PMAF: An Algebraic Framework for Static Analysis of Probabilistic Programs

Di Wang
Carnegie Mellon University
USA

Jan Hoffmann
Carnegie Mellon University
USA

Thomas Reps
University of Wisconsin
USA

Abstract

Automatically establishing that a probabilistic program satisfies some property $\phi$ is a challenging problem. While a sampling-based approach—which involves running the program repeatedly—can suggest that $\phi$ holds, to establish that the program satisfies $\phi$, 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 hypergraph 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.

CCS Concepts • Software and its engineering → Automated static analysis; • Theory of computation → Probabilistic computation; Program analysis;

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

ACM Reference Format:

1 Introduction

Probabilistic programming is becoming increasingly popular because it provides a rich framework for implementing randomized algorithms [5], cryptography protocols [6], cognitive [39] models, and machine learning [37] algorithms. Static analysis of probabilistic programs has received a lot of attention [10, 11, 13–18, 25, 29–31, 33, 36, 48–50, 72, 79]. 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 [18, 30, 31], Markov decision problem with rewards [75], and probabilistic-invariant generation [13, 15, 49].

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 hypergraph 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 §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 \( \lambda a.\lambda b.a\oplus b \)—where \( \oplus \) 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 \( [v_0, \{v_1, v_5\}] \) generates the inequality \( \mathcal{A}[v_0] \supseteq \mathcal{A}[v_1] \oplus \mathcal{A}[v_5] \), 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 intraprocedural probabilistic-program analyses—the Bayesian-inference algorithm proposed by Claret et al. [18], and Markov decision problem with rewards [75]—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) [25, 67–69], 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 [27, 46, 47, 64, 65, 82].

The concrete semantics of PAI isolates probabilistic choices from the non-probabilistic part of the semantics by interpreting programs as distributions \( P : \Omega \rightarrow (D \rightarrow D) \), where \( \Omega \) is a probability space and \( D \rightarrow D \) 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.

\[
\begin{align*}
\text{if } & \text{ then if prob}(\frac{1}{2}) \text{ then return 1 else return 2} \\
\text{else if prob}(\frac{1}{2}) \text{ then return 1 else return 2} & \text{ fi}
\end{align*}
\]

In contrast, the semantics used in PMAF resolves nondeterminism 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 nondeterministic choice (§4.1 and §4.2) and general recursion (§4.3) (as well as continuous sampling and unstructured control-flow).

• We show that two previous intraprocedural probabilistic program analyses can be reformulated to fit into PMAF, thereby creating new interprocedural analyses for such previous work.

• We develop a new program analysis, linear expectation-invariant analysis, by means of a suitable instantiation of PMAF. This analysis is more general than previous approaches to finding expectation invariants.

• We report on experiments with PMAF that show that the framework is easy to instantiate and works effectively. The experiments also show that linear expectation-invariant analysis can derive nontrivial invariants.

2 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.

2.1 Probabilistic Programming
Probabilistic programs contain two sources of randomness: (i) data randomness, i.e., the ability to draw random values from distributions, and (ii) control-flow randomness, i.e., the ability to branch probabilistically. A variety of probabilistic programming languages and systems has been proposed [12, 38, 61, 63, 74]. 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 sampling statement \( x \sim \text{Dist}(\theta) \) draws a value from a distribution 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 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 Uniform(\( l, r \)) represents a uniform distribution on the interval \( (l, r) \). The probabilistic choice \( \text{prob}(p) \) returns true with probability \( p \) and false with probability \( 1 - p \). Moreover, the program also exhibits nondeterminism, as the symbol \( \star \) stands for a nondeterministic choice that can behave like standard nondeterminism, as well as an

\[
\begin{align*}
&b_1 \sim \text{Bernoulli}(0.5); & &\text{while prob}(\frac{1}{2}) \text{ do} \\
&b_2 \sim \text{Bernoulli}(0.5); & &z \sim \text{Uniform}(0, 2); \\
&\text{while } (\neg b_1 \land \neg b_2) \text{ do} & &\text{if } \star & x := x + z \\
&b_1 \sim \text{Bernoulli}(0.5); & &\text{else } y := y + z \\
&b_2 \sim \text{Bernoulli}(0.5) & &\text{fi} \\
&\text{od} & &\text{od} \\
\end{align*}
\]

Figure 1. (a) Boolean probabilistic program; (b) Arithmetic probabilistic program

arbitrary probabilistic choice [60, §6.6]. Intuitively, the program describes two players \( x \) and \( y \) playing a round-based game that ends with probability \( \frac{1}{2} \) after each round. In each round, either player \( x \) or player \( y \) gains some reward that is uniformly distributed on \( [0, 2] \).

2.2 Two Static Analyses

Bayesian inference (BI). Probabilistic programs can be seen as descriptions of probability distributions [12, 38, 63]. For a Boolean probabilistic program, such as the one in Fig. 1a, Bayesian-inference analysis [18] 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 \( P[b_1 = \text{false}, b_2 = \text{true}] = P[b_1 = \text{true}, b_2 = \text{false}] = P[b_1 = \text{true}, b_2 = \text{true}] = \frac{1}{4} \). 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 [28, 34, 43]. 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 [55, 60]. Such expectation invariants are usually defined as random variables—specified as expressions over program variables—with some desirable properties [13, 14, 49]. In this paper, we work with a more general kind of expectation invariant, defined as follows:

Definition 2.1. For a program \( P \), \( \mathbb{E}[E_2] \models E_1 \) is called an expectation invariant if \( E_1 \) and \( E_2 \) are real-valued expressions over program variables, \( \models \) is one of \( \{=, <, >, \leq, \geq\} \), and the following property holds: For any initial valuation of the program variables, the expected value of \( E_2 \) in the final valuation (i.e., after the execution of \( P \)) is related to the value of \( E_1 \) in the initial valuation by \( \models \).

We typically use variables with primes in \( E_2 \) to denote the values in the final valuation. For example, for the program in

¹In 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 \( 1 - p \).
which does not provide enough information to establish that

This section explains the main ideas behind PMAF, which is
hyper-edges
hyper-paths
collections can be precisely formalized as
and define distributions over the collections. These kinds of
in probabilistic programs, paths are no longer independent,
conditional CFG represents a collection of execution paths, while

programs. In contrast to traditional program analyses, which
control-flow randomness by capturing the different types
probabilities to compute appropriate expectations in the re-
Abstraction'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); if (p < 0.3) . . .". For program analysis,
such a simulation can lead to suboptimal results if the con-
structs 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 is a transformer that summarizes the transfor-
mation 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 rea-
soning 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 ac-
tivities of the edge's source node as a function of properties of
an edge as a property transformer that computes proper-
soning in the backward direction. The framework interprets

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—either sequencing, conditional-
choice, probabilistic-choice, or nondeterministic-choice. A tra-
tditional 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.

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

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 analy-
sis designers by providing multiple ways to translate the
constructs of their specific probabilistic programming lan-
guage into the constructs of PMAF. Analysis designers
may find it useful to use the control-flow-randomness con-
struct directly (e.g., "if prob(0.3) . . ."), rather than simu-
lating 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 con-
structs 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 frag-
ment with the explicit control-flow-randomness construct
("if prob(0.3) . . .") the analyzer can directly assign the prob-
abilities 0.3 and 0.7 to the outgoing branches, and use those
probabilities to compute appropriate expectations in the re-
spective branches.

We achieve the separation between data randomness and
classic-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—either sequencing, conditional-
choice, probabilistic-choice, or nondeterministic-choice. A tra-
tditional 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(2/3),
and ndet are conditional-choice, probabilistic-choice, and
nondeterministic-choice actions. Data actions, like x := x + y
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
v1 and v5, respectively.

Backward Analysis. Traditional static analyses assign to a
CFG node either backward assertions—about the computa-
tions that can lead up to v—or forward assertions—about the
computations that can continue from v [21, 23]. 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
have two destination nodes, but only one source node.

The second principle of the framework is essentially dic-
tated 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 transforma-
mation 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 rea-
soning 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 ac-
tion. These property transformers propagate information in a
hypergraph-leaf-to-hypergraph-root manner, which is nat-
ural in hyper-graph problems. For example, standard formu-
lations of interprocedural dataflow analysis [52, 57, 71, 80]
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 E[b1 = true, b2 = 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 (b1 = true, b2 = true). For example, the property
that we would hope to compute for node $v_1$ is the function
\[ \lambda(b_1, b_2)[b_1 \land \neg b_2 \land \varepsilon \cdot \frac{1}{3}], \]
where $\varepsilon$ 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 §5, we show that we can reformulate BI to manipulate two-vocabulary properties. As in interprocedural dataflow analysis [22, 80], 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* [32, 76, 81].

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 $\mathcal{A}$ 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 $\mathcal{A}$.)
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 §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 [21, 51]: 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., [9]), 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 $S(v) \in \mathcal{M}$ are elements in the semantic algebra; $\llbracket \cdot \rrbracket$ is the approximation order on $\mathcal{M}$; $\llbracket \cdot \rrbracket$ is the semantic function, which maps data actions to $\mathcal{M}$; and $\mathcal{F}$ 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 BL, we instantiate our framework to give lower bounds on posterior distributions, using with an interpretation in which state transformers are probability matrices (see §5.1). For LEIA, we design an interpretation using a Cartesian product of polyhedra (see §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 [35] 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 \( (V, E, v_{\text{entry}}, v_{\text{exit}}) \), where \( V \) is a finite set of nodes, \( E \) is a set of hyper-edges, \( v_{\text{entry}} \in V \) is a distinguished entry node, and \( v_{\text{exit}} \in V \) 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 \( v_{\text{entry}} \) has no incoming edges, and \( v_{\text{exit}} \) has no outgoing edges.

Definition 3.2 (Probabilistic programs). A probabilistic program contains a finite set of procedures \( \{H_i\}_{1 \leq i \leq m} \), where each procedure \( H_i = (V_i, E_i, v_{i,\text{entry}}, v_{i,\text{exit}}) \) is a control-flow hyper-graph in which each node except \( v_{i,\text{exit}} \) 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 \( \mathcal{A} \) and logical conditions \( \mathcal{L} \), we associate with each hyper-edge \( e \in E = \bigcup_{1 \leq i \leq m} E_i \) a control-flow action \( \text{Ctrl}(e) \), where \( \text{Ctrl} \) is

\[
\text{Ctrl} ::= \text{seq}[\text{act}] \mid \text{call}[\text{lit}] \mid \text{cond}[\varphi] \mid \text{prob}[p] \mid \text{ndet}
\]

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 \( \text{call}[\text{lit}] \), and 2 otherwise.

Figure 3. The system of inequalities corresponding to Fig. 2b

\[ S(v_0) \supseteq \text{prob}\left[\frac{1}{2}\right]|S(v_1), S(v_2)| S(v_0) \supseteq \text{seq}\{x := x + z\}|S(v_0) \]
\[ S(v_0) \supseteq \text{seq}\{z \sim \text{Uniform}(0, 2)|S(v_1)\} S(v_0) \supseteq \text{seq}\{y := y + z\}|S(v_0) \]
\[ S(v_0) \supseteq \text{ndet}|S(v_1), S(v_2)| S(v_0) \supseteq \|

Fig. 2 shows two examples of hyper-graph–based probabilistic programs. See Fig. 4 for data actions \( \mathcal{A} \) and logical conditions \( \mathcal{L} \) 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 \( \mathcal{A} \) and logical conditions \( \mathcal{L} \), we review some standard definitions from measure theory [7, 73].

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 \( f : X_1 \to X_2 \) 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 \( \mathcal{B}(\mathbb{R}, \mathcal{B}) \) 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 integral of a \( \Sigma \)-measurable function \( f \) over the measurable space \( \mathcal{M} = \langle X, \Sigma, \mu \rangle \) can be defined following Lebesgue’s theory and denoted either by \( \int f \, d\mu \) or \( \int f(x) \mu(dx) \). The Dirac measure \( \delta(x) \) is defined as \( \lambda A \{ x \in A \} \).

A (sub-probability) kernel from a measurable space \( \langle X_1, \Sigma_1 \rangle \) to a measurable space \( \langle X_2, \Sigma_2 \rangle \) is a function \( \kappa : X_1 \times \Sigma_2 \to [0, 1] \) such that: (i) for each \( A \in \Sigma_2 \), the function \( \lambda x. \kappa(x, A) \) is \( \Sigma_1 \)-measurable, and (ii) for each \( x \in X_1 \), the function \( \kappa_x : \Sigma_2 \to [0, \infty] \) with respect to the distribution in (ii) as \( \int f(y) \kappa(x, dy) \).

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 [8] and existing results on domain-theoretic probabilistic nondeterminism [27, 46, 47, 64, 65, 82]. This semantics can describe several nontrivial constructs, including continuous sampling, nondeterministic choice, and recursion.

Three components are used to define the semantics:
A := x := e | x ~ ∅ | skip | observe(φ)
φ ∈ L ::= true | false | e ≈ u, where ≈ ∈ {=, ≤, ≥} | ¬φ
e, u ∈ Exp ::= x | c, where c ∈ ℜ | e • u, where • ∈ {+, −, ×, /}
x ∈ Var ::= x | y | z | ···
∅ ∈ Dist ::= Uniform(e, u) | Gaussian(e, u) | ···

Example 3.3. For an arithmetic program with a finite set of program variables, a program state is defined as Var → ℜ and P as the Borel space on Ω. Fig. 5 shows interpretation of the 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 μφ : 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-variable specifications, kernels are indeed two-variable transformers over program states. When there is no nondeterminism, we can define control-flow actions on kernels. A sequence of actions act1 • act2 with kernels k1 and k2, respectively, is modeled by their composition, denoted by k1 ⊗ k2, which yields a new kernel defined as follows:

\[ k_1 \otimes k_2 \overset{\text{def}}{=} \lambda(x, A). \int k_1(x, dy)k_2(y, A). \]

(1)

The conditional-choice k1 ⊗ k2 is defined as a new kernel λ(x, A).[φ(x)] • k1(x, A) + [¬φ(x)] • k2(x, A). The probabilistic-choice k1 ⊗ k2 is defined as a new kernel λ(x, A).p • k1(x, A) + (1 − p) • k2(x, A).

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

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

Fig. 6 shows its control-flow hyper-graph. The assignment \( n := n + 1 \) is interpreted as a kernel \( n := n + 1 = \lambda(ω, F).[n → n + 1] \).

\[ x := e = \lambda(ω, F).[x \mapsto e(ω)]ω ∈ F \]
\[ x := e = \lambda(ω, F).[x \mapsto e(ω)]ω ∈ F \]
\[ x := e = \lambda(ω, F).[x \mapsto e(ω)]ω ∈ F \]

The comparison \( n \geq 10 \) is interpreted as a measurable function \( n \geq 10 = \lambda(ω(n) ≥ 10) \). Let \( k \) stand for 0.3486784401; the semantics assigned to node \( v_0 \) is

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

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 [41] of kernels. We adopt Tix et al.’s constructions of probabilistic powerdomains [82], and extend them to work on kernels instead of distributions. We denote the set of feasible collections of kernels by \( PΩ \), and the composition, conditional-choice, probabilistic-choice, and nondeterministic-choice operators on that by \( ⟨, φ, ⊕, p, ⊗, \&⟩ \). \( PΩ \) is also equipped with a partial order \( ≤ \).

We reformulated distributions and kernels in a domain-theoretic way to adopt existing studies on powerdomains. We discuss the details of the construction of \( PΩ \) in a companion paper [83]; 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 [1, §6.2] over kernels. Kernels are ordered pointwise, i.e., \( k_1 ≤ k_2 \) if and only if for all \( ω \) and \( F \), \( k_1(ω, F) ≤ k_2(ω, F) \). The zero kernel \( λ(ω, F).0 \) is the bottom element of this order. Intuitively, the Hoare powerdomain is used for partial correctness, in which the order is set inclusion on the lower closures of the elements—because each downward-closed set contains a kernel that represents nontermination (i.e., the zero kernel), terminating and nonterminating executions cannot be distinguished. The Smyth powerdomain 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 nontermination 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 \( H_i = \langle V_i, E_i, v_i^\text{entry}, v_i^\text{exit} \rangle, \) 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 $S(v) \in \mathbb{P}\mathbb{W}$ be the semantics assigned to the node $v$; the following local properties should hold:

- if $e = \langle v, \{u_1, \ldots, u_k\} \rangle \in E$, $S(v) = \text{Ctrl}(e)(S(u_1), \ldots, S(u_k))$, and
- otherwise, $S(v) = 1_\mathcal{F}$.

The function $\pi$ for the different kinds of control-flow actions is defined as follows:

<table>
<thead>
<tr>
<th>$\text{seq}(\text{act})(S_1)$</th>
<th>$\text{cond}(\varphi)(S_1, S_2)$</th>
<th>$\text{call}(i)(S_1)$</th>
<th>$\text{prob}(p)(S_1, S_2)$</th>
<th>$\text{ndet}(S_1, S_2)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>${\text{act}} \otimes S_1$</td>
<td>$S_1 \uparrow \uplus S_2$</td>
<td>$S(v_i^{\text{entry}}) \otimes S_1$</td>
<td>$S_1 \otimes S_2$</td>
<td>$S_1 \otimes S_2$</td>
</tr>
</tbody>
</table>

**Lemma 3.5.** The function $F_\pi$ defined as

$$
\lambda S, \lambda \nu. \{ \text{Ctrl}(e)(S(u_1), \ldots, S(u_k)) \mid e = \langle v, \{u_1, \ldots, u_k\} \rangle \in E \}
\nu
$$

is $\omega$-continuous on $\langle V \rightarrow \mathbb{P}\mathbb{W}, \sqsubseteq \rangle$, which is an $\omega$-cpo with the least element $\sqsubseteq$. A dot over an operator denotes its application pointwise. By Kleene's fixed-point theorem, we have

**Theorem 3.6.** If $F_\pi^\mathcal{C}$ exists for all prob. programs $P$.

Thus, the semantics of a node $v$ is defined as $(F_\pi^\mathcal{C})_v(v)$.

## 4 Analysis Framework

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

### 4.1 An Algebraic Characterization of Fixpoint Semantics

In the denotational semantics, the concrete semantics is obtained by composing $\text{Ctrl}(e)$ 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-$\omega$-continuous functions). A function $f : X \rightarrow Y$ between two $\omega$-cpos $X$ and $Y$ is pre-$\omega$-continuous if it is monotone, and for every $\omega$-chain $C \subseteq X$, $f(\sup(C)) \leq \sup(f(C))$.

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

- $a \varphi \otimes b \sqsubseteq a \sqcup b, a \sqsubseteq a \sqcup b, a \sqcup a = a$;
- $a \sqcup b = b \varphi \otimes a$;
- $a \sqcup b = b \sqcup a$;
- $a \sqcup a \sqcup b = a$;
- $a \sqcup a = a$;
- $a \sqcup b = b$;
- $1 \sqcup a = 1$;
- $1 \sqcup b = 1$;
- $\varphi \otimes (b \varphi \sqcup c) = (a \varphi \otimes b) \varphi \otimes c$ where $\varphi = \varphi \sqcup \varphi' \sqcup \psi \sqcup \psi' = \varphi'$;
- $a \sqcup (b \sqcup c) = (a \sqcup b) \sqcup c$ where $p = p' \cdot q', \tilde{q} = \tilde{q'}$

The precedence of the operators is that $\varphi \otimes$ binds tightest, followed by $\varphi \sqcup, P \sqcup, \sqcup$, and $\sqsubseteq$.

**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 §3.3 is a PMA $C = \langle \mathbb{P}\mathbb{W}, , \sqsubseteq, \sqcup, P \sqcup, \sqcup, \downarrow, 1 \rangle$ (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 $\mathcal{I} = \langle M, [\cdot] \rangle$, where $M$ is a pre-Markov algebra, and $[\cdot] : \mathcal{A} \rightarrow M$, where $\mathcal{A}$ 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 $\mathcal{I} = \langle M, [\cdot] \rangle$, 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 $F_\pi^\mathcal{I}$, which is defined as

$$
\lambda S, \lambda \nu. \{ \text{Ctrl}(e)(S\langle v_i^{\text{entry}} \rangle) \mid e = \langle v, \{u_1, \ldots, u_k\} \rangle \in E \}
\nu
$$

We generalize Kleene's fixed-point theorem to prove the existence of the least prefixed point of $F_\pi^\mathcal{I}$.

**Theorem 4.6** (Generalized Kleene's fixed point theorem). Suppose $(\mathbb{X}, \leq)$ is an $\omega$-cpo with a least element $\downarrow$, and let $f : X \rightarrow X$ be a pre-$\omega$-continuous function. Then $f$ has a least prefixed point, which is the supremum of the ascending Kleene chain of $f$, denoted by $\text{lpp}_{\downarrow}^\mathbb{X}$. Di Wang, Jan Hoffmann, and Thomas Reps
We use the least prefixed point of \( F^\#_P \) to define the interpretation of a probabilistic program \( P \) as \( \mathcal{J}[P] = \text{lpp}_{\text{Act}_C \cup \text{An}_C \cup \text{An}_L} F^\#_P \).

The interpretation of a control-flow node \( v \) is then defined as \( \mathcal{J}[v] = \mathcal{J}[P](v) \).

### 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 concretion mapping \( γ : A \rightarrow C \), such that

- \( γ \) is monotone, i.e., for all \( Q_1, Q_2 \in A \), \( Q_1 \subseteq A Q_2 \) implies \( γ(Q_1) \subseteq γ(Q_2) \),
- \( \preceq_C \subseteq γ(\preceq_A) \) (or \( γ(\preceq_A) \subseteq \preceq_C \), resp.),
- \( \text{lpp}_C γ(\text{lpp}_A) \subseteq γ(\text{lpp}_A) \subseteq γ(\text{lpp}_C) \),
- for all \( Q_1, Q_2 \in A \), \( γ(Q_1) \cap γ(Q_2) \subseteq γ(Q_1 \cap A Q_2) \) (or \( γ(Q_1 \cap A Q_2) \subseteq γ(Q_1) \cap γ(Q_2) \), resp.),
- for all \( Q_1, Q_2 \in A \), \( γ(Q_1) \cap γ(Q_2) \subseteq γ(Q_1 \cap A Q_2) \) (or \( γ(Q_1 \cap A Q_2) \subseteq γ(Q_1) \cap γ(Q_2) \), resp.),
- for all \( Q_1, Q_2 \in A \), \( γ(Q_1) \cap γ(Q_2) \subseteq γ(Q_1 \cap A Q_2) \) (or \( γ(Q_1 \cap A Q_2) \subseteq γ(Q_1) \cap γ(Q_2) \), resp.),
- for all \( Q_1, Q_2 \in A \), \( γ(Q_1) \cap γ(Q_2) \subseteq γ(Q_1 \cap A Q_2) \) (or \( γ(Q_1 \cap A Q_2) \subseteq γ(Q_1) \cap γ(Q_2) \), resp.),
- for all \( Q_1, Q_2 \in A \), \( γ(Q_1) \cap γ(Q_2) \subseteq γ(Q_1 \cap A Q_2) \) (or \( γ(Q_1 \cap A Q_2) \subseteq γ(Q_1) \cap γ(Q_2) \), resp.),
- for all \( Q_1, Q_2 \in A \), \( γ(Q_1) \cap γ(Q_2) \subseteq γ(Q_1 \cap A Q_2) \) (or \( γ(Q_1 \cap A Q_2) \subseteq γ(Q_1) \cap γ(Q_2) \), resp.),
- A probabilistic abstraction leads to a sound analyses:

**Theorem 4.8.** Let \( C \) and \( A \) be interpretations over PMAs \( C \) and \( A \); let \( γ \) 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, \( γ(\text{act}) \subseteq C γ(\text{act}) \) (or \( γ(\text{act}) \subseteq C γ(\text{act}) \), resp.), then we have \( C[γ(P)] \subseteq C[γ(P)] \).

### 4.3 Interprocedural Analysis Algorithm

We are given a probabilistic program \( P \) and an interpretation \( A = \langle A, \text{act}_A \rangle \), where \( A = \langle M_{\text{Act}_C \cup \text{An}_C \cup \text{An}_L} \rangle \) is a PMA and \( \text{act}_A \) is a semantic function. The goal is to compute (an overapproximation of) \( A[P] = \text{lpp}_{M_{\text{Act}_C \cup \text{An}_C \cup \text{An}_L}} F^\#_P \). An equivalent way to define \( A[P] \) is to specify it as the least solution to a system of inequalities on \( \{A[v] | v \in V \} \) (where \( e \in E \) in each case):

\[
\begin{align*}
A[v] & \supseteq A[\text{act}_A] A[u] & \quad (v, (u_1)) & \quad \text{seq}[\text{act}] \\
A[v] & \supseteq A[u] \text{ for } A[u_2] & \quad (v, (u_1, u_2)) & \quad \text{cond}[\text{act}] \\
A[v] & \supseteq A[u_1] A[u_2] & \quad (v, (u_1, u_2)) & \quad \text{prob}[\text{act}] \\
A[v] & \supseteq A[u_1] A[u_2] A[u] & \quad (v, (u_1, u_2)) & \quad \text{ndet} \\
A[v] & \supseteq A[u_1] A[u_2] & \quad (v, (u_1, u_2)) & \quad \text{call}[\text{act}] \\
A[v] & \supseteq A[u_1] A[u_2] A[u] & \quad (v, (u_1)) & \quad \text{if } v = v_1 \text{ exit} \\
A[v] & \supseteq A[u_1] A[u_2] A[u] & \quad (v, (u_1)) & \quad \text{if } v = v_1 \text{ exit} \\
A[v] & \supseteq A[u_1] A[u_2] A[u] & \quad (v, (u_1)) & \quad \text{if } v = v_1 \text{ exit} \\
A[v] & \supseteq A[u_1] A[u_2] A[u] & \quad (v, (u_1)) & \quad \text{if } v = v_1 \text{ exit} \\
A[v] & \supseteq A[u_1] A[u_2] A[u] & \quad (v, (u_1)) & \quad \text{if } v = v_1 \text{ exit} \\
A[v] & \supseteq A[u_1] A[u_2] A[u] & \quad (v, (u_1)) & \quad \text{if } v = v_1 \text{ exit} \\
A[v] & \supseteq A[u_1] A[u_2] A[u] & \quad (v, (u_1)) & \quad \text{if } v = v_1 \text{ exit}
\end{align*}
\]

Note that in line 5 a call is treated as a hyper-edge with the action \( \lambda(entry, succ) \). entry \( \text{act}_A \) succ. There is no explicit return edge to match a call (as in many multi-procedure program representations, e.g., [77]); instead, each exit node is initialized with the constant \( 1 \).  

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). The analysis direction is backward, and the algorithm is similar to methods for computing summary edges in demand interprocedural-dataflow-analysis algorithms ([44, Fig. 4], [78, Fig. 10]). The algorithm uses a standard chaotic-iteration strategy (except that propagation is performed along hyper-edges instead of edges); it uses a fair iteration strategy for selecting the next edge to consider.

### 4.4 Widening

Widening is a general technique in static analysis to ensure and speed up convergence [20, 22]. 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 ordinary edges. More precisely, we consider a **dependence graph** \( G(H) = \langle N, A \rangle \) from hyper-graph \( H = \{ \langle v_i, e_i, v_{i+1}^\text{exit}, v_{i+1}^\text{exit} \rangle \}_{1 \leq i \leq n} \) by defining \( N = \bigcup_{1 \leq i \leq n} V_i \), and

\[
A = \{ (v, e) : \exists e \in E, e = \text{src}(e) \land v \in \text{Dst}(e) \} \cup \langle (v_{i+1}^\text{exit}, e) : \exists e \in E, e = \text{src}(e) \land \text{Ctrl}(e) = \text{call}[i] \rangle.
\]

We then compute a set \( W \) of widening points for \( G(H) \) via the algorithm of Bourdoncle [9, Fig. 4]. Because of the second set-former in Eqn. (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 these 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: \( \text{v}_1, \text{v}_2, \text{v}_3 \). Let \( v \in W \) be the source edge of \( e \in E \). Then the inequalities become

\[
\begin{align*}
\text{seq}[\text{act}] \quad & \quad (v, (u_1)) \\
\text{cond}[\text{act}] \quad & \quad (v, (u_1, u_2)) \\
\text{prob}[\text{act}] \quad & \quad (v, (u_1, u_2)) \\
\text{ndet} \quad & \quad (v, (u_1, u_2)) \\
\text{call}[\text{act}] \quad & \quad (v, (u_1, u_2))
\end{align*}
\]

**Observation 4.9.** Recall from Defn. 3.2 that in a probabilistic program each non-exit node has exactly one outgoing

---

4 As mentioned in §2.3, standard formulations of interprocedural dataflow analysis [52, 57, 71, 80] can be viewed as hyper-graph analyses. In that setting, one deals with hyper-graphs with constituent control-flow graphs. With PMAF, because each program 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.
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, whenever a widening operation \( a \vee b \) is performed, the property \( a \sqsubseteq \mathcal{R} b \) holds.

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

- the chain \( \{c_k\}_{k \in \mathbb{N}} \) defined by \( c_0 = a_0 \varnothing \mathcal{R} b_0 \) and \( c_{k+1} = c_k \vee c (a_{k+1} \varnothing \mathcal{R} b_{k+1}) \) is eventually stable;
- the chain \( \{c_k\}_{k \in \mathbb{N}} \) defined by \( c_0 = a_0 \varnothing \mathcal{R} b_0 \) and \( c_{k+1} = c_k \vee c (a_{k+1} \varnothing \mathcal{R} b_{k+1}) \) is eventually stable; and
- the chain \( \{c_k\}_{k \in \mathbb{N}} \) defined by \( c_0 = a_0 \cup \mathcal{R} b_0 \) and \( c_{k+1} = c_k \vee c (a_{k+1} \cup \mathcal{R} b_{k+1}) \) is eventually stable.

\[ 5 \text{ Instantiations} \]

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

\[ \text{5.1 Bayesian Inference} \]

Claret et al. [18] 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 \( \mathcal{R} \) be the set of program variables; the set of program states is \( \Omega = \mathcal{R} \rightarrow \mathbb{B} \). Note that \( \mathbb{B} \) is isomorphic to \( \mathbb{R}^{\mathcal{R}} \), and consequently, a distribution can be represented by a vector of length \( 2^{\mathcal{R}} \) of reals in \( \mathbb{R}_{[0,1]} \). (Their implementation uses Algebraic Decision Diagrams [2] to represent distributions compactly.)

The algorithm by Claret et al. is defined inductively on the structure of programs [18, 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 \( \lambda \sigma' \cdot \left( r \cdot \sum_{\sigma' \sigma \in \mathcal{R}} \mu(\sigma) + (1 - r) \cdot \sum_{\sigma' \sigma \in \mathcal{R}} \mu(\sigma) \right) \).

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 gives lower bounds on posterior distributions.

To reformulate the domain in the two- vocabulary setting needed for computing procedure summaries, we introduce \( \mathcal{R}' \), primed versions of the variables in \( \mathcal{R} \). \( \mathcal{R} \) and \( \mathcal{R}' \) 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 \( 2^{\mathcal{R}} \times 2^{\mathcal{R}} \) of reals in \( \mathbb{R}_{[0,1]} \). We define a PMA \( \mathcal{B} = \langle M_{\mathcal{B}}, \sqsubseteq_{\mathcal{B}} , \mathcal{B}, \mathcal{B}, \mathcal{B} \rangle \) as follows:

\[ M_{\mathcal{B}} \equiv 2^{\mathcal{R}} \times 2^{\mathcal{R}} \rightarrow \mathbb{R}_{[0,1]} \]

\[ a \sqsubseteq_{\mathcal{B}} b \equiv a \leq b \]
\[ a \oplus_{\mathcal{B}} b \equiv \min(a, b) \]
\[ a \otimes_{\mathcal{B}} b \equiv a \cdot b \]
\[ a \boxplus_{\mathcal{B}} b \equiv a + (1 - p) \cdot b \]
\[ a \boxtimes_{\mathcal{B}} b \equiv (s, t) \iff \begin{cases} a(s, t) & \text{if } a(s, t) \end{cases} \]

The use of pointwise min in the definition of \( a \oplus_{\mathcal{B}} b \) causes the analysis to compute procedure summaries that provide lower bounds on the posterior distributions.

\[ \text{Theorem 5.1. } \mathcal{B} \text{ is a PMA.} \]

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

We define the concretization mapping \( g_{\mathcal{B}} : M_{\mathcal{B}} \rightarrow \mathbb{R}_{[0,1]} \) as \( g_{\mathcal{B}}(a) = \langle \langle \gamma \mid \forall s', \lambda, (s, t') \rangle \geq a(s, s') \rangle \rangle \) where \( \langle C \rangle \) denotes the smallest element in \( \mathbb{R}_{[0,1]} \) such that contains \( C \).

\[ \text{Theorem 5.2. } g_{\mathcal{B}} \text{ is a prob. under-abstraction from } C \text{ to } \mathcal{B}. \]

We do not define widening operators for BI, because \( g_{\mathcal{B}} \) is an under-abstraction and our algorithm starts from the bottom element in the abstract domain, the intermediate result at any iteration is a sound answer.

\[ \text{5.2 Markov Decision Process with Rewards} \]

Analyses of finite-state Markov decision processes were originally developed in the fields of operational research and finance mathematics [75]. 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.

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

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 \text{prob}[p] or \text{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 $v$.

It is natural to extend MDPs with procedure calls and multiple procedures, to obtain recursive Markov decision processes. The set of program states is 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 $\mathcal{R} = (M_{\mathcal{R}}, \preceq_{\mathcal{R}}, \ominus_{\mathcal{R}}, \ominus_{\mathcal{R}}, \preceq_{\mathcal{R}}, \ominus_{\mathcal{R}}, \preceq_{\mathcal{R}}, \ominus_{\mathcal{R}})$ as follows:

$$
\begin{align*}
M_{\mathcal{R}} & \overset{\text{def}}{=} [0, \infty] \\
\preceq_{\mathcal{R}} & \overset{\text{def}}{=} \leq \\
\ominus_{\mathcal{R}} & \overset{\text{def}}{=} + \\
p \ominus_{\mathcal{R}} b & \overset{\text{def}}{=} p \cdot a + (1 - p) \cdot b \\
\preceq_{\mathcal{R}} & \overset{\text{def}}{=} 0 \\
\ominus_{\mathcal{R}} & \overset{\text{def}}{=} 0 \\
\preceq_{\mathcal{R}} & \overset{\text{def}}{=} \preceq_{\mathcal{R}} \\
\ominus_{\mathcal{R}} & \overset{\text{def}}{=} \ominus_{\mathcal{R}} \\
\preceq_{\mathcal{R}} & \overset{\text{def}}{=} \preceq_{\mathcal{R}} \\
\ominus_{\mathcal{R}} & \overset{\text{def}}{=} \ominus_{\mathcal{R}} \\
\preceq_{\mathcal{R}} & \overset{\text{def}}{=} \preceq_{\mathcal{R}} \\
\ominus_{\mathcal{R}} & \overset{\text{def}}{=} \ominus_{\mathcal{R}}
\end{align*}
$$

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

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

We define the concretization mapping $\gamma_I : M_{\mathcal{R}} \to \mathcal{R}$ as follows: $\gamma_I(a) = \langle \{k \mid \forall s. \int y \cdot \kappa(s, dy) \leq s + a\} \rangle$.

**Theorem 5.5.** $\gamma_R$ is a prob. over-abstraction from $C$ to $\mathcal{R}$.

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 expectation invariants obtained via linear expectation-invariant analysis (LEIA) were given in §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 [24]. 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 evaluations.

A polyhedron $P = \{ (x^T x')^T \in \mathbb{R}^n_{\geq 0} \mid A' x' + Ax \leq b \wedge D' x' + Dx = e \}$, 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 $C_P = \{ A' x' + Ax \leq b, D' x' + Dx = e \}$. 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 of the form

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

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

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

Let $\mathcal{E} \mathcal{P}$ be the set of expectation polyhedra. $\mathcal{E} \mathcal{P}$ is equipped with the same set of operations as $\mathcal{P}$.

We define the state space to be $\Omega = \mathbb{R}_+^n$. We then define a PMA $\mathcal{I}$ with a universe $M_I \overset{\text{def}}{=} \mathcal{P} \times \mathcal{E} \mathcal{P}$. An element $(P, EP) \in \mathcal{I}$ consists of (i) a set of standard constraints $P \in \mathcal{P}$, and (ii) a set of expectation constraints $EP \in \mathcal{E} \mathcal{P}$, such that $0 \cup P[\mathbb{E}[x']/x'] \supseteq EP$ holds, where $0 \overset{\text{def}}{=} \bigwedge_{i=1}^n (\mathbb{E}[x'_i] = 0)$. The latter property means that, if necessary, we can always ‘rebuild’ a pessimistic $\mathcal{E} \mathcal{P}$ component from the $\mathcal{P}$ component as $0 \cup P[\mathbb{E}[x']/x']$.\footnote{The intuition is that $P$ represents a convex overapproximation to some desired set of points; the expected value has to lie somewhere inside $0 \cup P$, where “$0 \cup \ldots$ ” is needed to account for subprobability distributions. For instance, for a nonnegative interval $[a, b]$, we must have expected $\in (0, 0] \cup [a, b]$; i.e., $0 \leq \text{expected} \leq b$.}

We define the concretization mapping $\gamma_I$ as follows:

$$
\gamma_I(P, EP) = \langle \{k \mid \forall s. \int y \cdot \kappa(s, dy) \leq s + a\} \rangle \overset{\text{def}}{=} 0 \wedge \left[ \int s' \kappa(s, ds') \overset{\text{def}}{=} EP \right].
$$

**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 $(P_1, EP_1) \subseteq_I (P_2, EP_2)$ as $P_1 \subseteq P_2 \wedge 0 \cup EP_1 \subseteq 0 \cup EP_2$.

**Composition.** For ordinary polyhedra, the composition of $P_1$ and $P_2$ can be defined as

$$
(\exists x''. C_{P_1}(x''/x') \wedge C_{P_2}(x''/x)) \Rightarrow C_{P_1 \otimes P_2},
$$

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 $\exists x''. C_{P_1}(x''/x') \wedge C_{P_2}(x''/x)$. Operationally, composition 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 $\mathbb{E}[X] = \mathbb{E}[\mathbb{E}[X \mid Y]]$, where $X$ and $Y$ are two random variables, and $\mathbb{E}[X \mid Y]$ is a conditional expectation. For instance, suppose that $EP_1$ and $EP_2$ are defined by the constraint sets $\{ \mathbb{E}(x') = x + 2 \}$ and $\{ \mathbb{E}(x') = 7x \}$, respectively. Following the renaming recipe above, we have $\mathbb{E}(x''') = x + 2$ and $\mathbb{E}(x'''/x') = 7x'$. By the tower property, we have $\mathbb{E}(x'') = \mathbb{E}(\mathbb{E}(x''/x')) = 7\mathbb{E}(x'') = 7(7x) = 7x + 14$. Operationally, the tower property allows us to compose linear expectation invariants, and eliminate the intermediate
vocabulary \( x'' \). Consequently, we define
\[
(P_1, EP_1) \otimes_I (P_2, EP_2) \overset{\text{df}}{=} (P_1 \otimes P_2, EP_1 \otimes EP_2).
\]

**Conditional-choice.** For the ordinary-polyhedron component, a conditional-choice \( \varphi \) 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
\[
(P_1, EP_1) \varphi \otimes_I (P_2, EP_2) \overset{\text{df}}{=} \{ \text{let } P = ((\varphi) \cap P_1) \cup (\neg \varphi) \cap P_2 \}
\]

in \((P_1, EP_1) \cup_P EP_2) \overset{\text{df}}{=} (P_1 \cup_P P_2, EP_1 \cup_P EP_2).

**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:

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

For the loop body, we can derive an expectation invariant \( \exists x' = y' = x = y \); however, for the entire loop this property does not hold: at the end of the loop \( x = y \) must hold, and hence \( \exists x' = y' \) 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.

\[
(P_1, EP_1) \nabla_c (P_2, EP_2) \overset{\text{df}}{=} (P_1 \nabla P_2, 0 \cup P_2[EP[x'/x']])
\]

\[
(P_1, EP_1) \nabla_n (P_2, EP_2) \overset{\text{df}}{=} (P_1 \nabla P_2, 0 \cup P_2[EP[x'/x']])
\]

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

\[
\text{let } P = (P_1 \nabla P_2) \text{ in } (P_1, EP_1 \nabla EP_2) \cup (0 \cup P[EP[x'/x']])
\]

In our experiments, we use \((P_1, EP_1) \nabla p (P_2, EP_2) \overset{\text{df}}{=} (P_1 \nabla P_2, EP_2)\), which does no extrapolation in the \( EP \) component.

**6 Evaluation**

In this Section, we first describe the implementation of PMAF, and then the instantiations introduced in §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 [19] as the implementation of fixed-point computation and Bourdoncle’s algorithm.

The plug 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 [70] 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 [45] for polyhedron operations. Most of the code in the plugins is to implement the PMAF structure of the analysis domain.
We tested our framework with Rewards. The tables contain the number of lines; whether the definition problem with
Bayesian inference and Markov decision problem with rewards on handcrafted examples. The results of the
evaluation of the two analyses are described in Tab. 2.

The tables contain 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 [84], a tool for probabilistic recursive models. We did not compare with probabilistic abstract interpretation [25] because its semantic foundation is substantially different from that of our framework—as we mentioned in §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 [2] 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 [84]), and our analysis results are consistent with the worst-case expected number of comparisons being $\Theta(n \log n)$.

binary10 is a model of randomized binary search algorithm on an array of size 10, and our analysis results are consistent with the worst-case expected number of comparisons being $\Theta(\log n)$.

The framework—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. [26] 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. 2.

<table>
<thead>
<tr>
<th>Program</th>
<th>Expectation invariants</th>
<th>#loc rec?</th>
<th>#call time</th>
</tr>
</thead>
<tbody>
<tr>
<td>2d-walk</td>
<td>$</td>
<td>x'</td>
<td>= x$, $</td>
</tr>
<tr>
<td>aggregate-rv</td>
<td>$</td>
<td>x' - j'</td>
<td>= 2x - j$, $</td>
</tr>
<tr>
<td>biased-coin</td>
<td>$</td>
<td>x'</td>
<td>\leq x + \frac{1}{2}$, $</td>
</tr>
<tr>
<td>binom-update</td>
<td>$</td>
<td>x' - n'</td>
<td>= 4x - n$, $</td>
</tr>
<tr>
<td>coupon5</td>
<td>$</td>
<td>\text{count} - i'</td>
<td>= \text{count} - i (1st)$, $</td>
</tr>
<tr>
<td>dist</td>
<td>$</td>
<td>x'</td>
<td>= x$, $</td>
</tr>
<tr>
<td>eg</td>
<td>$</td>
<td>x' + y'</td>
<td>= x + y + 3$, $</td>
</tr>
<tr>
<td>eg-tail</td>
<td>$</td>
<td>x'</td>
<td>\geq \frac{x}{2}$, $</td>
</tr>
<tr>
<td>hare-turtle</td>
<td>$</td>
<td>2h' - 5i'</td>
<td>= 2h - 5i$, $</td>
</tr>
<tr>
<td>hawk-dove</td>
<td>$</td>
<td>pib' - \text{count}'</td>
<td>= pib - \text{count}$, $</td>
</tr>
<tr>
<td>mot-ex</td>
<td>$</td>
<td>2x' - y'</td>
<td>= 2x - y$, $</td>
</tr>
<tr>
<td>recursive</td>
<td>$</td>
<td>x'</td>
<td>= x + 9$</td>
</tr>
<tr>
<td>uniform-dist</td>
<td>$</td>
<td>n'</td>
<td>\leq 2n$, $</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Program</th>
<th>#loc rec?</th>
<th>#call time</th>
</tr>
</thead>
<tbody>
<tr>
<td>compare 17</td>
<td>0</td>
<td>2.22</td>
</tr>
<tr>
<td>dice 12</td>
<td>0</td>
<td>0.02</td>
</tr>
<tr>
<td>eg1 10</td>
<td>0</td>
<td>0.02</td>
</tr>
<tr>
<td>eg1-tail 16</td>
<td>t</td>
<td>0.02</td>
</tr>
<tr>
<td>eg2 10</td>
<td>0</td>
<td>0.02</td>
</tr>
<tr>
<td>eg2-tail 16</td>
<td>t</td>
<td>0.01</td>
</tr>
<tr>
<td>recursive 14</td>
<td>r</td>
<td>0.01</td>
</tr>
<tr>
<td>binary10</td>
<td>90</td>
<td>0.03</td>
</tr>
<tr>
<td>loop 100</td>
<td>n</td>
<td>0.03</td>
</tr>
<tr>
<td>quicksort7</td>
<td>109</td>
<td>0.03</td>
</tr>
<tr>
<td>recursive 13</td>
<td>t</td>
<td>0.03</td>
</tr>
<tr>
<td>student 43</td>
<td>t</td>
<td>0.03</td>
</tr>
</tbody>
</table>

### Table 2. Top: Bayesian inference. Bottom: Markov decision problem with rewards. (Time is in seconds.)
The results of the evaluation are shown in Tab. 1, which lists the expectation invariants obtained, and the time taken by the implementation. In general, the analysis runs quickly—all the examples are processed in less than one second. The analysis time mainly depends on the number of program variables and the size of the control-flow hyper-graph.

As shown in Tab. 1, our analysis can derive nontrivial expectation invariants, e.g., relations among different program variables such as $E[x' + y'] = x + y + 3$, $E[2x' - y'] = 2x - y$. In most cases, our results are at least as precise as those in [14, 49]. Exceptions are biased-coin and uniform-dist, collected from [49], where their invariant-generation algorithm uses a template-based approach and the form of expectations can be more complicated, e.g., $[P_1] \cdot E_1 + [P_2] \cdot E_2$ where $P_1, P_2$ are linear assertions and $E_1, E_2$ are linear expressions. Nevertheless, our analysis is fully automated and applicable to general programs, while [49] requires interactive proofs for nested loops, and [14] works only for single loops.

7 Related Work

Static Analysis for Standard Programs. Our framework is an extension of interprocedural dataflow analysis [52, 57, 71, 80] 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 [21, 23], 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 [25, 67–69], which is discussed in the introduction. There is a long line of research on manual reasoning techniques for probabilistic programs [33, 48, 56, 59, 72]. The main difference to this work is that we focus on the design and implementation of automatic techniques that that rely on computing fixed points.

Other work focuses on specialized automatic analyses for specific properties. Claret et al. [18] 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 [10, 11] and martingales and stochastic invariants [16, 17]. Martingales for automatic analysis of probabilistic programs have been pioneered by Chakarov et al. [13]. Compared with existing techniques for probabilistic invariant generation [4, 13, 14, 17], the expectation-invariant analysis proposed in §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 [56] 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 [27, 46, 47, 64, 65, 82], which develop powerdomain constructions over probability distributions, but do not consider powerdomains over kernels. Borgström et al. [8] have used kernels to define the operational semantics of a probabilistic lambda calculus. The main novelty of our denotational semantics in §3.3 is that it is defined for control-flow hypergraphs, 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 [53]. Other analyses based on hypergraphs includes Möncke and Wilhelm’s [66] 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 [58]. 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 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


