{j\in J} \text{ for,} \\
\nu &= \{\!\{p_i : \sigma_i\}\!\}_{i\in I} \uplus \{\!\{q_j : \tau_j \triangleright \mathtt{C}_j\}\!\}_{j\in J} \ .
\end{aligned}$$

Abbreviate $g = \mathrm{ect}[\to]^{(n)}(f)(\bullet \triangleright \mathtt{D})$ and observe that

$$\begin{aligned}
&\mathbb{E}_\mu(\mathrm{ect}[\to]^{(n)}(f)) \\
&\quad = \sum_{i\in I} p_i \cdot \mathrm{ect}[\to]^{(n)}(f)(\sigma_i \triangleright \mathtt{D}) \\
&\qquad + \sum_{j\in J} q_j \cdot \mathrm{ect}[\to]^{(n)}(f)(\tau_j \triangleright \mathtt{C}_j;\mathtt{D}) \\
&\qquad (\textit{induction hypothesis}) \\
&\quad \le \sum_{i\in I} p_i \cdot \mathrm{ect}[\to]^{(n)}(f)(\sigma_i \triangleright \mathtt{D}) \\
&\qquad + \sum_{j\in J} q_j \cdot \mathrm{ect}[\to]^{(n)}(g)(\tau_j \triangleright \mathtt{C}_j) \\
&\qquad (\textit{since } \mathrm{ect}[\to]^{(n)}(f)(\sigma_i \triangleright \mathtt{D}) = \mathrm{ect}[\to]^{(n)}(g)(\sigma_i)) \\
&\quad = \mathbb{E}_\nu(\mathrm{ect}[\to]^{(n)}(g))
\end{aligned}$$

In conclusion

$$\begin{aligned}
&\mathrm{ect}[\to]^{(n+1)}(f)(\sigma \triangleright \mathtt{C};\mathtt{D}) \\
&\quad (\textit{definition of } \mathrm{ect}[\to]^{(n+1)}(f)) \\
&= \sup\{w + \mathbb{E}_\mu(\mathrm{ect}[\to]^{(n)}(f)) \mid \sigma \triangleright \mathtt{C};\mathtt{D} \xrightarrow{w} \mu\} \\
&\quad (\textit{above observation}) \\
&\le \sup\{w + \mathbb{E}_\nu(\mathrm{ect}[\to]^{(n)}(g)(\sigma \triangleright \mathtt{C})) \mid \sigma \triangleright \mathtt{C} \xrightarrow{w} \nu\} \\
&\quad (\textit{definition of } \mathrm{ect}[\to]^{(n)}(g)) \\
&= \mathrm{ect}[\to]^{(n+1)}(g)(\sigma \triangleright \mathtt{C}) \\
&\quad (g \le \mathrm{ect}[\to]^{(n+1)}(f)(\bullet \triangleright \mathtt{D}) \textit{ and monoton. of } \mathrm{ect}[\to]^{(n+1)}) \\
&\le \mathrm{ect}[\to]^{(n+1)}(\mathrm{ect}[\to]^{(n+1)}(f)(\bullet \triangleright \mathtt{D}))(\sigma \triangleright \mathtt{C}) \,. \qquad \square
\end{aligned}$$

Lemma B.7 (Composition).

$$\mathrm{ect}[\to](f)(\bullet \triangleright \mathtt{C};\mathtt{D}) = \mathrm{ect}[\to](\mathrm{ect}[\to](f)(\bullet \triangleright \mathtt{D}))(\bullet \triangleright \mathtt{C}) \,.$$

Proof. Note that *lhs* $\le$ *rhs* is an immediate consequence of Lemma B.5 and Lemma B.6. For the inverse direction, let us abbreviate $g = \mathrm{ect}[\to](f)(\bullet \triangleright \mathtt{D})$. By Lemma B.5, it is sufficient to show

$$\mathrm{ect}[\to]^{(n)}(g)(\bullet \triangleright \mathtt{C}) \le \mathrm{ect}[\to](f)(\bullet \triangleright \mathtt{C};\mathtt{D})$$

for all $n \in \mathbb{N}$. The proof is by induction on n, we consider the inductive step. Suppose $\sigma \triangleright \mathtt{C} \xrightarrow{w} \mu$, hence $\sigma \triangleright \mathtt{C};\mathtt{D} \xrightarrow{w} \nu$ where

$$\begin{aligned}
\mu &= \{\!\{p_i : \sigma_i\}\!\}_{i\in I} \uplus \{\!\{q_j : \tau_j \triangleright \mathtt{C}_j\}\!\}_{j\in J} \,, \text{ and} \\
\nu &= \{\!\{p_i : \sigma_i \triangleright \mathtt{D}\}\!\}_{i\in I} \uplus \{\!\{q_j : \tau_j \triangleright \mathtt{C}_j;\mathtt{D}\}\!\}_{j\in J} \,.
\end{aligned}$$

Observe

$$\begin{aligned}
&\mathbb{E}_\mu(\mathrm{ect}[\rightarrow]^{(n)}(g)) \\
&\quad (\textit{definition of } \mathrm{ect}[\rightarrow]^{(n)}(g)) \\
&= \sum_{i\in I} p_i \cdot g(\sigma_i) + \sum_{j\in J} q_j \cdot \mathrm{ect}[\rightarrow]^{(n)}(g)(\tau_j \triangleright \mathtt{C}_j) \\
&\quad (\textit{induction hypothesis}) \\
&\leq \sum_{i\in I} p_i \cdot g(\sigma_i) + \sum_{j\in J} q_j \cdot \mathrm{ect}[\rightarrow](f)(\tau_j \triangleright \mathtt{C}_j;\mathtt{D}) \\
&\quad (\textit{since } g(\sigma_i) = \mathrm{ect}[\rightarrow](f)(\sigma_i \triangleright \mathtt{D})) \\
&= \mathbb{E}_\nu(\mathrm{ect}[\rightarrow](f)) \ .
\end{aligned}$$

Conclusively,

$$\begin{aligned}
&\mathrm{ect}[\rightarrow]^{(n+1)}(g)(\sigma \triangleright \mathtt{C}) \\
&\quad (\textit{definition of } \mathrm{ect}[\rightarrow]^{(n+1)}(g)) \\
&= \sup\{w + \mathbb{E}_\mu(\mathrm{ect}[\rightarrow]^{(n)}(g)) \mid \sigma \triangleright \mathtt{C} \xrightarrow{w} \mu\} \\
&\quad (\textit{above observation}) \\
&\leq \sup\{w + \mathbb{E}_\nu(\mathrm{ect}[\rightarrow](f)) \mid \sigma \triangleright \mathtt{C};\mathtt{D} \xrightarrow{w} \nu\} \\
&= \mathrm{ect}[\rightarrow](f)(\sigma \triangleright \mathtt{C};\mathtt{D}) \ .
\end{aligned}$$

□

Lemma B.8 (Loops).

$$\mathrm{ect}[\rightarrow](f)(\bullet \triangleright \mathtt{while}\ (\phi)\ \{\mathtt{C}\}) = \mathsf{lfp}(g.[\![\phi]\!] \cdot \mathrm{ect}[\rightarrow](g)(\bullet \triangleright \mathtt{C}) + [\![\neg\phi]\!] \cdot f) \ .$$

Proof. Define

$$\Gamma_f^{(0)} \triangleq \mathbf{0} \qquad \Gamma_f^{(n+1)} \triangleq [\![\phi]\!] \cdot \mathrm{ect}[\rightarrow](\Gamma_f^{(n)})(\bullet \triangleright \mathtt{C}) + [\![\neg\phi]\!] \cdot f \ .$$

Consequently, the right-hand side *rhs* is equal to $\sup_{n\in\mathbb{N}} \Gamma_f^{(n)}$. To prove $lhs \leq rhs$, we show

$$\mathrm{ect}[\rightarrow]^{(n)}(f)(\bullet \triangleright \mathtt{while}\ (\phi)\ \{\mathtt{C}\}) \leq \Gamma_f^{(n)} \ ,$$

by induction on n. It is sufficient to consider the inductive step, where we have

$$\begin{aligned}
&\mathrm{ect}[\to]^{(n+1)}(f)(\bullet \triangleright \texttt{while}\ (\phi)\ \{\mathtt{C}\}) \\
&\quad (\textit{definition of}\ \mathrm{ect}[\to]^{(n+1)}(f)\textit{; case analysis on}\ \sigma \vDash \phi) \\
&= [\phi] \cdot \mathrm{ect}[\to]^{(n)}(f)(\bullet \triangleright \mathtt{C}; \texttt{while}\ (\phi)\ \{\mathtt{C}\}) + [\neg\phi] \cdot f \\
&\quad (\textit{Lemma B.6}) \\
&\leq [\phi] \cdot \mathrm{ect}[\to]^{(n)}(\mathrm{ect}[\to]^{(n)}(\bullet \triangleright \texttt{while}\ (\phi)\ \{\mathtt{C}\}))(\bullet \triangleright \mathtt{C}) \\
&\quad + [\neg\phi] \cdot f \\
&\quad (\textit{IH \& monotonicity of}\ \mathrm{ect}[\to]^{(n)}(\cdot)(\bullet \triangleright \mathtt{C})) \\
&\leq [\phi] \cdot \mathrm{ect}[\to]^{(n)}(\Gamma_f^{(n)})(\bullet \triangleright \mathtt{C}) + [\neg\phi] \cdot f \\
&\quad (\textit{definition of}\ \Gamma_f^{(n+1)}) \\
&= \Gamma_f^{(n)} \ .
\end{aligned}$$

Hence, by Lemma B.5,

$$\begin{aligned}
\mathit{lhs} &= \sup_{n\in\mathbb{N}} \mathrm{ect}[\to]^{(n)}(f)(\bullet \triangleright \texttt{while}\ (\phi)\ \{\mathtt{C}\}) \\
&\leq \sup_{n\in\mathbb{N}} \Gamma_f^{(n)} = \mathit{rhs}\ .
\end{aligned}$$

Finally, to prove $\mathit{rhs} \leq \mathit{lhs}$, we show

$$\Gamma_f^{(n)} \leq \mathrm{ect}[\to](f)(\bullet \triangleright \texttt{while}\ (\phi)\ \{\mathtt{C}\})\ ,$$

by induction on n. Then

$$\begin{aligned}
&\Gamma_f^{(n+1)} \\
&\quad (\textit{definition of}\ \Gamma_f^{(n+1)}) \\
&= [\phi] \cdot \mathrm{ect}[\to](\Gamma_f^{(n)})(\bullet \triangleright \mathtt{C}) + [\neg\phi] \cdot f \\
&\quad (\textit{induction hypothesis}) \\
&= [\phi] \cdot \mathrm{ect}[\to](\mathrm{ect}[\to](f)(\bullet \triangleright \texttt{while}\ (\phi)\ \{\mathtt{C}\}))(\bullet \triangleright \mathtt{C}) \\
&\quad + [\neg\phi] \cdot f \\
&\quad (\textit{Lemma B.6}) \\
&= [\phi] \cdot \mathrm{ect}[\to](f)(\bullet \triangleright \mathtt{C}; \texttt{while}\ (\phi)\ \{\mathtt{C}\}) + [\neg\phi] \cdot f \\
&\quad (\textit{definition of}\ \mathrm{ect}[\to](f)\textit{; case analysis on}\ \sigma \vDash \phi) \\
&= \mathrm{ect}[\to](f)(\bullet \triangleright \texttt{while}\ (\phi)\ \{\mathtt{C}\})\ .
\end{aligned}$$

□

Lemma 5.3 (Composition and Loop Lemma).
(1) $\mathrm{ect}[\to](f)(\bullet \triangleright \mathtt{C};\mathtt{D}) = \mathrm{ect}[\to](\mathrm{ect}[\to](f)(\bullet \triangleright \mathtt{D}))(\bullet \triangleright \mathtt{C})$*;*
(2) $\mathrm{ect}[\to](f)(\bullet \triangleright \texttt{while}\ (\phi)\ \{\mathtt{C}\}) = \mathrm{lfp}(g.[\phi] \cdot \mathrm{ect}[\to](g)(\bullet \triangleright \mathtt{C}) + [\neg\phi] \cdot f)$.

Proof. The two properties have been proven in Lemma B.7 and Lemma B.8, respectively. □

Theorem 5.4 (Soundness & Completeness). *For every command* $\mathtt{C} \in \mathsf{Cmd}$*, we have*
(1) $\mathrm{ect}[\to](f)(\bullet \triangleright \mathtt{C}) = \mathrm{ect}[\mathtt{C}](f)$*; and consequently*
(2) $\mathrm{ecost}[\to](\bullet \triangleright \mathtt{C}) = \mathrm{ecost}[\mathtt{C}]$.

Proof. The proof of this statement is by induction on the C. The only interesting cases are those of composition and loops, which follow by Lemma B.7 and Lemma B.8, respectively. □

PROOFS OF SECTION 6

Lemma 6.2 (Separating Expected Cost and Value).

$$\mathrm{ect}[\mathtt{C}](f) \leq \mathrm{ecost}[\mathtt{C}] + \mathrm{evalue}[\mathtt{C}](f) \ .$$

Proof. One proofs the stronger property

$$\mathrm{ect}[\mathtt{C}](f + g) \leq \mathrm{ect}[\mathtt{C}](g) + \mathrm{evalue}[\mathtt{C}](f)$$

by a standard induction on C.

$$\begin{aligned}
&\mathrm{ect}[\mathtt{consume}(e)](f + g)\\
&\quad = \langle e \rangle + (g + f)\\
&\quad = (\langle e \rangle + g) + f\\
&\quad = \mathrm{ect}[\mathtt{consume}(e)](g) + \mathrm{evalue}[\mathtt{consume}(e)](f)\\
&\mathrm{ect}[\mathtt{skip}](f + g)\\
&\quad = f + g\\
&\quad = \mathrm{ect}[\mathtt{skip}](g) + \mathrm{evalue}[\mathtt{skip}](f)\\
&\mathrm{ect}[\mathtt{abort}](f + g)\\
&\quad = \mathbf{0}\\
&\quad = \mathrm{ect}[\mathtt{abort}](g) + \mathrm{evalue}[\mathtt{abort}](f)\\
&\mathrm{ect}[\mathtt{C};\mathtt{D}](f + g)\\
&\quad = \mathrm{ect}[\mathtt{C}](\mathrm{ect}[\mathtt{D}](f + g))\\
&\quad \leq \mathrm{ect}[\mathtt{C}](\mathrm{ect}[\mathtt{D}](g) + \mathrm{evalue}[\mathtt{D}](f))\\
&\quad \leq \mathrm{ect}[\mathtt{C}](\mathrm{ect}[\mathtt{D}](g)) + \mathrm{evalue}[\mathtt{C}](\mathrm{evalue}[\mathtt{D}](f))\\
&\quad = \mathrm{ect}[\mathtt{C};\mathtt{D}](g) + \mathrm{evalue}[\mathtt{C};\mathtt{D}](f)
\end{aligned}$$

$$
\begin{aligned}
&\mathrm{ect}[x \coloneqq d](f+g)\\
&\quad = \lambda\sigma.\mathbb{E}_{d(\sigma)}(\lambda v.(f+g)[x/v](\sigma))\\
&\quad = \lambda\sigma.\mathbb{E}_{d(\sigma)}(\lambda v.g[x/v](\sigma)) + \lambda\sigma.\mathbb{E}_{d(\sigma)}(\lambda v.f[x/v](\sigma))\\
&\quad = \mathrm{ect}[x \coloneqq d](g) + \mathrm{evalue}[x \coloneqq d](f)\\
&\mathrm{ect}[\texttt{if } (\phi)\ \{\mathtt{C}\}\ \{\mathtt{D}\}](f+g)\\
&\quad = [\phi]\cdot \mathrm{ect}[\mathtt{C}](f+g) + [\neg\phi]\cdot \mathrm{ect}[\mathtt{D}](f+g)\\
&\quad \le [\phi]\cdot (\mathrm{ect}[\mathtt{C}](g) + \mathrm{evalue}[\mathtt{C}](f)) + [\neg\phi]\cdot (\mathrm{ect}[\mathtt{D}](g) + \mathrm{evalue}[\mathtt{D}](f))\\
&\quad = [\phi]\cdot \mathrm{ect}[\mathtt{C}](g) + [\neg\phi]\cdot \mathrm{ect}[\mathtt{D}](g)\\
&\quad + [\phi]\cdot \mathrm{evalue}[\mathtt{C}](f) + [\neg\phi]\cdot \mathrm{evalue}[\mathtt{D}](f)\\
&\quad = \mathrm{ect}[\texttt{if } (\phi)\ \{\mathtt{C}\}\ \{\mathtt{D}\}](g) + \mathrm{evalue}[\texttt{if } (\phi)\ \{\mathtt{C}\}\ \{\mathtt{D}\}](f)\\
&\mathrm{ect}[\texttt{while } (\phi)\ \{\mathtt{C}\}](f+g)\\
&\quad = \chi_{f+g}^{\langle\phi,\mathtt{C}\rangle}(h)\\
&\quad = [\phi]\cdot \mathrm{ect}[\mathtt{C}](h) + [\neg\phi]\cdot (f+g)\\
&\quad \le [\phi]\cdot \mathrm{ect}[\mathtt{C}](h+h) + [\neg\phi]\cdot (f+g)\\
&\quad \le [\phi]\cdot (\mathrm{ect}[\mathtt{C}](h) + \mathrm{evalue}[\mathtt{C}](h)) + [\neg\phi]\cdot (f+g)\\
&\quad = ([\phi]\cdot \mathrm{ect}[\mathtt{C}](h) + [\neg\phi]\cdot g) + ([\phi]\cdot \mathrm{evalue}[\mathtt{C}](h) + [\neg\phi]\cdot f)\\
&\quad = \mathrm{ect}[\texttt{while } (\phi)\ \{\mathtt{C}\}](g) + \mathrm{evalue}[\texttt{while } (\phi)\ \{\mathtt{C}\}](f)\\
&\mathrm{ect}[\{\mathtt{C}\} <> \{\mathtt{D}\}](f+g)\\
&\quad = \mathbf{max}(\mathrm{ect}[\mathtt{C}](f+g), \mathrm{ect}[\mathtt{D}](f+g))\\
&\quad \le \mathbf{max}(\mathrm{ect}[\mathtt{C}](g) + \mathrm{evalue}[\mathtt{C}]f, \mathrm{ect}[\mathtt{D}](g) + \mathrm{evalue}[\mathtt{D}](f)\\
&\quad \le \mathbf{max}(\mathrm{ect}[\mathtt{C}](g), \mathrm{ect}[\mathtt{D}](g)) + \mathbf{max}(\mathrm{evalue}[\mathtt{C}](f), \mathrm{evalue}[\mathtt{D}](f))\\
&\quad = \mathrm{ect}[\{\mathtt{C}\} <> \{\mathtt{D}\}](f) + \mathrm{evalue}[\{\mathtt{C}\} <> \{\mathtt{D}\}](f)\ .
\end{aligned}
$$

□

Theorem 6.4 (Modular Upper-Invariants). *Let* C *and* κ *be as in Lemma 6.3. Then*

1. $\phi \vDash \mathrm{ecost}[\mathtt{C}] + \boldsymbol{\kappa}(\mathrm{evalue}[\mathtt{C}](b_1), \ldots, \mathrm{evalue}[\mathtt{C}](b_k)) \le I \Rightarrow \mathrm{ecost}[\texttt{while } (\phi)\ \{\mathtt{C}\}] \le I$;
2. $\phi \vDash \boldsymbol{\kappa}(\mathrm{evalue}[\mathtt{C}](b_1), \ldots, \mathrm{evalue}[\mathtt{C}](b_k)) \le I \wedge \neg\phi \vDash f \le I \Rightarrow \mathrm{evalue}[\texttt{while } (\phi)\ \{\mathtt{C}\}](f) \le I$.

Proof. Concerning the first inequality, Lemma 6.2 and Lemma 6.3 yield $\chi_f^{\langle\phi,\mathtt{C}\rangle}(\boldsymbol{\kappa}(\vec{b})) \le \hat{\chi}_f^{\langle\phi,\mathtt{C}\rangle}(\boldsymbol{\kappa}(\vec{b}))$, and consequently, the inequality witnesses that $\boldsymbol{\kappa}(\vec{b})$ is an upper invariant (Theorem 5.5) for $\texttt{while } (\phi)\ \{\mathtt{C}\}$ wrt. f. Relying only on Lemma 6.3, the second inequality witnesses that $\boldsymbol{\kappa}(\vec{b})$ is an upper invariant for the expected cost of

$$
\begin{aligned}
&\mathrm{ect}[\texttt{while } (\phi)\ \{\mathrm{costFree}(\mathtt{C})\}](f)\\
&\quad = \mathrm{ect}[\mathrm{costFree}(\texttt{while } (\phi)\ \{\mathtt{C}\})](f)\\
&\quad = \mathrm{evalue}[\texttt{while } (\phi)\ \{\mathtt{C}\}]\ .
\end{aligned}
$$

□

Theorem 6.5 (Modular Sequential Analysis). *Let* C *and* κ *be as in Lemma 6.3. Then*

1. $\mathrm{ecost}[\mathtt{D}](f) \le \boldsymbol{\kappa}(b_1, \ldots, b_k) \Rightarrow \mathrm{ecost}[\mathtt{C};\mathtt{D}] \le \mathrm{ecost}[\mathtt{C}] + \boldsymbol{\kappa}(\mathrm{evalue}[\mathtt{C}](b_1), \ldots, \mathrm{evalue}[\mathtt{C}](b_k))$;
2. $\mathrm{evalue}[\mathtt{D}](f) \le \boldsymbol{\kappa}(b_1, \ldots, b_k) \Rightarrow \mathrm{evalue}[\mathtt{C};\mathtt{D}](f) \le \boldsymbol{\kappa}(\mathrm{evalue}[\mathtt{C}](b_1), \ldots, \mathrm{evalue}[\mathtt{C}](b_k))$.

Proof. The statement follows from the definition of $\mathrm{ect}[\mathtt{C}]$, Lemma 6.2 and κ being concave.

$$\begin{aligned}
&\mathrm{ect}[\mathtt{C};\mathtt{D}](f)\\
&\quad = \mathrm{ect}[\mathtt{C}](\mathrm{ect}[\mathtt{D}](f))\\
&\quad \leq \mathrm{ect}[\mathtt{C}](\boldsymbol{\kappa}(\vec{b}))\\
&\quad = \mathrm{ecost}[\mathtt{C}] + \mathrm{evalue}[\mathtt{C}](\boldsymbol{\kappa}(\vec{b}))\\
&\quad = \mathrm{ecost}[\mathtt{C}] + \boldsymbol{\kappa}(\mathrm{evalue}[\mathtt{C}](\vec{b}))\ .
\end{aligned}$$

□