PMAF: An Algebraic Framework for Static Analysis of Probabilistic Programs

Di Wang\textsuperscript{1}, Jan Hoffmann\textsuperscript{1}, and Thomas Reps\textsuperscript{2,3}
\textsuperscript{1}Carnegie Mellon University
\textsuperscript{2}University of Wisconsin
\textsuperscript{3}GrammaTech, Inc.

Abstract
Automatically establishing that a probabilistic program satisfies some property \(\varphi\) is a challenging problem. While a sampling-based approach—which involves running the program repeatedly—can suggest that \(\varphi\) holds, to establish that the program satisfies \(\varphi\), analysis techniques must be used. Despite recent successes, probabilistic static analyses are still more difficult to design and implement than their deterministic counterparts. This paper presents a framework, called PMAF, for designing, implementing, and proving the correctness of static analyses of probabilistic programs with challenging features such as recursion, unstructured control-flow, divergence, nondeterminism, and continuous distributions. PMAF introduces pre-Markov algebras to factor out common parts of different analyses. To perform interprocedural analysis and to create procedure summaries, PMAF extends ideas from non-probabilistic interprocedural dataflow analysis to the probabilistic setting. One novelty is that PMAF is based on a semantics formulated in terms of a control-flow hyper-graph for each procedure, rather than a standard control-flow graph. To evaluate its effectiveness, PMAF has been used to reformulate and implement existing intraprocedural analyses for Bayesian-inference and the Markov decision problem, by creating corresponding interprocedural analyses. Additionally, PMAF has been used to implement a new interprocedural linear expectation-invariant analysis. Experiments with benchmark programs for the three analyses demonstrate that the approach is practical.

Keywords—Program analysis, probabilistic programming, expectation invariant, pre-Markov algebra

1 Introduction
Hermanns 2015; Gehr et al. 2016; Kaminski et al. 2016; Katoen et al. 2010; Kattenbelt et al. 2009; Olmedo et al. 2016; Sankaranarayanan et al. 2013]. Unfortunately, analyses of probabilistic programs have usually been standalone developments, and it is not immediately clear how different techniques relate.

This paper presents a framework, which we call **PMAF** (for Pre-Markov Algebra Framework), for designing, implementing, and proving the correctness of static analyses of probabilistic programs. We show how several analyses that may appear to be quite different, can be formulated—and generalized—using PMAF. Examples include Bayesian inference [Claret et al. 2013; Etessami and Yannakakis 2005, 2015], Markov decision problem with rewards [Puterman 1994], and probabilistic-invariant generation [Chakarov and Sankaranarayanan 2013; Chatterjee et al. 2016a; Katoen et al. 2010]

New constructs in probabilistic programs are of two kinds, to express **data randomness** (e.g., sampling) and **control-flow randomness** (e.g., probabilistic choice). To express both features, we introduce a new algebraic structure, called a pre-Markov algebra, which is equipped with operations corresponding to control-flow actions in probabilistic programs: **sequencing**, **conditional-choice**, **probabilistic-choice**, and **nondeterministic-choice**. PMAF is based on a new fixed-point semantics that models challenging features such as divergence, unstructured control-flow, nondeterminism, and continuous distributions. To establish correctness, we introduce **probabilistic abstractions** between two pre-Markov algebras that represent the concrete and abstract semantics.

Our work shows how, with suitable extensions, a blending of ideas from prior work on (i) static analysis of single-procedure probabilistic programs, and (ii) interprocedural dataflow analysis of standard (non-probabilistic) programs can be used to create a framework for interprocedural analysis of multi-procedure probabilistic programs. In particular,

- The semantics on which PMAF is based is an interpretation of the control-flow graphs (CFGs) for a program’s procedures. One insight is to treat each CFG as a **hyper-graph** rather than a standard graph.
- The abstract semantics is formulated so that the analyzer can obtain **procedure summaries**.

Hyper-graphs contain **hyper-edges**, each of which consists of one source node and possibly several destination nodes. Conditional-branching, probabilistic-branching, and nondeterministic-branching statements are represented by hyper-edges. In ordinary CFGs, nodes can also have several successors; however, the operator applied at a confluence point \(q\) when analyzing a CFG is join \((\sqcup)\), and the paths leading up to \(q\) are analyzed independently. For reasons discussed in section 2.3, PMAF is based on a backward analysis, so the confluence points represent the program’s branch points (i.e., for if-statements and while-loops). If the CFG is treated as a graph, join would be applied at each branch-node, and the subpaths from each successor would be analyzed independently. In contrast, when the CFG is treated as a hyper-graph, the operator applied at a probabilistic-choice node with probability \(p\) is \(\lambda a.\lambda b. a_p \oplus b\)—where \(p \oplus\) is not join, but an operator that weights the two successor paths by \(p\) and \(1 - p\). For instance, in Fig. 2(b), the hyper-edge \(\langle v_0, \{v_1, v_5\}\rangle\) generates the inequality \(\mathcal{A}[v_0] \supseteq \mathcal{A}[v_1]_{0.75} \oplus \mathcal{A}[v_5]\), for some analysis \(\mathcal{A}\). This approach allows the (hyper-)subpaths from the successors to be analyzed jointly.

To perform interprocedural analyses of probabilistic programs, we adopt a common practice from interprocedural analysis of standard non-probabilistic programs: the abstract domain is a **two-vocabulary domain** (each value represents an abstraction of a state transformer) rather than a **one-vocabulary domain** (each value represents an abstraction of a state). In the algebraic approach, an element in the algebra represents a two-vocabulary transformer. Elements can be “multiplied” by the algebra’s formal multiplication operator, which is typically interpreted as (an abstraction of) the reversal of transformer composition. The transformer obtained for the set of hyper-paths from the entry of procedure \(P\) to the exit of \(P\) is the summary for \(P\).
In the case of loops and recursive procedures, PMAF uses widening to ensure convergence. Here our approach is slightly non-standard: we found that for some instantiations of the framework, we could improve precision by using different widening operators for loops controlled by conditional, probabilistic, and nondeterministic branches.

The main advantage of PMAF is that instead of starting from scratch to create a new analysis, you only need to instantiate PMAF with the implementation of a new pre-Markov algebra. To establish soundness, you have to establish some well-defined algebraic properties, and can then rely on the soundness proof of the framework. To implement your analysis, you can rely on PMAF to perform sound interprocedural analysis, with respect to the abstraction that you provided. The PMAF implementation supplies common parts of different static analyses of probabilistic programs, e.g., efficient iteration strategies with widenings and interprocedural summarization. Moreover, any improvements made to the PMAF implementation immediately translate into improvements to all of its instantiations.

To evaluate PMAF, we created a prototype implementation, and reformulated two existing interprocedural probabilistic-program analyses—the Bayesian-inference algorithm proposed by Claret et al. [Claret et al. 2013], and Markov decision problem with rewards [Puterman 1994]—to fit into PMAF: Reformulation involved changing from the one-vocabulary abstract domains proposed in the original papers to appropriate two-vocabulary abstract domains. We also developed a new program analysis: linear expectation-invariant analysis (LEIA). Linear expectation-invariants are equalities involving expected values of linear expressions over program variables.

A related approach to static analysis of probabilistic programs is probabilistic abstract interpretation (PAI) [Cousot and Monerau 2012; Monniaux 2000, 2001, 2003], which lifts standard program analysis to the probabilistic setting. PAI is both general and elegant, but the more concrete approach developed in our work on PMAF has a couple of advantages. First, PMAF is algebraic and provides a simple and well-defined interface for implementing new abstractions. We provide an actual implementation of PMAF that can be easily instantiated to specific abstract domains. Second, PMAF is based on a different semantic foundation, which follows the standard interpretation of non-deterministic probabilistic programs in domain theory [den Hartog and de Vink 1999; Jones 1989; Jones and Plotkin 1989; Mislove 2000; Mislove et al. 2004; Tix et al. 2009].

The concrete semantics of PAI isolates probabilistic choices from the non-probabilistic part of the semantics by interpreting programs as distributions $P : \Omega \to (D \to D)$, where $\Omega$ is a probability space and $D \to D$ is the space of non-probabilistic transformers. As a result, the PAI interpretation of the following non-deterministic program is that with probability $\frac{1}{2}$, we have a program that non-deterministically returns 1 or 2; with probability $\frac{1}{4}$, we have a program that returns 1; and with probability $\frac{1}{4}$, a program that returns 2.

if ⋆ then if prob(\frac{1}{2}) then return 1 else return 2 else if prob(\frac{1}{2}) then return 1 else return 2 fi

In contrast, the semantics used in PMAF resolves non-determinism on the outside, and thus the semantics of the program is that it returns 1 with probability $\frac{1}{2}$ and 2 with $\frac{1}{2}$. As a result, one can conclude that the expected return value $r$ is 1.5. However, PAI—and every static analysis based on PAI—can only conclude $1.25 \leq r \leq 1.75$.

Contributions. Our work makes five main contributions:

- We present a new denotational semantics for probabilistic programs, which is capable of expressing several nontrivial features of probabilistic-programming languages.
- We develop PMAF, an algebraic framework for static analyses of probabilistic programs. PMAF provides a novel approach to analyzing probabilistic programs with non-deterministic choice.
\begin{align*}
b_1 & \sim \text{Bernoulli}(0.5); \\
b_2 & \sim \text{Bernoulli}(0.5); \\
\text{while } (\neg b_1 \land \neg b_2) \text{ do } & \\
b_1 & \sim \text{Bernoulli}(0.5); \\
b_2 & \sim \text{Bernoulli}(0.5) \\
\text{od}
\end{align*}

\begin{align*}
\text{while } \text{prob}(\frac{3}{4}) \text{ do } & \\
z & \sim \text{Uniform}(0, 2); \\
\text{if } \star \text{ then } x := x + z \\
\text{else } y := y + z \\
\text{fi} \\
\text{od}
\end{align*}

(a) Boolean probabilistic program; (b) Arithmetic probabilistic program

\section{Overview}

In this Section, we familiarize the reader with probabilistic programming, and briefly introduce two different static analyses of probabilistic programs: Bayesian inference and linear expectation-invariant analysis. We then informally explain the main ideas behind our algebraic framework for analyzing probabilistic programs and show how it generalizes the aforementioned analyses.

\subsection{Probabilistic Programming}

Probabilistic programs contain two sources of randomness: (i) \textit{data randomness}, i.e., the ability to draw random values from distributions, and (ii) \textit{control-flow randomness}, i.e., the ability to branch probabilistically. A variety of probabilistic programming languages and systems has been proposed [Carpenter et al. 2017; Goodman et al. 2008; Kok et al. 2007; Milch et al. 2005; Minka et al. 2014; Pfeffer 2005]. In this paper, our prototypical language is imperative.

We use the Boolean program in Fig. 1a to illustrate data randomness. In the program, \(b_1\) and \(b_2\) are two Boolean-valued variables. The \textit{sampling statement} \(x \sim \text{Dist}(\theta)\) draws a value from a distribution \(\text{Dist}\) with a vector of parameters \(\theta\), and assigns it to the variable \(x\), e.g., \(b_1 \sim \text{Bernoulli}(0.5)\) assigns to \(b_1\) a random value drawn from a Bernoulli distribution with mean 0.5. Intuitively, the program tosses two fair Boolean-valued coins repeatedly, until one coin is \textit{true}.

We introduce control-flow randomness through the arithmetic program in Fig. 1b. In the program, \(x\), \(y\), and \(z\) are real-valued variables. As in the previous example, we have sampling statements, and \(\text{Uniform}(l, r)\) represents a uniform distribution on the interval \((l, r)\). The \textit{probabilistic choice} \(\text{prob}(p)\) returns true with probability \(p\) and false with probability \(1 - p\). Moreover, the program also exhibits \textit{nondeterminism}, as the symbol \(\star\) stands for a \textit{nondeterministic choice} that can behave like standard non-determinism, as well as an arbitrary probabilistic choice [McIver and Morgan 2005, \S6.6]. Intuitively, the program describes two players \(x\) and \(y\) playing a round-based game that ends with probability
2 OVERVIEW

Bayesian inference (BI). Probabilistic programs can be seen as descriptions of probability distributions [Carpenter et al. 2017; Goodman et al. 2008; Minka et al. 2014]. For a Boolean probabilistic program, such as the one in Fig. 1a, Bayesian-inference analysis [Claret et al. 2013] calculates the distribution over variable valuations at the end of the program, conditioned on the program terminating. The inferred probability distribution is called the posterior probability distribution. The program in Fig. 1a specifies the posterior distribution over the variables \( b_1, b_2 \) given by: \( P[b_1 = \text{false}, b_2 = \text{false}] = 0 \), and \( P[b_1 = \text{false}, b_2 = \text{true}] = P[b_1 = \text{true}, b_2 = \text{false}] = P[b_1 = \text{true}, b_2 = \text{true}] = \frac{1}{2} \). This distribution also indicates that the program terminates almost surely, i.e., the probability that the program terminates is 1.\(^1\)

Linear expectation invariant analysis (LEIA). Loop invariants are crucial to verification of imperative programs [Dijkstra 1997; Floyd 1967; Hoare 1969]. Although loop invariants for traditional programs are usually Boolean-valued expressions over program variables, real-valued invariants are needed to prove the correctness of probabilistic loops [Kozen 1981; McIver and Morgan 2005]. Such expectation invariants are usually defined as random variables—specified as expressions over program variables—with some desirable properties [Chakarov and Sankaranarayanan 2013, 2014; Katoen et al. 2010]. In this paper, we work with a more general kind of expectation invariant, defined as follows:

Definition 2.1. For a program \( P \), \( E[\mathcal{E}_2] \gg \mathcal{E}_1 \) is called an expectation invariant if \( \mathcal{E}_1 \) and \( \mathcal{E}_2 \) are real-valued expressions over \( P \)'s program variables, \( \gg \) is one of \( \{=,<,>,\leq,\geq\} \), and the following property holds: For any initial valuation of the program variables, the expected value of \( \mathcal{E}_2 \) in the final valuation (i.e., after the execution of \( P \)) is related to the value of \( \mathcal{E}_1 \) in the initial valuation by \( \gg \).

We typically use variables with primes in \( \mathcal{E}_2 \) to denote the values in the final valuation. For example, for the program in Fig. 1b, \( E[x' + y'] = x + y + 3 \), \( E[z'] = \frac{1}{4}z + \frac{3}{2} \), \( E[x'] \leq x + 3 \), \( E[x'] \geq x \), \( E[y'] \leq y + 3 \), and \( E[y'] \geq y \) are several linear expectation invariants, and our analysis can derive all of these automatically! The expectation invariant \( E[x' + y'] = x + y + 3 \) indicates that the expected value of the total reward that the two players would gain is exactly 3.

2.3 The Algebraic Framework

This section explains the main ideas behind PMAF, which is general enough to encode the two analyses from section 2.2.

\(^1\) In general, we work with with subprobability distributions, where the probabilities add up to strictly less than 1. In the case of a program that diverges with probability \( p > 0 \), the posterior distribution is a subprobability distribution in which the probabilities of the states sum up to \( 1 - p \).
Data Randomness vs. Control-Flow Randomness. Our first principle is to make an explicit separation between data randomness and control-flow randomness. This distinction is intended to make the framework more flexible for analysis designers by providing multiple ways to translate the constructs of their specific probabilistic programming language into the constructs of PMAF. Analysis designers may find it useful to use the control-flow-randomness construct directly (e.g., “if prob(0.3) . . .”), rather than simulating control-flow randomness by data randomness (e.g., “p ~ Uniform(0, 1); if (p < 0.3) . . .”). For program analysis, such a simulation can lead to suboptimal results if the constructs used in the simulation require properties to be tracked that are outside the class of properties that a particular analysis’s abstract domain is capable of tracking. For example, if an analysis domain only keeps track of expectations, then analysis of “p ~ Uniform(0,1)” only indicates that E[p] = 0.5, which does not provide enough information to establish that P[p < 0.3] = 0.3 in the then-branch of “if (p < 0.3) . . .”. In contrast, when “prob(0.3) . . .” is analyzed in the fragment with the explicit control-flow-randomness construct (“if prob(0.3) . . .”) the analyzer can directly assign the probabilities 0.3 and 0.7 to the outgoing branches, and use those probabilities to compute appropriate expectations in the respective branches.

We achieve the separation between data randomness and control-flow randomness by capturing the different types of randomness in the graphs that we use for representing programs. In contrast to traditional program analyses, which usually work on control-flow graphs (CFGs), we use control-flow hyper-graphs to model probabilistic programs. Hyper-graphs are directed graphs, each edge of which (i) has one source and possibly multiple destinations, and (ii) has an associated control-flow action (e.g., sequencing, conditional-choice, probabilistic-choice, or nondeterministic-choice). A traditional CFG represents a collection of execution paths, while in probabilistic programs, paths are no longer independent, and the program specifies probability distributions over the paths. It is natural to treat a collection of paths as a whole and define distributions over the collections. These kinds of collections can be precisely formalized as hyper-paths made up of hyper-edges in hyper-graphs.

Fig. 2 shows the control-flow hyper-graphs of the two programs in Fig. 1. Every edge has an associated action, e.g., the control-flow actions cond(¬b1 ∧ ¬b2), prob(b1/3), and ndet are conditional-choice, probabilistic-choice, and nondeterministic-choice actions. Data actions, like x := x + z and b1 ∼ Bernoulli(0.5), also perform a trivial control-flow action to transfer control to their one destination node.

Just as the control-flow graph of a procedure typically has a single entry node and a single exit node, a procedure’s control-flow hyper-graph also has a single entry node and a single exit node. In Fig. 2a, the entry and exit nodes are v0 and v3, respectively; in Fig. 2b, the entry and exit nodes are v0 and v5, respectively.

Backward Analysis. Traditional static analyses assign to a CFG node v either backward assertions—about the computations that can lead up to v—or forward assertions—about the computations that can continue from v [Cousot and Cousot 1977, 1979]. Backward assertions are computed via a forward analysis (in the same direction as CFG edges); forward assertions are computed via a backward analysis (counter to the flow of CFG edges).

Because we work with hyper-graphs rather than CFGs, from the perspective of a node v, there is a difference in how things “look” in the backward and forward direction: hyper-edges fan out in the forward direction. Hyper-edges can have two destination nodes, but only one source node.

The second principle of the framework is essentially dictated by this structural asymmetry: the framework supports backward analyses that compute a particular kind of forward assertion. In particular, the property to be computed for a node v in the control-flow hyper-graph for procedure P is (an abstraction of) a transformer that summarizes the transformation carried out by the hyper-graph fragment that extends from v to the exit node of P. It is possible to reason in the forward direction—i.e., about computations that lead up to v—but one would have to “break” hyper-paths into paths and
"relocate" probabilities, which is more complicated than reasoning in the backward direction. The framework interprets an edge as a property transformer that computes properties of the edge’s source node as a function of properties of the edge’s destination node(s) and the edge’s associated action. These property transformers propagate information in a hypergraph-leaf-to-hypergraph-root manner, which is natural in hyper-graph problems. For example, standard formulations of interprocedural dataflow analysis [Knoop and Steffen 1992; Lal et al. 2005; Müller-Olm and Seidl 2004; Sharir and Pnueli 1981] can be viewed as hyper-graph analyses, and propagation is performed in the leaf-to-root direction there as well.

Recall the Boolean program in Fig. 1a. Suppose that we want to perform BI to analyze \( P[b_1 = \text{true}, b_2 = \text{true}] \) in the posterior distribution. The property to be computed for a node will be a mapping from variable valuations to probabilities, where the probability reflects the chance that a given state will cause the program to terminate in the post-state \((b_1 = \text{true}, b_2 = \text{true})\). For example, the property that we would hope to compute for node \( v_1 \) is the function \( \lambda(b_1, b_2) \cdot [b_1 \wedge b_2] + [\neg b_1 \wedge \neg b_2] \cdot \frac{1}{2} \), where \([\varphi]\) is an Iverson bracket, which evaluates to 1 if \( \varphi \) is true, and 0 otherwise.

**Two-Vocabulary Program Properties.** In the example of BI above, we observe that the property transformation discussed above is not suitable for interprocedural analysis. Suppose that (i) we want analysis results to tell us something about \( P[b_1 = \text{true}, b_2 = \text{true}] \) in the posterior distribution of the main procedure, but (ii) to obtain the answer, the analysis must also analyze a call to some other procedure \( Q \). In the procedure main, the analysis is driven by the posterior-probability query \( P[b_1 = \text{true}, b_2 = \text{true}] \); in general, however, \( Q \) will need to be analyzed with respect to some other posterior probability (obtained from the distribution of valuations at the point in main just after the call to \( Q \)). One might try to solve this issue by analyzing each procedure multiple times with different posterior probabilities. However, in an infinite state space, this approach is no longer feasible.

Following common practice in interprocedural static analysis of traditional programs, the third principle of the framework is to work with two-vocabulary program properties. The property sketched in the BI example above is actually one-vocabulary, i.e., the property assigned to a control-flow node only involves the state at that node. In contrast, a two-vocabulary property at node \( v \) (in the control-flow hyper-graph for procedure \( P \)) should describe the state transformation carried out by the hyper-graph fragment that extends from \( v \) to the exit node of \( P \).

For instance, LEIA assigns to each control-flow node a conjunction of expectation invariants, which relate the state at the node to the state at the exit node; consequently, LEIA deals with two-vocabulary properties. In section 5, we show that we can reformulate BI to manipulate two-vocabulary properties. As in interprocedural dataflow analysis [Cousot and Cousot 1978; Sharir and Pnueli 1981], procedure summaries are used to interpret procedure calls.

**Separation of Concerns.** Our fourth principle—which is common to most analysis frameworks—is separation of concerns, by which we mean

| Provide a declarative interface for a client to specify the program properties to be tracked by a desired analysis, but leave it to the framework to furnish the analysis implementation by which the analysis is carried out. |

We achieve this goal by adopting (and adapting) ideas from previous work on algebraic program analysis [Farzan and Kincaid 2015; Ramalingam 1996; Tarjan 1981]. Algebraic program analysis is based on the following idea:

Any static analysis method performs reasoning in some space of program properties and property transformers; such property transformers should obey algebraic laws.

For instance, the data action **skip**, which does nothing, can be interpreted as the identity element in an algebra of program-property transformers.
Concretely, our fourth principle has three aspects:

1. For our intended domain of probabilistic programs, identify an appropriate set of algebraic laws that hold for useful sets of property transformers.

2. Define a specific algebra \( A \) for a program-analysis problem by defining a specific set of property transformers that obey the laws identified in item 1. Give translations from data actions and control-flow actions to such property transformers. (When such a translation is applied to a specific program, it sets up an equation system to be solved over \( A \).)

3. Develop a generic analysis algorithm that solves an equation system over any algebra that satisfies the laws identified in item 1.

Items 1 and 3 are tasks for us, the framework designers; they are the subjects of §3 and §4. Item 2 is a task for a client of the framework: examples are given in section 5.

A client of the framework must furnish an interpretation—which consists of a semantic algebra and a semantic function—and a program. The semantic algebra consists of a universe, which defines the space of possible program-property transformers, and sequencing, conditional-choice, probabilistic-choice, and nondeterministic-choice operators, corresponding to control-flow actions. The semantic function is a mapping from data actions to the universe. (An interpretation is also called a domain.)

To address Item 3, our prototype implementation follows the standard iterative paradigm of static analysis [Cousot and Cousot 1977; Kildall 1973]: We first transform the control-flow hyper-graph into a system of inequalities, and then use a chaotic-iteration algorithm to compute a solution to it (e.g., [Bourdoncle 1993]), which repeatedly applies the interpretation until a fixed point is reached (possibly using widening to ensure convergence). For example, the control-flow hyper-graph in Fig. 2b can be transformed into the system shown in Fig. 3, where \( S(v) \in M \) are elements in the semantic algebra; \( \sqsubseteq \) is the approximation order on \( M \); \( \llbracket \cdot \rrbracket \) is the semantic function, which maps data actions to \( M \); and \( 1 \) is the transformer associated with the exit node.

The soundness of the analysis (with respect to a concrete semantics) is proved by (i) establishing an approximation relation between the concrete domain and the abstract domain; (ii) showing that the abstract semantic function approximates the concrete one; and (iii) showing that the abstract operators (sequencing, conditional-choice, probabilistic-choice, and nondeterministic-choice) approximate the concrete ones.

For BI, we instantiate our framework to give lower bounds on posterior distributions, using with an interpretation in which state transformers are probability matrices (see section 5.1). For LEIA, we design an interpretation using a Cartesian product of polyhedra (see section 5.3). Once the functions of the interpretations are implemented, and a program is translated into the appropriate hyper-graph, the framework handles the rest of the work, namely, solving the equation system.

### 3 Probabilistic Programs

In this Section, we first review the concepts of hyper-graphs [Gallo et al. 1993] and introduce a probabilistic-program model based on them. Then we briefly sketch a new denotational semantics for our hyper-graph based imperative program model.
3.1 A Hyper-Graph Model of Probabilistic Programs

Definition 3.1 (Hyper-graphs). A hyper-graph $H$ is a quadruple $\langle V, E, \nu_{\text{entry}}, \nu_{\text{exit}} \rangle$, where $V$ is a finite set of nodes, $E$ is a set of hyper-edges, $\nu_{\text{entry}} \in V$ is a distinguished entry node, and $\nu_{\text{exit}} \in V$ is a distinguished exit node. A hyper-edge is an ordered pair $(x, Y)$, where $x \in V$ is a node and $Y \subseteq V$ is an ordered, non-empty set of nodes. For a hyper-edge $e = (x, Y)$ in $E$, we use $\text{src}(e)$ to denote $x$ and $\text{Dst}(e)$ to denote $Y$. Following the terminology from graphs, we say that $e$ is an outgoing edge of $x$ and an incoming edge of each of the nodes $y \in Y$. We assume that $\nu_{\text{entry}}$ has no incoming edges, and $\nu_{\text{exit}}$ has no outgoing edges.

Definition 3.2 (Probabilistic programs). A probabilistic program contains a finite set of procedures $\{H_i\}_{1 \leq i \leq n}$, where each procedure $H_i = \langle V_i, E_i, \nu_{\text{entry}}^i, \nu_{\text{exit}}^i \rangle$ is a control-flow hyper-graph in which each node except $\nu_{\text{exit}}^i$ has exactly one outgoing hyper-edge. We assume that the nodes of each procedure are pairwise disjoint. To assign meanings to probabilistic programs modulo data actions $A$ and logical conditions $L$, we associate with each hyper-edge $e \in E = \bigcup_{1 \leq i \leq n} E_i$ a control-flow action $\text{Ctrl}(e)$, where $\text{Ctrl}$ is

$$
\text{Ctrl} := \text{seq}[\text{act}] \text{ where } \text{act} \in A | \text{call}[i] \text{ where } 1 \leq i \leq n \\
| \text{cond}[\varphi] \text{ where } \varphi \in L | \text{prob}[p] \text{ where } 0 \leq p \leq 1 \\
| \text{ndet}
$$

where the number of destination nodes $|\text{Dst}(e)|$ of a hyper-edge $e$ is 1 if $\text{Ctrl}(e)$ is $\text{seq}[\text{act}]$ or $\text{call}[i]$, and 2 otherwise.

Fig. 2 shows two examples of hyper-graph–based probabilistic programs. See Fig. 4 for data actions $A$ and logical conditions $L$ that would be used for an arithmetic program like the one shown in Fig. 1b.

3.2 Background from Measure Theory

To define denotational semantics for probabilistic programs modulo data actions $A$ and logical conditions $L$, we review some standard definitions from measure theory [Billingsley 2012; Panangaden 1999].

A measurable space is a pair $\langle X, \Sigma \rangle$ where $X$ is a non-empty set called the sample space, and $\Sigma$ is a $\sigma$-algebra over $X$ (i.e., a set of subsets of $X$ which contains $\emptyset$ and is closed under complement and countable union). A measurable function from a measurable space $\langle X_1, \Sigma_1 \rangle$ to another measurable space $\langle X_2, \Sigma_2 \rangle$ is a mapping $f : X_1 \rightarrow X_2$ such that for all $A \in \Sigma_2$, $f^{-1}(A) \in \Sigma_1$. The measurable functions from a measurable space $\langle X, \Sigma \rangle$ to the Borel space $\mathcal{B}(\mathbb{R}_{\geq 0})$ on nonnegative real numbers (the smallest $\sigma$-algebra containing all open intervals) is called $\Sigma$-measurable.

A measure $\mu$ on a measurable space $\langle X, \Sigma \rangle$ is a function from $\Sigma$ to $[0, \infty]$ such that: (i) $\mu(\emptyset) = 0$, and (ii) for all pairwise-disjoint countable sequences of sets $A_1, A_2, \ldots \in \Sigma$ (i.e., $A_i \cap A_j = \emptyset$ for all $i \neq j$) we have $\sum_{i=1}^{\infty} \mu(A_i) = \mu(\bigcup_{i=1}^{\infty} A_i)$. The measure $\mu$ is called a (sub-probability) distribution if $\mu(X) \leq 1$. A measure space is a triple $\mathcal{M} = \langle X, \Sigma, \mu \rangle$ where $\mu$ is a measure on the measurable space $\langle X, \Sigma \rangle$. The
The next step is to define semantics based on the control-flow hyper-graphs. We use a denotational semantics, as described by Jones [1989; Jones and Plotkin 1989; Mislove 2000; Mislove et al. 2004; Tix et al. 2009]. This semantics is based on conditional transformers over program states. When there is no nondeterminism, we can assign a kernel to every state that satisfies the condition.

A kernel is a sub-probability function that describes the probability of an action leading to a specific outcome. Kernels are indeed two-vocabulary specifications, whereas distributions can be seen as one-vocabulary specifications. While distributions are used to describe the probability of an event occurring in a specific state, kernels are used to describe the probability of transitioning from one state to another.

### 3.3 A Denotational Semantics

The next step is to define semantics based on the control-flow hyper-graphs. We use a denotational approach because it abstracts away how a program is evaluated and concentrates only on the effect of the program. This property makes it suitable as a starting point for static analysis, which is aimed at reasoning about program properties.

We develop a new semantics for probabilistic programming by combining Borgström et al.’s distribution-based semantics using the concept of kernels from measure theory [Borgström et al. 2016] and existing results on domain-theoretic probabilistic nondeterminism [den Hartog and de Vink 1999; Jones 1989; Jones and Plotkin 1989; Mislove 2000; Mislove et al. 2004; Tix et al. 2009]. This semantics can describe several nontrivial constructs, including continuous sampling, nondeterministic choice, and recursion.

Three components are used to define the semantics:

- A measurable space $P = (Ω, F)$ over program states (e.g., finite mappings from program variables to values).
- A mapping from data act actions to kernels $\widehat{act} : Ω × F → R$. The intuition to keep in mind is that $\widehat{act}(ω, F)$ is the probability that the action, starting in state $ω ∈ Ω$, halts in a state that satisfies $F ∈ F$ [Kozen 1985].
- A mapping from logical conditions $φ$ to measurable functions $\widehat{φ} : Ω → \{true, false\}$.

**Example 3.3.** For an arithmetic program with a finite set $Var$ of program variables, $Ω$ is defined as $Var → R$ and $P$ as the Borel space on $Ω$. Fig. 5 shows the interpretation of data actions and logical conditions in Fig. 4, where $e(ω)$ evaluates expression $e$ in state $ω$, $(x → v)ω$ updates $x$ in $ω$ with $v$, and $μ_P : B(R) → [0, 1]$ is the measure corresponding to the distribution $P$ on reals. Note that the action $observe(φ)$ performs conditioning on states that satisfy $φ$.

While distributions can be seen as one-vocabulary specifications, kernels are indeed two-vocabulary transformers over program states. When there is no nondeterminism, we can assign a kernel to every state.

---

$\overline{x} := e = \lambda(ω, F).[(x → e(ω))ω ∈ F] \quad true = \lambda ω.true$

$\overline{x} ∼ ∼ P = \lambda(ω, F).μ_P((v | (x → v)ω ∈ F)) \quad false = \lambda ω.false$

$observe(φ) = \lambda(ω, F).\overline{φ}(ω) · [ω ∈ F] \quad \overline{e} ∼ u = \lambda ω.[e(ω) ∼ u(ω)]$

$\overline{φ} = \lambda ω.¬\overline{φ}(ω)$

Fig. 5: Interpretation of actions and conditions
control-flow node. We can also define control-flow actions on kernels. A sequence of actions act\_1; act\_2 with kernels κ\_1 and κ\_2, respectively, is modeled by their composition, denoted by κ\_1 ⊗ κ\_2, which yields a new kernel defined as follows:

\[ \kappa_1 \otimes \kappa_2 \overset{\text{def}}{=} \lambda(x, A). \int \kappa_1(x, dy) \kappa_2(y, A). \]  

(1)

The conditional-choice κ\_1 ϕ ⊙ κ\_2 is defined as a new kernel \( \lambda(x, A).[\bar{\varphi}(x)] \cdot \kappa_1(x, A) + [-\varphi(x)] \cdot \kappa_2(x, A) \).

The probabilistic-choice κ\_1 p ⊕ κ\_2 is defined as a new kernel \( \lambda(x, A).p \cdot \kappa_1(x, A) + (1 - p) \cdot \kappa_2(x, A) \).

**Example 3.4.** Consider the following program that models a variation on a geometric distribution.

\begin{verbatim}
 n := 0;
 while prob(0.9) do
    n := n + 1;
    if n \geq 10 then break else continue fi
 od
\end{verbatim}

Fig. 6 shows its control-flow hyper-graph. The assignment \( n := n + 1 \) is interpreted as a kernel \( n := n + 1 = \lambda(\omega, F).((n \mapsto \omega(n) + 1) \omega \in F) \). The comparison \( n \geq 10 \) is interpreted as a measurable function \( n \geq 10 = \lambda\omega.((n \geq 10) \omega \in F) \).

Let \( K \) stand for 0.3486784401; the semantics assigned to node \( v_0 \) is

\[ \lambda(\omega, F). \sum_{k=0}^{9} (0.1 \times 0.9^k) \cdot [(n \mapsto k)\omega \in F] + K \cdot [(n \mapsto 10)\omega \in F]. \]

When nondeterminism comes into the picture, we need to associate each control-flow node with a collection of kernels. In other words, we need to consider powerdomains [Gunter et al. 1989] of kernels. We adopt Tix et al.’s constructions of probabilistic powerdomains [Tix et al. 2009], and extend them to work on kernels instead of distributions. We denote the set of feasible collections of kernels by \( P\Omega \), and the composition, conditional-choice, probabilistic-choice, and nondeterministic-choice operators on that by \( \otimes, \varphi \circ, p \oplus \), and \( \varpi \). \( P\Omega \) is also equipped with a partial order \( \subseteq \).

We reformulated distributions and kernels in a domain-theoretic way to adopt existing studies on powerdomains. We discuss the details of the construction of \( P\Omega \) in a companion paper [Wang et al. 2018]; the focus of this paper is static analysis and we will keep the domain-theoretic terminology to a minimum.

We adopted Hoare powerdomains and Smyth powerdomains [Abramsky and Jung 1994, §6.2] over kernels. Kernels are ordered pointwise, i.e., \( \kappa_1 \leq \kappa_2 \) if and only if for all \( \omega \) and \( F \), \( \kappa_1(\omega, F) \leq \kappa_2(\omega, F) \). The zero kernel \( \lambda(\omega, F).0 \) is the bottom element of this order. Intuitively, the Hoare powerdomain is a new kernel defined as follows:

\[ \kappa_1 \otimes \kappa_2 \overset{\text{def}}{=} \lambda(x, A). \int \kappa_1(x, dy) \kappa_2(y, A). \]

For finite or countable \( \Omega \), and the matrix representation described in footnote 2, the integral in (1) degenerates to matrix multiplication [Kozen 1985].
kernel), terminating and nonterminating executions cannot be distinguished. The Smyth power-domain is used for total correctness: the order is reverse inclusion on the upper closures of the elements—nontermination is interpreted as the worst output, and the kernel that represents non-termination does not occur in an upward-closed set that represents the semantics of a terminating computation.

Given a probabilistic program \( P = \{ H_i \}_{1 \leq i \leq n} \), where \( H_i = (V_i, E_i, v_i^{\text{entry}}, v_i^{\text{exit}}) \), we want to define the semantics of each node \( v \) as a set of kernels that represent the effects from \( v \) to the exit node of the procedure that contains \( v \). Let \( S(v) \in \mathbb{P}^\Omega \) be the semantics assigned to the node \( v \); the following local properties should hold:

- if \( e = (v, \{ u_1, \ldots , u_k \}) \in E \), \( S(v) = \text{Ctrl}(e)(S(u_1), \ldots , S(u_k)) \), and
- otherwise, \( S(v) = 1 \).

The function \( \text{act} \) for the different kinds of control-flow actions is defined as follows:

\[
\begin{align*}
\text{seq}(\text{act})(S_1) & \triangleq (\text{act}) \otimes S_1 \\
\text{call}(i)(S_1) & \triangleq S(v_i^{\text{entry}}) \otimes S_1 \\
\text{prob}(p)(S_1, S_2) & \triangleq S_1 \circ p \oplus S_2 \\
\text{nondet}(S_1, S_2) & \triangleq S_1 \uparrow S_2
\end{align*}
\]

**Lemma 3.5.** The function \( F_P \) defined as

\[
\lambda S, \lambda v. \left\{ \begin{array}{ll}
\text{Ctrl}(e)(S(u_1), \ldots , S(u_k)) & e = (v, \{ u_1, \ldots , u_k \}) \in E \\
1_P & \text{otherwise}
\end{array} \right.
\]

is \( \omega \)-continuous on \( \langle V \rightarrow \mathbb{P}^\Omega, \sqsubseteq \rangle \), which is an \( \omega \)-cpo with the least element \( \lambda v. \bot \).

A dot over an operator denotes its application pointwise. By Kleene’s fixed-point theorem, we have

**Theorem 3.6.** \( \lambda v. \bot ) F_P \) exists for all prob. programs \( P \).

Thus, the semantics of a node \( v \) is defined as \( (\lambda v. \bot ) F_P(v) \).

### 4 Analysis Framework

To aid in creating abstractions of probabilistic programs, we first identify, in section 4.1, some algebraic properties that underlie the mechanisms used in the semantics from section 3.3. This algebra will aid our later definitions of abstractions in section 4.2. We then discuss interprocedural analysis (in section 4.3) and widening (section 4.4).

#### 4.1 An Algebraic Characterization of Fixpoint Semantics

In the denotational semantics, the concrete semantics is obtained by composing Ctrl(\( e \)) operations along hyper-paths. Hence in the algebraic framework, the semantics of probabilistic programs is denoted by an interpretation, which consists of two parts: (i) a semantic algebra, which defines a set of possible program meanings, and which is equipped with sequencing, conditional-choice, probabilistic-choice, and nondeterministic-choice operators to compose these meanings, and (ii) a semantic function, which assigns a meaning to each basic program action.

The semantic algebras that we use—and the lattices used for abstract interpretation—are pre-Markov algebras:
Definition 4.1 (Pre-ω-continuous functions). A function $f : X \to Y$ between two ω-cpos $X$ and $Y$ is pre-ω-continuous if it is monotone, and for every ω-chain $C \subseteq X$, $f(\text{sup}(C)) \leq \text{sup}(f(C))$.

Definition 4.2 (Pre-Markov algebras). A pre-Markov algebra (PMA) over a set of logical conditions $L$ is an 8-tuple $M = (\{M, \sqcap, \sqcup, \varphi \},_p \otimes, _p \odot, _p \uparrow, _p \downarrow, 1)$, where $(M, \sqcap, 1)$ forms an ω-cpo with a least element $\bot$; $(M, \otimes, 1)$ forms a monoid (i.e., $\otimes$ is an associative binary operator with 1 as its identity element); $\varphi$ is a binary operator parametrized by $\varphi$ which is a function in $L$; $p \otimes$ is a binary operator parametrized by $p \in [0, 1]$; $\odot$ is a binary operator that is idempotent, commutative, and associative; $\otimes, p \odot, \varphi \odot$, and $\odot$ are pre-ω-continuous; and the following properties hold:

- $\varphi(a \otimes b) \sqsubseteq a \odot b$, $a \sqsubseteq a \varphi \odot b$, $a \varphi \odot b = b = \neg\varphi \odot a$
- $a \varphi \odot b \sqsubseteq a \otimes b$, $a \sqsubseteq a \varphi \odot a$, $a \varphi \odot a = a \sqsubseteq b$, $a \varphi \odot a = b \sqsubseteq a \odot a$
- $a \varphi \odot (b \psi \odot c) = (a \varphi \odot b) \psi \odot c$ where $\varphi = \varphi' \land \psi', \varphi \lor \psi = \psi'$
- $a \varphi \odot (b \psi \odot c) = (a \p \odot b) \psi \odot c$ where $p = p' \lor \psi \land \psi = \psi'$

The precedence of the operators is that $\otimes$ binds tightest, followed by $\odot$, $p \odot$, and $\varphi$.

Remark 4.3. These algebraic laws are not needed to prove soundness of the framework (stated in Thm. 4.8). These laws helped us when designing the abstract domains. Exploiting these algebraic laws to design better algorithms is an interesting direction for future work.

Lemma 4.4. The denotational semantics in section 3.3 is a PMA $C = (\{\Omega, \sqsubseteq, \varphi \otimes, \varphi \odot, \psi \odot, \odot, 1\})$ (which we call the concrete domain for our framework).

As is standard in abstract interpretation, the order on the algebra should represent an approximation order: $a \sqsubseteq b$ iff $a$ is approximated by $b$ (i.e., if $a$ represents a more precise property than $b$).

Definition 4.5 (Interpretations). An interpretation is a pair $\mathcal{I} = (M, [\cdot])$, where $M$ is a pre-Markov algebra, and $[\cdot] : A \to M$, where $A$ is the set of data actions for probabilistic programs. We call $M$ the semantic algebra of the interpretation and $[\cdot]$ the semantic function.

Given a probabilistic program $P$ and an interpretation $\mathcal{I} = (M, [\cdot])$, we define $\mathcal{I}[P]$ to be the interpretation of the probabilistic program. $\mathcal{I}[P]$ is then defined as the least prefixed point (i.e., the least $\rho$ such that $f(\rho) \leq \rho$ for a function $f$) of the function $F^p_\mathcal{I}$, which is defined as

$$\lambda S^4, \lambda \nu \cdot \begin{cases} \text{Ctrl}(e) \overset{\mathcal{I}}{=} (S^4(u_1), \ldots, S^4(u_k)) & e = \langle v, \{u_1, \ldots, u_k\} \rangle \in E \\ \text{otherwise} \end{cases}$$

where

$$\begin{align*} \text{seq}^\mathcal{I}(a_1) &= [\text{act}] \otimes a_1 \\ \text{call}^\mathcal{I}(a_1) &= S^4(\text{entry}) \otimes a_1 \\ \text{cond}^\mathcal{I}(a_1, a_2) &= a_1 \varphi \odot a_2 \\ \text{probdet}^\mathcal{I}(a_1, a_2) &= a_1 p \odot a_2 \\ \text{ndet}^\mathcal{I}(a_1, a_2) &= a_1 \psi \odot a_2 \end{align*}$$

We generalize Kleene’s fixed-point theorem to prove the existence of the least prefixed point of $F^p_\mathcal{I}$.

Theorem 4.6 (Generalized Kleene’s fixed point theorem). Suppose $(X, \leq)$ is an ω-cpo with a least element $\bot$, and let $f : X \to X$ be a pre-ω-continuous function. Then $f$ has a least prefixed point, which is the supremum of the ascending Kleene chain of $f$, denoted by $\text{lpp}^{\mathcal{I}}_\bot f$.

We use the least prefixed point of $F^p_\mathcal{I}$ to define the interpretation of a probabilistic program $P$ as $\mathcal{I}[P] = \text{lpp}^{\mathcal{I}}_\bot F^p_\mathcal{I}$. The interpretation of a control-flow node $v$ is then defined as $\mathcal{I}[v] = \mathcal{I}[P](v)$. 

4.2 Abstractions of Probabilistic Programs

Given two PMAs $C$ and $A$, a probabilistic abstraction is defined as follows:

Definition 4.7 (Probabilistic abstractions). A probabilistic over-abstraction (or under-abstraction, resp.) from a PMA $C$ to a PMA $A$ is a concretization mapping, $\gamma : A \rightarrow C$, such that

- $\gamma$ is monotone, i.e., for all $Q_1, Q_2 \in A$, $Q_1 \subseteq_A Q_2$ implies that $\gamma(Q_1) \subseteq_e \gamma(Q_2)$.
- $\perp_e \subseteq_e \gamma(\perp_A)$ (or $\gamma(\perp_A) \subseteq_e \perp_e$, resp.),
- $\perp_e \subseteq_e \gamma(\perp_A)$ (or $\gamma(\perp_A) \subseteq_e \perp_e$, resp.),
- for all $Q_1, Q_2 \in A$, $\gamma(Q_1) \otimes_{e} \gamma(Q_2) \subseteq_e \gamma(Q_1 \otimes_A Q_2)$ (or $\gamma(Q_1 \otimes A Q_2) \subseteq_e \gamma(Q_1) \otimes_{e} \gamma(Q_2)$, resp.),
- for all $Q_1, Q_2 \in A$, $\gamma(Q_1) \phi \otimes_{e} \gamma(Q_2) \subseteq_e \gamma(Q_1 \phi \otimes A Q_2)$ (or $\gamma(Q_1 \phi \otimes A Q_2) \subseteq_e \gamma(Q_1) \phi \otimes_{e} \gamma(Q_2)$, resp.),
- for all $Q_1, Q_2 \in A$, $\gamma(Q_1) \rho \otimes_{e} \gamma(Q_2) \subseteq_e \gamma(Q_1 \rho \otimes A Q_2)$ (or $\gamma(Q_1 \rho \otimes A Q_2) \subseteq_e \gamma(Q_1) \rho \otimes_{e} \gamma(Q_2)$, resp.),
- for all $Q_1, Q_2 \in A$, $\gamma(Q_1) \rho \otimes_{e} \gamma(Q_2) \subseteq_e \gamma(Q_1 \rho \otimes A Q_2)$ (or $\gamma(Q_1 \rho \otimes A Q_2) \subseteq_e \gamma(Q_1) \rho \otimes_{e} \gamma(Q_2)$, resp.).

A probabilistic abstraction leads to a sound analyses:

Theorem 4.8. Let $C$ and $A$ be interpretations over PMAs $C$ and $A$; let $\gamma$ be a probabilistic over-abstraction (or under-abstraction, resp.) from $C$ to $A$; and let $P$ be an arbitrary probabilistic program. If for all basic actions $act$, $[act]^{C} \subseteq_e \gamma([act]^{A})$ (or $[act]^{A} \subseteq_e \gamma([act]^{C})$, resp.), then we have $C[P] \subseteq_e \gamma(A[P])$ (or $A[P] \subseteq_e \gamma(C[P])$, resp.).

Proof. We only show the proof for the over-approximations. By definition, $C[P] = \text{Ipp}_{\lambda v \perp_e}^{C} F^C_{P}$ and $A[P] = \text{Ipp}_{\lambda v \perp_A}^{A} F^A_{P}$. We want to show that for all $n$ we have $([F^C_{P}]^{n})^{\perp_e} \subseteq_e \gamma(([F^A_{P}]^{n})^{\perp_A})$. Let’s prove by induction on $n$. The base case follows directly from the fact that $\perp_e \subseteq_e \gamma(\perp_A)$. Suppose we know $([F^A_{P}]^{n})^{\perp_A} \subseteq_e \gamma(([F^A_{P}]^{n})^{\perp_A})$ for some $n$. Let’s denote the left hand side by LHS and the right hand side by $\hat{\gamma}$(RHS). Then for all $v$ we have $\text{LHS}(v) \subseteq_e \gamma(\text{RHS}(v))$. Let $\text{LHS}'(v) \subseteq \gamma(\text{RHS}(v))$. Then $v \in \text{LHS}'(v) \subseteq_e \gamma(\text{RHS}(v))$.

- If $v$ isn’t associated with any edges, then $\text{LHS}'(v) = 1_e$ and $\text{RHS}'(v) = 1_A$ and because of $1_e \subseteq_e \gamma(1_A)$, we know that $\text{LHS}'(v) \subseteq_e \gamma(\text{RHS}(v))$.

- If $v$ is associated with $e = \langle i_1, \ldots, i_k \rangle$, then
  - If $\text{Act}(e) = \text{seq}[act]$, then $\text{LHS}'(v) = \gamma([act]^{C} \otimes_{e} \text{LHS}(u_1))$ and $\text{RHS}'(v) = \gamma([act]^{A} \otimes_{e} \text{RHS}(u_1))$.
    - Then $\gamma(\text{RHS}(v)) = \gamma([act]^{C} \otimes_{A} \text{RHS}(u_1)) \subseteq_e \gamma([act]^{C} \otimes_{e} \text{RHS}(u_1)) \subseteq_e \gamma([act]^{A} \otimes_{e} \text{LHS}(u_1)) = \text{LHS}'(v)$.
    - The two inequalities come from the definition of probabilistic abstractions and the pre-$\omega$-continuity of $\otimes_{e}$.
  - If $\text{Act}(e) = \text{cond}[\phi]$, then $\text{LHS}'(v) = \text{LHS}(u_1) \phi \otimes_{e} \text{LHS}(u_2)$ and $\text{RHS}'(v) = \text{RHS}(u_1) \phi \otimes_{A} \text{RHS}(u_2)$. Then $\gamma(\text{RHS}'(v)) = \gamma(\text{RHS}(u_1) \phi \otimes_{A} \text{RHS}(u_2)) \subseteq_e \gamma(\text{RHS}(u_1)) \phi \otimes_{e} \gamma(\text{RHS}(u_2)) \subseteq_e \gamma(\text{LHS}(u_1) \phi \otimes_{e} \text{LHS}(u_2)) = \text{LHS}'(v)$.
    - The two inequalities come from the definition of probabilistic abstractions and the pre-$\omega$-continuity of $\phi \otimes_{e}$.
  - If $\text{Act}(e) = \text{call}[l]$, then $\text{LHS}'(v) = \text{LHS}(v^{\text{entry}_{l}}) \otimes_{e} \text{LHS}(u_1)$ and $\text{RHS}'(v) = \text{RHS}(v^{\text{entry}_{l}}) \otimes_{A} \text{RHS}(u_1)$. It is similar to the seq[act] case.
- If $\text{Act}(e) = \text{prob}[p]$, then $\text{LHS}'(v) = \text{LHS}(u_1)_{p \oplus e} \text{LHS}(u_2)$ and $\text{RHS}'(v) = \text{RHS}(u_1)_{p \oplus e} \text{RHS}(u_2)$. Then $\gamma(\text{RHS}'(v)) = \gamma(\text{RHS}(u_1)_{p \oplus e} \text{RHS}(u_2)) \supseteq e \gamma(\text{RHS}(u_1))_{p \oplus e} \gamma(\text{RHS}(u_2)) \supseteq e \text{LHS}(u_1)_{p \oplus e} \text{LHS}(u_2) = \text{LHS}'(v)$. The two inequalities come from the definition of probabilistic abstractions and the pre-$\omega$-continuity of $p \oplus e$.

- If $\text{Act}(e) = \text{nondet}$, then $\text{LHS}'(v) = \text{LHS}(u_1)_{\text{ue}} \text{LHS}(u_2)$ and $\text{RHS}'(v) = \text{RHS}(u_1)_{\text{ue}} \text{RHS}(u_2)$. Then $\gamma(\text{RHS}'(v)) = \gamma(\text{RHS}(u_1))_{\text{ue}} \text{RHS}(u_2)) \supseteq e \gamma(\text{RHS}(u_1))_{\text{ue}} \gamma(\text{RHS}(u_2)) \supseteq e \text{LHS}(u_1)_{\text{ue}} \text{LHS}(u_2) = \text{LHS}'(v)$. The two inequalities come from the definition of probabilistic abstractions and the pre-$\omega$-continuity of $\text{ue}$.

Hence we conclude that $\text{LHS}' \supseteq e \gamma(\text{RHS}')$, i.e., $(F_P^e)^{n+1}(\lambda v. \bot e) \supseteq e \gamma((F_P^e)^{n+1}(\lambda v. \bot e))$. \hfill $\Box$

### 4.3 Interprocedural Analysis Algorithm

We are given a probabilistic program $P$ and an interpretation $\mathcal{A} = \langle A, [\cdot]^{\mathcal{A}} \rangle$, where $A = \langle M_A, \sqsubseteq_A, \circlearrowleft_A, \psi_A, \sigma_A, \text{ue}_A, \bot_A, I_A \rangle$ is a PMA and $[\cdot]^{\mathcal{A}}$ is a semantic function. The goal is to compute (an overapproximation of) $\mathcal{A}[P] = \text{lpp}_{\mathcal{A}} F_P^{\mathcal{A}}$. An equivalent way to define $\mathcal{A}[P]$ is to specify it as the least solution to a system of inequalities on $\{\mathcal{A}[v] | v \in V\}$ (where $e \in E$ in each case):

<table>
<thead>
<tr>
<th>$\mathcal{A}[v] \supseteq_A [\text{act}]^{\mathcal{A}} \circlearrowleft_A \mathcal{A}[u_1]$</th>
<th>$e$</th>
<th>$\text{Ctrl}(e)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\mathcal{A}[v] \supseteq_A \mathcal{A}[u_1] \psi_A$</td>
<td>$\text{seq}(\text{act})$</td>
<td></td>
</tr>
<tr>
<td>$\mathcal{A}[v] \supseteq_A \mathcal{A}[u_1] \circlearrowleft_A$</td>
<td>$\text{cond}(\psi)$</td>
<td></td>
</tr>
<tr>
<td>$\mathcal{A}[v] \supseteq_A \mathcal{A}[u_1]_{\text{ue}}$</td>
<td>$\text{prob}(p)$</td>
<td></td>
</tr>
<tr>
<td>$\mathcal{A}[v] \supseteq_A \mathcal{A}[u_1]_{\bot}$</td>
<td>$\text{nondet}$</td>
<td></td>
</tr>
<tr>
<td>$\mathcal{A}[v] \supseteq_A \mathcal{A}[v']_{\text{entry}} \circlearrowleft_A$</td>
<td>$\text{call}(i)$</td>
<td></td>
</tr>
<tr>
<td>$\mathcal{A}[v] \supseteq_A I_A$</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Note that in line 5 a call is treated as a hyper-edge with the action $\lambda (\text{entry}, \text{succ}).\text{entry} \circlearrowleft_A \text{succ}$. There is no explicit return edge to match a call (as in many multi-procedure program representations, e.g., [Reps et al. 1995]); instead, each exit node is initialized with the constant $I_A$ (line 6).

We mainly use known techniques from previous work on interprocedural dataflow analysis, with some adaptations to our setting, which uses hyper-graphs instead of ordinary graphs (i.e., CFGs). In that setting, one deals with hyper-graphs with consistent control-flow graphs. With PMAF, because each procedure is represented as a hyper-graph, one has hyper-graphs of constituent hyper-graphs. Fortunately, each procedure’s hyper-graph is a single-entry/single-exit hyper-graph, so the basic ideas and algorithms from standard interprocedural dataflow analysis carry over to PMAF.

### 4.4 Widening

Widening is a general technique in static analysis to ensure and speed up convergence [Cousot 1981; Cousot and Cousot 1978]. To choose the nodes at which widening is to be applied, we treat the hyper-graph as a graph—i.e., each hyper-edge (including calls) contributes one or two

---

4 As mentioned in section 2.3, standard formulations of interprocedural dataflow analysis [Knoop and Steffen 1992; Lal et al. 2005; Müller-Olm and Seidl 2004; Sharir and Pnueli 1981] can be viewed as hyper-graph analyses. In that setting, one deals with hyper-graphs with consistent control-flow graphs. With PMAF, because each procedure is represented as a hyper-graph, one has hyper-graphs of constituent hyper-graphs. Fortunately, each procedure’s hyper-graph is a single-entry/single-exit hyper-graph, so the basic ideas and algorithms from standard interprocedural dataflow analysis carry over to PMAF.
ordinary edges. More precisely, we construct a *dependence graph* \( G(H) = \langle N, A \rangle \) from hyper-graph 
\[ H = \langle \{V_i, E_i, v_i^{\text{entry}}, v_i^{\text{exit}}\}_{1 \leq i \leq n} \rangle \]
by defining \( N = \bigcup_{1 \leq i \leq n} V_i \), and
\[ A \triangleq \{ (u, v) \mid \exists e \in E. (v = \text{src}(e) \land u \in \text{Dst}(e)) \} \cup \{ (v_1^{\text{entry}}, v) \mid \exists e \in E. (v = \text{src}(e) \land \text{Ctrl}(e) = \text{call}[i]) \}. \]  
(2)

We then compute a set \( W \) of widening points for \( G(H) \) via the algorithm of Bourdoncle [Bourdoncle 1993, Fig. 4]. Because of the second set-former in (2), \( W \) contains widening points that cut each cycle caused by recursion.

While traditional programs exhibit only one sort of choice operator, probabilistic programs can have three different kinds of choice operators, and hence loops can exhibit three different kinds of behavior. We found that if we used the same widening operator for all widening nodes, there could be a substantial loss in precision. Thus, we equip the framework with three separate widening operators: \( \sqcap_c, \sqcap_p, \) and \( \sqcap_n \). Let \( v \in W \) be the source of edge \( e \in E \). Then the inequalities become

<table>
<thead>
<tr>
<th>( e )</th>
<th>( \text{Ctrl}(e) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( [\text{act}] \cap_{A} \alpha</td>
<td>v_n )</td>
</tr>
<tr>
<td>( [\text{act}] \cap_{A} \alpha</td>
<td>v_n )</td>
</tr>
<tr>
<td>( [\text{act}] \cap_{A} \alpha</td>
<td>v_n )</td>
</tr>
<tr>
<td>( [\text{act}] \cap_{A} \alpha</td>
<td>v_n )</td>
</tr>
<tr>
<td>( [\text{act}] \cap_{A} \alpha</td>
<td>v_n )</td>
</tr>
</tbody>
</table>

**Observation 4.9.** Recall from Defn. 3.2 that in a probabilistic program each non-exit node has exactly one outgoing hyper-edge. In each right-hand side above, the second argument to the widening operator re-evaluates the action of the (one outgoing) hyper-edge. Consequently, during an analysis, we have the invariant that whenever a widening operation \( a \cap b \) is performed, the property \( a \sqsubseteq_A b \) holds.

The safety properties for the three widening operators are adaptations of the standard stabilization condition: For every pair of ascending chains \( \{a_k\}_{k \in N} \) and \( \{b_k\}_{k \in N} \),

- the chain \( \{c_k\}_{k \in N} \) defined by \( c_0 = a_0 \cup_A b_0 \) and \( c_{k+1} = c_k \sqcap_c (a_{k+1} \cup_A b_{k+1}) \) is eventually stable;
- the chain \( \{c_k\}_{k \in N} \) defined by \( c_0 = a_0 \cup_A b_0 \) and \( c_{k+1} = c_k \sqcap_p (a_{k+1} \cup_A b_{k+1}) \) is eventually stable; and
- the chain \( \{c_k\}_{k \in N} \) defined by \( c_0 = a_0 \cup_A b_0 \) and \( c_{k+1} = c_k \sqcap_n (a_{k+1} \cup_A b_{k+1}) \) is eventually stable.

## 5 Instantiations

In this Section, we instantiate the framework to derive three important analyses: Bayesian inference (BI) (section 5.1), computing rewards in Markov decision processes (section 5.2), and linear expectation-invariant analysis (LEIA) (section 5.3).

### 5.1 Bayesian Inference

Claret et al. [Claret et al. 2013] proposed a technique to perform Bayesian inference on Boolean programs using dataflow analysis. They use a forward analysis to compute the posterior distribution of a single-procedure, well-structured, probabilistic program. Their analysis is similar to an intraprocedural dataflow analysis: they use discrete joint-probability distributions as dataflow facts,
merge these facts at join points, and compute fixpoints in the presence of loops. Let Var be the set of program variables; the set of program states is \( \Omega = \text{Var} \rightarrow \mathbb{B} \). Note that \( \Omega \) is isomorphic to \( \mathbb{B}^{\text{Var}} \), and consequently, a distribution can be represented by a vector of length \( 2^{\text{Var}} \) of reals in \( \mathbb{R}_{[0,1]} \). (Their implementation uses Algebraic Decision Diagrams [Bahar et al. 1997] to represent distributions compactly.)

The algorithm by Claret et al. is defined inductively on the structure of programs [Claret et al. 2013, Alg. 2]—for example, the output distribution of \( x \sim \text{Bernoulli}(r) \) from an input distribution \( \mu \), denoted by \( \text{POST}(\mu, x \sim \text{Bernoulli}(r)) \), is computed as \( \lambda \cdot (r \cdot \sum_{\sigma' | \sigma' = \sigma(x \leftarrow \text{true})} \mu(\sigma) + (1 - r) \cdot \sum_{\sigma' | \sigma' = \sigma(x \leftarrow \text{false})} \mu(\sigma)) \).

We have used PMAF to extend their work in two dimensions, creating (i) an interprocedural version of Bayesian inference with (ii) nondeterminism. Because of nondeterminism, for a given input state the posterior distribution is not unique; consequently, our goal is to compute procedure summaries that give lower bounds on posterior distributions.

To reformulate the domain in the two-variable-setting needed for computing procedure summaries, we introduce \( \text{Var}' \), primed versions of the variables in \( \text{Var} \). \( \text{Var} \) and \( \text{Var}' \) denote the variables in the pre-state and post-state of a state transformer. A distribution transformer (and therefore a procedure summary) is a matrix of size \( 2^{\text{Var}} \times 2^{\text{Var}'} \) of reals in \( \mathbb{R}_{[0,1]} \). We define a PMAF \( \mathcal{B} = (M_\mathcal{B}, \sqsubseteq_\mathcal{B}, \odot_\mathcal{B}, p_\mathcal{B}, \oplus_\mathcal{B}, \ominus_\mathcal{B}, \bot_\mathcal{B}) \) as follows:

<table>
<thead>
<tr>
<th>( M_\mathcal{B} )</th>
<th>( \rightarrow \mathbb{R}_{[0,1]} )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( a \sqsubseteq_\mathcal{B} b )</td>
<td>( \downarrow_\mathcal{B} \equiv \min(a, b) )</td>
</tr>
<tr>
<td>( a \odot_\mathcal{B} b )</td>
<td>( \uparrow_\mathcal{B} \equiv \lambda(s, t).0 )</td>
</tr>
<tr>
<td>( a \oplus_\mathcal{B} b )</td>
<td>( \mathcal{B} \cdot a + (1 - p) \cdot b )</td>
</tr>
<tr>
<td>( a \ominus_\mathcal{B} b )</td>
<td>( \mathcal{B} \cdot \lambda(s, t), {s = t} )</td>
</tr>
<tr>
<td>( a \odot_\mathcal{B} b )</td>
<td>( \mathcal{B} \cdot \lambda(s, t) \cdot \text{if } \varphi(s) \text{ then } a(s, t) \text{ else } b(s, t) )</td>
</tr>
</tbody>
</table>

The point of view is that \( \odot_\mathcal{B} b \) causes the analysis to compute procedure summaries that provide lower bounds on the posterior distributions.

**Theorem 5.1.** \( \mathcal{B} \) is a PMA.

Let \( \mathcal{C} = (\mathcal{B}, [\{\}]^{\mathcal{B}}) \) be the interpretation for Bayesian inference. We define the semantic function as \( [x := e]^\mathcal{B} = \lambda(s, A), [s[x \leftarrow e(s)] \in A] \) and \( [x := e]^\mathcal{C} = \lambda(s, t), [s[x \leftarrow e(s)] = t] \), as well as \( [x \sim \text{Bernoulli}(p)]^\mathcal{C} = \lambda(s, A), p \cdot [s[x \leftarrow \text{true}] \in A] + (1 - p) \cdot [s[x \leftarrow \text{false}] \in A] \) and \( [x \sim \text{Bernoulli}(p)]^\mathcal{C} = \lambda(s, t), p \cdot [s[x \leftarrow true] = t] + (1 - p) \cdot [s[x \leftarrow false] = t] \).

We define the concretization mapping \( \gamma_B : M_\mathcal{B} \rightarrow \mathbb{P}\Omega \) as \( \gamma_B(a) = \langle \{s \mid \forall s', \lambda(s, s') \geq a(s, s')\} \rangle \), where \( \langle C \rangle \) denotes the smallest element in \( \mathbb{P}\Omega \) such that contains \( C \).

**Theorem 5.2.** \( \gamma_B \) is a prob. under-abstraction from \( e \) to \( B \).

**Proof.** Let \( e \in \mathbb{S}_\mathcal{O}_\bot \), where \( \mathcal{O} \equiv 2^{\text{Var}} \) is the set of program states, as a flat domain \( \mathcal{O}_\bot \equiv \mathcal{O} \cup \{\bot\} \) with a distinguished bottom element \( \bot \). Because \( \mathcal{O}_\bot \) is a finite set, it is straightforward to show that \( \mathcal{O}_\bot \) is an FS-domain. Hence \( \mathbb{S}_\mathcal{O}_\bot \) is well-defined. Then \( \gamma_B(a) = \{a, a, s' \cdot s, s', \varphi(s', s')\} \).

- We want to show \( \gamma_B(\bot_\mathcal{B}) \subseteq e \). It is sufficient to show \( \downarrow(\lambda s.\lambda s', [s \in S]) \). Straightforward.
- We want to show \( \gamma_B(1_\mathcal{B}) \subseteq e \). It is sufficient to show \( \uparrow(\lambda s.\lambda s', [s \in S]) \). Straightforward.
- We want to show for all \( Q_1, Q_2 \in \mathcal{B} \), \( \gamma_B(Q_1 \odot_\mathcal{B} Q_2) \subseteq e \gamma_B(Q_1) \odot_\mathcal{B} \gamma_B(Q_2) \). It is sufficient to show \( \gamma_B(Q_1 \times Q_2) \supseteq \mathcal{O}(\gamma_B(Q_1) \odot_\mathcal{B} \gamma_B(Q_2)) \). Observe that \( \gamma_B(Q_1 \times Q_2) \) is saturated and generally convex, it is sufficient to show \( \gamma_B(Q_1) \odot_\mathcal{B} \gamma_B(Q_2) \subseteq \gamma_B(Q_1 \times Q_2) \). Suppose \( k_1 \in \)
were defined as finite-state machines with actions that exhibit probabilistic transitions. In this paper, reward analyses of finite-state Markov decision processes were originally developed in the fields of operational research and finance mathematics [Puterman 1994]. Originally, Markov decision processes were defined as finite-state machines with actions that exhibit probabilistic transitions. In this paper, we use a slightly different formalization, using hyper-graphs.

Definition 5.3 (Markov decision process). A Markov decision process (MDP) is a hyper-graph \( H = \langle V, E, \text{entry}, \text{exit} \rangle \), where every node except \( \text{exit} \) has exactly one outgoing hyper-edge; each hyper-edge with just a single destination has an associated reward, seq[reward(r)], where \( r \) is a positive real number; and each hyper-edge with two destinations has either prob[p], where \( 0 \leq p \leq 1 \), or ndet. Note that MDPs are a specialization of single-procedure probabilistic programs without conditional-choice.

We can also treat the hyper-graph as a graph: each hyper-edge contributes one or two graph edges. A path through the graph has a reward, which is the sum of the rewards that label the edges of the path. (Edges from hyper-edges with the actions prob[p] or ndet are considered to have reward 0.) The analysis problem that we wish to solve is to determine, for each node \( v \), the greatest expected reward that one can gain by executing the program from \( v \).
5 \text{ INSTANTIATIONS}

It is natural to extend MDPs with procedure calls and multiple procedures, to obtain recursive Markov decision processes. The set of program states is defined to be the set of nonnegative real numbers: $\Omega = [0, \infty)$. To address the maximum-expected-reward problem for a recursive Markov decision process, we define a PMA $\mathcal{R} = (M_\mathcal{R}, \sqsubseteq_\mathcal{R}, \circ_\mathcal{R}, \varphi, \otimes_\mathcal{R}, \psi_\mathcal{R}, \sqsubseteq_\mathcal{R}, \sqcup_\mathcal{R})$ as follows:

<table>
<thead>
<tr>
<th>$M_\mathcal{R}$</th>
<th>$\sqsubseteq_\mathcal{R}$</th>
<th>$\circ_\mathcal{R}$</th>
<th>$\varphi$</th>
<th>$\otimes_\mathcal{R}$</th>
<th>$\psi_\mathcal{R}$</th>
<th>$\sqsubseteq_\mathcal{R}$</th>
<th>$\sqcup_\mathcal{R}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$[0, \infty]$</td>
<td>$\subseteq$</td>
<td>$\leq$</td>
<td>$\max$</td>
<td>$a \cdot p \otimes b \defeq p \cdot a + (1 - p) \cdot b$</td>
<td>$\max$</td>
<td>$0$</td>
<td>$0$</td>
</tr>
</tbody>
</table>

Theorem 5.4. $\mathcal{R}$ is a PMA.

Let $\mathcal{R} = (\mathcal{R}, [\cdot]^{\mathcal{R}})$ be the interpretation for a Markov decision process with rewards. We define the semantic function as $[\text{reward}(r)]^{\mathcal{R}} = \lambda(s, A), [s + r \in A]$ and $[\text{reward}(r)]^{\mathcal{R}} = r$.

We define the concretization mapping $\gamma_\mathcal{R} : M_\mathcal{R} \rightarrow \mathbb{P}[0, \infty]$ as follows: $\gamma_\mathcal{R}(a) = \langle\{k \mid \forall s. \int y \cdot \kappa(s, dy) \leq s + a\}\rangle$.

Theorem 5.5. $\gamma_\mathcal{R}$ is a prob. over-approximation from $\mathcal{R}$ to $\mathcal{R}$.

Proof. Let $\mathcal{E}$ be $\mathbb{H}_\Omega$, where $\Omega \defeq [0, \infty]$ is the set of program states, as a dcpo with the linear order. Then $\gamma_\mathcal{R}(a) = \{s \mid \forall s. \int y \cdot \kappa(s, dy) \leq s + a\}$.

- We want to show $\sqsubseteq_\mathcal{E} \subseteq_\mathcal{E} \gamma_\mathcal{R}(\sqsubseteq_\mathcal{R})$. It is sufficient to show $\sqsubseteq_\mathcal{K} \in \gamma_\mathcal{R}(0)$. Because $1_\mathcal{K} \in \gamma_\mathcal{R}(0)$, we know $\gamma_\mathcal{R}(0)$ is nonempty, and observe that it is Scott-closed, hence we conclude the proof.

- We want to show $1_\mathcal{E} \subseteq_\mathcal{E} \gamma_\mathcal{R}(1_\mathcal{R})$. It is sufficient to show $1_K \in \gamma_\mathcal{R}(0)$. Straightforward.

- We want to show for all $Q_1, Q_2 \in \mathcal{R}$, $\gamma_\mathcal{R}(Q_1) \otimes_\mathcal{E} \gamma_\mathcal{R}(Q_2) \subseteq_\mathcal{E} \gamma_\mathcal{R}(Q_1 \otimes Q_2)$. It is sufficient to show $\gamma_\mathcal{R}(Q_1) \otimes_\mathcal{E} \gamma_\mathcal{R}(Q_2) \subseteq_\mathcal{E} \gamma_\mathcal{R}(Q_1 + Q_2)$. Observe that the right-hand-side is Scott-closed and generally convex, it is sufficient to show that $\gamma_\mathcal{R}(Q_1) \otimes_\mathcal{R} \gamma_\mathcal{R}(Q_2) \subseteq \gamma_\mathcal{R}(Q_1 + Q_2)$. Suppose $\kappa_1 \in \gamma_\mathcal{R}(Q_1)$ and $\kappa_2 \in \gamma_\mathcal{R}(Q_2)$. Observe that $\int y \cdot \kappa_1(s)(dy) \leq s + Q_1$ and $\int y \cdot \kappa_2(s)(dy) \leq s + Q_2$. Then $\int y \cdot (\kappa_1 \otimes_\mathcal{R} \kappa_2)(s)(dy) = \int y \cdot (\int z \cdot \kappa_1(s)(dz) \cdot \kappa_2(z)(dy)) = \int z \cdot \int y \cdot \kappa_1(s)(dz) \cdot \kappa_2(z)(dy) \leq \int (z + Q_2) \cdot \kappa_1(s)(dz) = \int z \cdot \kappa_1(s)(dz) + \int Q_2 \cdot \kappa_1(s)(dz) \leq s + Q_1 + Q_2$. Hence $\kappa_1 \otimes_\mathcal{R} \kappa_2 \in \gamma_\mathcal{R}(Q_1 + Q_2)$.

- We want to show for all $Q_1, Q_2 \in \mathcal{R}$ and $p \in [0, 1]$, $\gamma_\mathcal{R}(Q_1) \otimes_\mathcal{R} \gamma_\mathcal{R}(Q_2) \subseteq_\mathcal{E} \gamma_\mathcal{R}(Q_1 \oplus_\mathcal{R} Q_2)$. It is sufficient to show that $\gamma_\mathcal{R}(Q_1) \otimes_\mathcal{R} \gamma_\mathcal{R}(Q_2) \subseteq_\mathcal{E} \gamma_\mathcal{R}(pQ_1 + (1 - p)Q_2)$. Observe that the right-hand-side is Scott-closed, it is sufficient to show that $\gamma_\mathcal{R}(Q_1) \otimes_\mathcal{R} \gamma_\mathcal{R}(Q_2) \subseteq_\mathcal{E} \gamma_\mathcal{R}(pQ_1 + (1 - p)Q_2)$. Suppose $\kappa_1 \in \gamma_\mathcal{R}(Q_1)$ and $\kappa_2 \in \gamma_\mathcal{R}(Q_2)$. Observe that $\int y \cdot \kappa_1(s)(dy) \leq s + Q_1$ and $\int y \cdot \kappa_2(s)(dy) \leq s + Q_2$. Then $\int y \cdot (\kappa_1 \oplus_\mathcal{R} \kappa_2)(s)(dy) = \int y \cdot (p \kappa_1 + (1 - p) \kappa_2)(s)(dy) = \int y \cdot p \kappa_1(s)(dy) + \int y \cdot (1 - p) \kappa_2(s)(dy) \leq pQ_1 + (1 - p)Q_2$. Hence $\kappa_1 \oplus_\mathcal{R} \kappa_2 \in \gamma_\mathcal{R}(pQ_1 + (1 - p)Q_2)$.

- We want to show for all $Q_1, Q_2 \in \mathcal{R}$, $\gamma_\mathcal{R}(Q_1) \psi_\mathcal{R}(Q_2) \subseteq_\mathcal{E} \gamma_\mathcal{R}(Q_1 \psi_\mathcal{R} Q_2)$. It is sufficient to show that $\gamma_\mathcal{R}(Q_1) \cup_\mathcal{R} \gamma_\mathcal{R}(Q_2) \subseteq_\mathcal{E} \gamma_\mathcal{R}(\max(Q_1, Q_2))$. Observe that the right-hand-side is Scott-closed and generally convex, it is sufficient to show that $\gamma_\mathcal{R}(Q_1) \cup_\mathcal{R} \gamma_\mathcal{R}(Q_2) \subseteq_\mathcal{E} \gamma_\mathcal{R}(\max(Q_1, Q_2))$. It follows directly from the fact that $Q_1 \leq \max(Q_1, Q_2)$ and $Q_2 \leq \max(Q_1, Q_2)$, as the definition of $\gamma_\mathcal{R}$.

\[ \square \]

We use a trivial widening in this analysis: if after some fixed number of iterations the analysis does not converge, it returns $\infty$ as the result.
5.3 Linear Expectation-Invariant Analysis

Several examples of section expectation invariants obtained via linear expectation-invariant analysis (LEIA) were given in section 2.2. This section gives details of the abstract domain for LEIA.

We make use of an existing abstract domain, namely, the domain of convex polyhedra [Cousot and Halbwachs 1978]. Elements of the polyhedral domain are defined by linear-inequality and linear-equality constraints among program variables. For LEIA, we use two-vocabulary polyhedra over nonnegative program variables. Let \( x = (x_1, \ldots, x_n)^T \) be a column vector of nonnegative program variables and \( x' = (x'_1, \ldots, x'_n)^T \) be a column vector of the “primed” versions of corresponding program variables. A polyhedron \( P \subseteq \mathbb{R}_{\geq 0}^n \) captures linear-inequality constraints among \( x \) and \( x' \), which can be interpreted as a relation between pre-state and post-state variable valuations.

A polyhedron \( P = ((x'Tx')^T \in \mathbb{R}_{\geq 0}^n | A'x' + Ax \leq b \land D'x' + Dx = e) \), can be encoded as the intersection of a finite number of closed half spaces and a finite number of subspaces, where \( A', A, D', D \) are matrices and \( b, e \) are vectors. The associated constraint set is defined as \( \mathcal{EP} = \{A'x' + Ax \leq b, D'x' + Dx = e \} \). Let \( \mathcal{P} \) be the set of polyhedra; \( \mathcal{P} \) is equipped with meet, join, renaming, forgetting, and comparison operations.

LEIA uses expectation polyhedra. They are actually the same as polyhedra, except that the two vocabularies are \( x = (x_1, \ldots, x_n)^T \) and \( \mathbb{E}[x'] = (\mathbb{E}[x'_1], \ldots, \mathbb{E}[x'_n])^T \). An expectation polyhedron represents a constraint set of the form

\[
\{A'\mathbb{E}[x'] + Ax \leq b, D'\mathbb{E}[x'] + Dx = e\}. \tag{3}
\]

Because of the linearity of the expectation operator \( \mathbb{E} \), an equivalent way to express (3) is as follows:

\[
\{\mathbb{E}[A'x'] + Ax \leq b, \mathbb{E}[D'x'] + Dx = e\}.
\]

Let \( \mathcal{EP} \) be the set of expectation polyhedra. \( \mathcal{EP} \) is equipped with the same set of operations as \( \mathcal{P} \).

We define the state space to be \( \Omega = \mathbb{R}^n_{\geq 0} \). We then define a PMA \( \gamma \) with a universe \( \mathcal{M}_2 \equiv \mathcal{P} \times \mathcal{EP} \). An element \( (P, EP) \in \gamma \) consists of (i) a set of standard constraints \( P \subseteq \mathcal{P} \), and (ii) a set of expectation constraints \( EP \subseteq \mathcal{EP} \), such that \( 0 \cup \mathbb{P}[\mathbb{E}[x']/x'] \cup EP \) holds, where \( 0 \equiv \bigwedge_{i=1}^n (\mathbb{E}[x'_i] = 0) \). The latter property means that, if necessary, we can always “build” a pessimistic \( \mathcal{EP} \) component from the \( \mathcal{P} \) component as \( 0 \cup \mathbb{P}[\mathbb{E}[x']/x'] \).

We define the concretization mapping \( \gamma \) as follows:

\[
\gamma(P, EP) = \{ \gamma \in \mathcal{M} | \forall s, \langle s', s' \rangle \cup \{ \gamma \} = 0 \land \left[ \begin{array}{c} s' \delta \gamma) \bar{s} \rangle \\ s' \delta \gamma) \bar{s} \rangle \\ \end{array} \right] \models \mathcal{EP} \}.
\]

Comparison. The comparison operation on ordinary polyhedra can be defined as standard set inclusion. For expectation polyhedra, taking into account subprobability distributions, we define \( EP_1 \subseteq EP_2 \) to be \( 0 \cup EP_1 \subseteq 0 \cup EP_2 \), so that any element inside or below \( EP_1 \) should also be inside or below \( EP_2 \). Consequently, we define \( (P_1, EP_1) \subseteq (P_2, EP_2) \equiv P_1 \subseteq P_2 \land 0 \cup EP_1 \subseteq 0 \cup EP_2 \).

Composition. For ordinary polyhedra, the composition of \( P_1 \) and \( P_2 \) can be defined as

\[
(\exists x''. \mathcal{E}_{P_1}[x''/x'] \land \mathcal{E}_{P_2}[x'']/x)) \Rightarrow \mathcal{E}_{P_1 \otimes P_2},
\]

where we introduce an intermediate vocabulary \( x'' = (x'_1, \ldots, x''_n)^T \), and use it to connect \( P_1 \) and \( P_2 \). Consequently, we define \( P_1 \otimes P_2 \) to be \( \exists x''. \mathcal{E}_{P_1}[x''/x'] \land \mathcal{E}_{P_2}[x'']/x) \). Operationally, composition

\[\text{...}\]

\[\text{...}\]
involves first introducing a new vocabulary; renaming the variables properly; performing a meet, and finally forgetting the intermediate vocabulary.

Somewhat surprisingly, because of the tower property in probability theory, exactly the same steps can be used to compose expectation polyhedra. Informally, the tower property means that \( E[X] = E[E[X \mid Y]] \), where \( X \) and \( Y \) are two random variables, and \( E[X \mid Y] \) is a conditional expectation. For instance, suppose that \( EP_1 \) and \( EP_2 \) are defined by the constraint sets \( \{E(x') = x + 2\} \) and \( \{E(x') = 7x\} \), respectively. Following the renaming recipe above, we have \( E(x'') = x + 2 \) and \( E(x' \mid x'') = 7x'' \). By the tower property, we have \( E(x') = E(E(x' \mid x'')) = 7(7x'') = 7(x + 14) \). Operationally, the tower property allows us to compose linear expectation invariants, and eliminate the intermediate vocabulary \( x'' \). Consequently, we define

\[
[P_1, EP_1] \otimes [P_2, EP_2] \overset{\text{def}}{=} [P_1 \otimes P_2, EP_1 \otimes EP_2].
\]

**Conditional-choice.** For the ordinary-polyhedron component, a conditional-choice \( \varphi \diamond \) is performed by first meeting each operand with the logical constraint \( \varphi \), and then joining the results. However, for the expectation-polyhedron component, conditioning can split the probability space in almost arbitrary ways. Consequently, the constraints on post-state expectations as a function of pre-state valuations are not necessarily true after conditioning. Thus, we define

\[
(P_1, EP_1) \varphi \diamond (P_2, EP_2) \overset{\text{def}}{=} \text{let } P = ((\varphi) \cap P_1) \cup ((\neg \varphi) \cap P_2) \text{ in } (P_1, EP_1 \cup EP_2) \cap (0 \cup P[E|x'']/x')).
\]

The \( \cap \) in the second component is performed to maintain the invariant that \( 0 \cup P[E|x'']/x' \) \( \not\subseteq \) the second component.

**Probabilistic-choice.** For the ordinary-polyhedron component, we merely join the components of the two operands. For the expectation-polyhedron component, we introduce two more vocabularies and have

\[
(\exists x'', x'''. \mathcal{C}_{EP_1}[x''/E[x']'] \land \mathcal{C}_{EP_2}[x'''/E[x']'] \land \bigwedge_{i=1}^{n} E[x'_i] = p \cdot x''_i + (1-p) \cdot x'''_i) \Rightarrow \mathcal{C}_{EP_1p \oplus EP_2}.
\]

Consequently, we define \( EP_1p \oplus EP_2 \) to be

\[
\exists x'', x'''. (\mathcal{C}_{EP_1}[x''/E[x']'] \land \mathcal{C}_{EP_2}[x'''/E[x']'] \land \bigwedge_{i=1}^{n} E[x'_i] = p \cdot x''_i + (1-p) \cdot x'''_i),
\]

and \( (P_1, EP_1) \varphi \otimes (P_2, EP_2) \overset{\text{def}}{=} (P_1 \cup P_2, EP_1 \otimes EP_2) \).

**Nondeterministic-choice.** The nondeterministic-choice operations on both ordinary polyhedra and expectation polyhedra can be defined as join. Hence, we define \( (P_1, EP_1) \otimes (P_2, EP_2) \overset{\text{def}}{=} (P_1 \cup P_2, EP_1 \cup EP_2) \).

**Bottom and Unit Element.** We define \( \perp \overset{\text{def}}{=} (false, 0) \), and \( 1_X \overset{\text{def}}{=} (\{x'_i = x_i \mid 1 \leq i \leq n\}, \{E[x'_i] = x_i \mid 1 \leq i \leq n\}) \).

**Semantic Function.** Some examples of the semantic mapping \([\cdot]^{\mathcal{F}}\) are as follows, where \( \min(\mathcal{D}) \) and \( \max(\mathcal{D}) \) represents the interval of the support of a distribution \( \mathcal{D} \), while \( \text{mean}(\mathcal{D}) \) stands for its average.

\[
[x_i := \varepsilon]^{\mathcal{F}} \overset{\text{def}}{=} \left( \{x'_i = \varepsilon(x) \} \cup \{x'_i = x_j \mid j \neq i\}, \{E[x'_i] = \varepsilon(x)\} \cup \{E[x'_i] = x_j \mid j \neq i\} \right)
\]

\[
[x_i \sim \mathcal{D}]^{\mathcal{F}} \overset{\text{def}}{=} \left( \{\min(\mathcal{D}) \leq x'_i \leq \max(\mathcal{D})\} \cup \{x'_i = x_j \mid j \neq i\}, \{E[x'_i] = \text{mean}(\mathcal{D})\} \cup \{E[x'_i] = x_j \mid j \neq i\} \right)
\]

\[
[\text{skip}]^{\mathcal{F}} \overset{\text{def}}{=} 1_X
\]
Note we assume all expressions in the program are linear. For nonlinear arithmetic programs, one can adopt some linearization techniques [Farzan and Kincaid 2015; Miné 2006].

**Theorem 5.6.** $\gamma_{Q}$ is a prob. over-abstraction from $\mathcal{C}$ to $\mathcal{Q}$.

**Proof.** Let $\mathcal{C} \subseteq \mathcal{H} \mathcal{O}_{\bot}$, where $\mathcal{O} \triangleq \mathbb{R}_{>0}^n$ is the set of program states, as a flat domain $\mathcal{O}_{\bot} \triangleq \mathcal{O} \cup \{\bot_{\mathcal{O}}\}$ with a distinguished bottom element $\bot_{\mathcal{O}}$. Then

\[
\gamma_{Q}(P, \mathcal{E}) = \{s \mid \forall s, k(s)(P|_{s}) = 0 \land \int_{s} y \cdot k(s)(dy) \in \mathcal{E}\}
\]

- We want to show $\bot_{\mathcal{O}} \subseteq \exists \mathcal{E} \subseteq \gamma_{Q}(\bot_{\mathcal{O}})$. It is sufficient to show $\bot_{K} \in \gamma_{Q}(false, 0)$. Straightforward.
- We want to show $\bot_{\mathcal{O}} \subseteq \gamma_{Q}(\bot_{\mathcal{Q}})$. It is sufficient to show $\bot_{K} \subseteq \gamma_{Q}([x_{1} = x_{1}], \mathcal{E}[x_{1}^{\prime} = x_{1}])$. It is sufficient to show $\bot_{K} \in \gamma_{Q}([x_{1} = x_{1}], \mathcal{E}[x_{1}^{\prime} = x_{1}])$. Straightforward.
- We want to show for all $(P_{1}, \mathcal{E}_{1}) \land (P_{2}, \mathcal{E}_{2}) \in \mathcal{J}$, $\gamma_{Q}(P_{1}, \mathcal{E}_{1}) \otimes \mathcal{E}_{2} \subseteq \gamma_{Q}((P_{1}, \mathcal{E}_{1}) \otimes (P_{2}, \mathcal{E}_{2}))$. It is sufficient to show that $\gamma_{Q}(P_{1}, \mathcal{E}_{1}) \otimes \mathcal{E}_{2} \subseteq \gamma_{Q}(P_{1} \otimes \mathcal{E}_{2}, \mathcal{E}_{2}) \otimes (P_{2}, \mathcal{E}_{2})$. Suppose $\kappa_{1} \in \gamma_{Q}(P_{1}, \mathcal{E}_{1})$ and $\kappa_{2} \in \gamma_{Q}(P_{2}, \mathcal{E}_{2})$). Observe that $(\kappa_{1} \otimes \kappa_{2})(s)(P_{1} \otimes P_{2}|_{s}) = \int_{\kappa_{1}}(1)(s)(dy) \cdot \kappa_{2}(y)(P_{1} \otimes P_{2}|_{s})$. If $y \in (P_{1})^{c},$ then $\kappa_{1}(s)[(y)] = 0$. If $y \in P_{1}|_{s}$, then by the definition of $P_{1} \otimes P_{2}$, we know $\kappa_{2}(y)(P_{1} \otimes P_{2}|_{s}) = 0$. Hence $(\kappa_{1} \otimes \kappa_{2})(s)(P_{1} \otimes P_{2}|_{s}) = 0$. On the other hand, observe that $\int_{y} \cdot (\kappa_{1} \otimes \kappa_{2})(s)(dy) = \int_{z} \cdot (\kappa_{1}(s)(z) \cdot \kappa_{2}(z)(dy)) = \int_{z}(\int_{y} \cdot \kappa_{2}(z)(dy)) \cdot \kappa_{1}(dz)$, and $\int_{y} \cdot \kappa_{2}(z)(dy) \cdot \kappa_{1}(dz) \in \mathcal{E}_{2}$ for all $z$ by the fact that $\mathcal{E}_{2}$ is convex, we know that $\int_{y} \cdot \kappa_{2}(z)(dy) \cdot \kappa_{1}(dz) \in \mathcal{E}_{2}$. Because $\int_{z} \cdot \kappa_{1}(s)(dz) \in \mathcal{E}_{1}$, we have

- We want to show for all $(P_{1}, \mathcal{E}_{1}), (P_{2}, \mathcal{E}_{2}) \in \mathcal{J}$ and $\varphi \in \mathcal{L}$, $\gamma_{Q}(P_{1}, \mathcal{E}_{1}) \varphi \otimes \mathcal{E}_{2} \subseteq \mathcal{Q}_{2}(P_{2}, \mathcal{E}_{2})$. It is sufficient to show that $\gamma_{Q}(P_{1}, \mathcal{E}_{1}) \varphi \otimes \mathcal{E}_{2} \subseteq \mathcal{Q}_{2}(P_{2}, \mathcal{E}_{2})$. Suppose $\kappa_{1} \in \gamma_{Q}(P_{1}, \mathcal{E}_{1})$ and $\kappa_{2} \in \gamma_{Q}(P_{2}, \mathcal{E}_{2})$. Observe that $(\kappa_{1} \varphi \otimes \kappa_{2})(s)(P_{1})^{c} = if \varphi(s) \ then \kappa_{1}(s)((P_{1})^{c}) else \kappa_{2}(s)((P_{1})^{c})$. If $\varphi(s)$, then $P_{1} = s \in P_{1}$, hence $(\kappa_{1} \varphi \otimes \kappa_{2})(s)(P_{1})^{c} = 0$. If $\varphi(s)$, then $P_{1} = s \in P_{1}$, hence $(\kappa_{1} \varphi \otimes \kappa_{2})(s)(P_{1})^{c} = 0$. On the other hand, observe that $\int_{y} \cdot (\kappa_{1} \varphi \otimes \kappa_{2})(s)(dy) = if \varphi(s) \ then \int_{y} \cdot \kappa_{2}(s)(dy) else \int_{y} \cdot \kappa_{2}(s)(dy)$. Hence $\int_{y} \cdot (\kappa_{1} \varphi \otimes \kappa_{2})(s)(dy) \in \mathcal{E}_{1} \cup \mathcal{E}_{2}$.
- We want to show for all $(P_{1}, \mathcal{E}_{1}), (P_{2}, \mathcal{E}_{2}) \in \mathcal{J}$ and $p \in [0, 1]$, $\gamma_{Q}(P_{1}, \mathcal{E}_{1}) p \otimes \mathcal{E}_{2} \subseteq \gamma_{Q}(P_{2}, \mathcal{E}_{2})$. It is sufficient to show that $\gamma_{Q}(P_{1}, \mathcal{E}_{1}) p \otimes \mathcal{E}_{2} \subseteq \gamma_{Q}(P_{2}, \mathcal{E}_{2}) p \otimes \mathcal{E}_{2})$. Suppose $\kappa_{1} \in \gamma_{Q}(P_{1}, \mathcal{E}_{1})$ and $\kappa_{2} \in \gamma_{Q}(P_{2}, \mathcal{E}_{2})$. Observe that $(\kappa_{1} p \otimes \kappa_{2})(s)(P_{1} \otimes P_{2}|_{s}) = p \cdot \kappa_{1}(s)(P_{1} \otimes P_{2}|_{s}) + (1 - p) \cdot \kappa_{2}(s)(P_{1} \otimes P_{2}|_{s}) = 0$. On the other hand, observe that $\int_{y} \cdot (\kappa_{1} p \otimes \kappa_{2})(s)(dy) = p \cdot \int_{y} \cdot \kappa_{1}(s)(dy) + (1 - p) \int_{y} \cdot \kappa_{2}(s)(dy)$. Hence $\kappa_{1} p \otimes \kappa_{2} \in \mathcal{E}_{1} p \otimes \mathcal{E}_{2}$.
- We want to show that for all $(P_{1}, \mathcal{E}_{1}), (P_{2}, \mathcal{E}_{2}) \in \mathcal{J}$, $\gamma_{Q}(P_{1}, \mathcal{E}_{1}) \cup \mathcal{E}_{2} \subseteq \gamma_{Q}(P_{2}, \mathcal{E}_{2})$. It is sufficient to show that $\gamma_{Q}(P_{1}, \mathcal{E}_{1}) \cup \gamma_{Q}(P_{2}, \mathcal{E}_{2}) \subseteq \gamma_{Q}(P_{1} \cup P_{2}, \mathcal{E}_{1} \cup \mathcal{E}_{2})$. Straightforward.

$\square$
6 EVALUATION

Widening. Let $\triangledown$ be the standard widening operator on ordinary polyhedra [Halbwachs 1979]. Recall from Obs. 4.9 that whenever a widening operation $a \triangledown b$ is performed, the property $a \sqsubseteq A b$ holds. There is a subtle issue with expectation invariants when dealing with conditional or nondeterministic loops.

Observation 5.7. In a conventional program, if you have a loop “while $B$ do $S$ od,” and $I$ is a loop-invariant, then $I \land \neg B$ (which implies $I$) holds on exiting the loop. In contrast, for a conditional or nondeterministic loop in a probabilistic program, a loop-invariant that holds at the beginning and end of the loop body does not necessarily hold on exiting the loop.

Example 5.8. Consider the following program:

```plaintext
while \neg(\mathit{\text{x}} = \mathit{\text{y}}) do
  \text{if prob}(\frac{1}{2}) then \mathit{\text{x}} := \mathit{\text{x}} + 1 \text{ else } \mathit{\text{y}} := \mathit{\text{y}} + 1 fi
od
```

For the loop body, we can derive an expectation invariant $\mathbb{E}[x' - y'] = x - y$; however, for the entire loop this property does not hold: at the end of the loop $x = y$ must hold, and hence $\mathbb{E}[x' - y']$ should be equal to 0.

Because of this issue, we use a pessimistic widening operator for conditional-choice and nondeterministic-choice: the widening operator forgets the expectation invariants and rebuilds them from standard invariants.

\[
(P_1, EP_1) \triangleleft_c (P_2, EP_2) \triangleq (P_1 \triangledown P_2, 0 \sqcup P_2[\mathbb{E}[x'/x']])
\]

\[
(P_1, EP_1) \triangleleft_n (P_2, EP_2) \triangleq (P_1 \triangledown P_2, 0 \sqcup P_2[\mathbb{E}[x'/x']])
\]

We do not have a good method for $(P_1, EP_1) \triangleleft_p (P_2, EP_2)$. We found that the following approach loses precision:

\[
\text{let } P = (P_1 \triangledown P_2) \text{ in } (P, (EP_1 \triangledown EP_2) \cap (0 \sqcup P[\mathbb{E}[x'/x']]))
\]

In our experiments, we use $(P_1, EP_1) \triangleleft_p (P_2, EP_2) \triangleq (P_1 \triangledown P_2, EP_2)$, which does no extrapolation in the $EP$ component.

6 Evaluation

In this Section, we first describe the implementation of PMAF, and the three instantiations introduced in section 5. Then, we evaluate the effectiveness and performance of the three analyses.

6.1 Implementation

PMAF is implemented in OCaml; the core framework consists of about 400 lines of code. The framework is implemented as a functor parametrized by a module representing a PMA, with some extra functions, such as widening and printing. This organization allows any analysis that can be formulated in PMAF to be implemented as a plugin. Also, the core framework relies on control-flow hyper-graphs, and provides users the flexibility to employ it with any front end. We use OCamlGraph [Conchon et al. 2007] as the implementation of fixed-point computation and Bourdoncle’s algorithm.

The plugin for Bayesian inference is about 400 lines of code, including a lexer and a parser for the imperative language that we use in the examples of this paper. We use Lacaml [Mottl 2017] to manipulate matrices. The plugins for the Markov decision problem with rewards and linear expectation-invariant analysis are about 200 lines and 500 lines, respectively. We use APRON [Jeannet
and Miné 2009] for polyhedron operations. Most of the code in the plugins is to implement the PMA structure of the analysis domain.

Because of the numerical reasoning required when analyzing probabilistic programs, we need to be concerned about finite numerical precision in our implementations of the instantiations (although they are sound on a theoretical machine operating on reals). In our implementation, we use the fact that ascending chains of floating numbers always converge in a finite number of steps. The user could use the technique proposed by Darulova et al. [Darulova and Kuncak 2014] to obtain a sound guarantee on numerical precision.

6.2 Experiments

Evaluation Platform. Our experiments were performed on a machine with an Intel Core i5 2.4 GHz processor and 8GB of RAM under Mac OS X 10.13.4.

Bayesian Inference and Markov Decision Problem with Rewards. We tested our framework on Bayesian inference and Markov decision problem with rewards on handcrafted examples. The results of the evaluation of the two analyses are described in Tab. 1. The tables contains the number of lines; whether the program is non-recursive, tail-recursive, or recursive; the number of procedure calls; and the time taken by the implementation (measured by running each program 5 times and computing the 20% trimmed mean).

Our framework computed the same answer (modulo floating-point round-off errors) as PReMo [Wojtczak and Etessami 2017], a tool for probabilistic recursive models. We did not compare with probabilistic abstract interpretation [Cousot and Monerau 2012] because its semantic foundation is substantially different from that of our framework—as we mentioned in section 1, the order for resolving probabilistic behavior and nondeterministic behavior is different.

The analysis time of Bayesian inference grows exponentially with respect to the number of program variables. The time cost comes from the explicit matrix representation of domain elements. One could use Algebraic Decision Diagrams [Bahar et al. 1997] as a compact representation to improve the efficiency.

The analyzer for the Markov decision problem with rewards works quickly and obtains some interesting results. quicksort7 is a model of a randomized quicksort algorithm on an array of size 7 (obtained from [Wojtczak and Etessami 2017]), and our analysis results are consistent with the worst-case expected number of comparisons being $\Theta(n \log n)$.

Linear Expectation-Invariant Analysis. We performed a more thorough evaluation of linear

\[ \text{max}_{\text{non-det. resolution}} \mathbb{E}[\#\text{comparisons under resolution}] \]

6 One should not assume that exponential growth makes the analysis useless; after all, predicate-abstraction domains [Graf and Saïdi 1997] also grow exponentially: the universe of assignments to a set of Boolean variables grows exponentially in the number of variables. Finding useful coarser abstractions for Bayesian inference—by analogy with the techniques of Ball et al. [Ball et al. 2001] for predicate abstraction—might be an interesting direction for future work.

7 The analysis computes worst-case expected number because the underlying semantics resolves nondeterminism first and probabilistic-choice second, and thus the analysis computes $\max_{\text{non-det. resolution}} \mathbb{E}[\#\text{comparisons under resolution}]$. 

Table 1: Top: Bayesian inference. Bottom: Markov decision problem with rewards. (Time is in seconds.)

<table>
<thead>
<tr>
<th>Program</th>
<th>#loc</th>
<th>rec?</th>
<th>#call</th>
<th>time</th>
</tr>
</thead>
<tbody>
<tr>
<td>compare</td>
<td>17</td>
<td>n</td>
<td>0</td>
<td>2.22</td>
</tr>
<tr>
<td>dice</td>
<td>12</td>
<td>n</td>
<td>0</td>
<td>0.02</td>
</tr>
<tr>
<td>eg1</td>
<td>10</td>
<td>n</td>
<td>0</td>
<td>0.02</td>
</tr>
<tr>
<td>eg1-tail</td>
<td>16</td>
<td>t</td>
<td>2</td>
<td>0.02</td>
</tr>
<tr>
<td>eg2</td>
<td>10</td>
<td>n</td>
<td>0</td>
<td>0.02</td>
</tr>
<tr>
<td>eg2-tail</td>
<td>16</td>
<td>t</td>
<td>2</td>
<td>0.01</td>
</tr>
<tr>
<td>recursive</td>
<td>14</td>
<td>r</td>
<td>1</td>
<td>0.01</td>
</tr>
<tr>
<td>binary10</td>
<td>184</td>
<td>n</td>
<td>90</td>
<td>0.03</td>
</tr>
<tr>
<td>loop</td>
<td>10</td>
<td>n</td>
<td>0</td>
<td>0.03</td>
</tr>
<tr>
<td>quicksort7</td>
<td>109</td>
<td>n</td>
<td>42</td>
<td>0.03</td>
</tr>
<tr>
<td>recursive</td>
<td>13</td>
<td>t</td>
<td>1</td>
<td>0.03</td>
</tr>
<tr>
<td>student</td>
<td>43</td>
<td>t</td>
<td>8</td>
<td>0.03</td>
</tr>
</tbody>
</table>
programs. For the examples obtained from the loop-invariant-generation benchmark, we extracted variables.

The interpretation [Cousot and Monerau 2012; Monniaux 2000, 2001, 2003], which is discussed in the

Most closely related to our work is probabilistic abstract

and Cousot 1977, 1979], our definition of probabilistic abstractions is based on just a concretization

analysis has been used to address, e.g., calls through function pointers.

Our framework is an extension of interprocedural dataflow

Static Analysis for Standard Programs.

7 Related Work

7 RELATED WORK

Static Analysis for Standard Programs. Our framework is an extension of interprocedural dataflow analysis [Knoop and Steffen 1992; Lal et al. 2005; Müller-Olm and Seidl 2004; Sharir and Pnueli 1981] to probabilistic programs, but it does not support some language features that standard dataflow analysis has been used to address, e.g., calls through function pointers.

Compared to the Galois connections that are ordinarily used in abstract interpretation [Cousot and Cousot 1977, 1979], our definition of probabilistic abstractions is based on just a concretization function, so PMAF does not have the full power of standard abstract-interpretation machinery.

Static Analysis for Probabilistic Programs. Most closely related to our work is probabilistic abstract interpretation [Cousot and Monet 2012; Monniaux 2000, 2001, 2003], which is discussed in the
introduction. There is a long line of research on manual reasoning techniques for probabilistic programs [Ferrer Fioriti and Hermanns 2015; Kaminski et al. 2016; Kozen 1985; McIver and Morgan 2001; Olmedo et al. 2016]. The main difference to this work is that we focus on the design and implementation of automatic techniques that rely on computing fixed points.

Other work focuses on specialized automatic analyses for specific properties. Claret et al. [Claret et al. 2013] proposed a dataflow analysis for Bayesian inference on Boolean programs that we reformulate in PMAF to lift it to the interprocedural level. There are different techniques for automatically proving termination, such as probabilistic pushdown automata [Brázdil et al. 2014, 2015] and martingales and stochastic invariants [Chatterjee et al. 2016b, 2017]. Martingales for automatic analysis of probabilistic programs have been pioneered by Chakarov et al. [Chakarov and Sankaranarayanan 2013]. Compared with existing techniques for probabilistic invariant generation [Barthe et al. 2016a; Chakarov and Sankaranarayanan 2013, 2014; Chatterjee et al. 2017], the expectation-invariant analysis proposed in section 5.3 is designed as a two-vocabulary domain utilizing the well-studied polyhedral abstract domain.

Semantics for Probabilistic Programs. There is a long tradition of using probability kernels to define the semantics of probabilistic programs. Kernels were used by Kozen [Kozen 1985] to give a semantics for Probabilistic Propositional Dynamic Logic (PPDL), a probabilistic generalization of PDL. Kozen considers well-structured programs with sequencing and conditional-choice, but without non-deterministic choice. He does not consider reasoning methods that use abstract interpretation of his PPDL semantics. There are a list of domain-theoretic studies on probabilistic nondeterminism [den Hartog and de Vink 1999; Jones 1989; Jones and Plotkin 1989; Mislove 2000; Mislove et al. 2004; Tix et al. 2009], which develop powerdomain constructions over probability distributions, but do not consider powerdomains over kernels. Borgström et al. [Borgström et al. 2016] have used kernels to define the operational semantics of a probabilistic lambda calculus. The main novelty of our denotational semantics in section 3.3 is that it is defined for control-flow hyper-graphs, based on kernels.

Other Analyses Based on Hyper-Graphs. Hyper-graph-based analyses go back to the join-over-all-hyper-path-valuations of Knuth [Knuth 1977]. Other analyses based on hyper-graphs includes Möncke and Wilhelm’s [Möncke and Wilhelm 1991] framework for finding join-over-all-hyper-path-valuations for partially ordered abstract domains. In the hyper-paths in this paper, we use binary hyper-edges to model calls, as well as conditional, probabilistic, and nondeterministic choice. For acyclic hyper-graphs, Eisner has considered semirings for computing expectations and variances of random variables [Li and Eisner 2009]. He works with a discrete sample space: all hyper-paths in a given hyper-graph, and the value of a random variable for a given hyper-path is built up as the sum of the values contributed by each hyper-edge. In our work, we consider cyclic hyper-graphs, and the nature of the computation that a hyper-path represents is more complex than that considered by Eisner.

Acknowledgments

This article is based on research supported, in part, by a gift from Rajiv and Ritu Batra; by AFRL under DARPA MUSE award FA8750-14-2-0270, DARPA STAC award FA8750-15-C-0082, and DARPA award FA8750-16-2-0274; and by the UW-Madison Office of the Vice Chancellor for Research and Graduate Education with funding from the Wisconsin Alumni Research Foundation. The U.S. Government is authorized to reproduce and distribute reprints for Governmental purposes notwithstanding any copyright notation thereon. Any opinions, findings, and conclusions or recommendations expressed in this publication are those of the authors, and do not necessarily reflect the views of the sponsoring
7 RELATED WORK

agencies.

We thank the nurses from the Univ. of Pittsburgh Medical Center for their professional medical care, which was instrumental in finishing the submission before the PLDI deadline.

References


