

Probabilistic Program Analysis with Martingales

Aleksandar Chakarov and Sriram Sankaranarayanan
CAV'13

Report date: March 9, 2021

Introduction

- ▶ Probabilistic programs: Standard imperative program + *random value generators*
 - ▶ Branching.
 - ▶ Assignment.
- ▶ Problem: Invariant synthesis and termination checking in probabilistic settings.

Contributions

- ▶ Extend *quantitative invariants* using Azuma-Hoeffding theorem to generate probabilistic assertions.
- ▶ Define *super martingale ranking functions* (SMRF) to prove almost sure termination ($\Pr(\textit{terminates}) = 1$) of probabilistic programs.
- ▶ A constraint-based algorithm for supermartingale expression generation.

Restrictions

- ▶ Only applies to stochastic programs. (Not a demonic program with non-determinism)
- ▶ Restricted on linear expressions and systems.
- ▶ A.s. termination proving is sound but incomplete.

Motivating Examples

Example

```
1  real x = 0;  
2  real N = 500;  
3  for ( i=0; i < N; ++i )  
4      x = x + unifRand(0,1);  
5  // Prob(x \in [200,300]) ?
```

- ▶ Traditional invariant at loop exit: $0 \leq x \leq 501 \wedge i = N$
- ▶ Probabilistic assertion: $\Pr(x \in [200, 300]) \geq 0.84$

Motivating Examples

Example (Hare and Tortoise)

```
1  real h, t;  
2  // h is hare and t is tortoise  
3  h = 0; t = 30;  
4  while ( h <= t ){  
5      if (flip (0.5) )  
6          h = h + unifRand(0,10);  
7      t = t +1;  
8  } // almost sure terminate?
```

- ▶ Worst case: non-terminating.
- ▶ The expression $t - h$ decrease by 1.5 in expectation each iteration.

State and Post-Distribution

A *state* of PTS is a tuple (l, \mathbf{x}) where $l \in L$ and \mathbf{x} is a valuation of X .

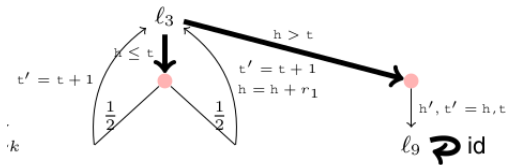
Given a transition $\tau = \langle l, \phi, f_1, \dots, f_k \rangle$, if $\mathbf{x} \models \phi$ then the result of executing τ is a *probability distribution* over post states, obtained by:

1. Choose fork f_j with probability p_j , and a vector of random variables $\mathbf{r} : (r_1, \dots, r_m)$ is drawn according to the joint distribution.
2. Update the states by computing the function $\mathbf{x}' = F_j(\mathbf{x}, \mathbf{r})$ and update l to m_j .

$$\text{POST-DISTRIB}(s, \tau), \text{POST-DISTRIB}(s)$$

Operationally, PTS is a Markov chain.

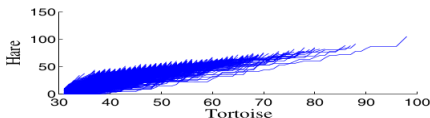
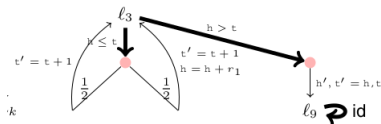
State and Post-Distribution



Sampled Executions

Definition 2 (Sample Executions). Let Π be a transition system. A sample execution σ of Π is a countably infinite sequence of states $\sigma : (\ell_0, \mathbf{x}_0) \xrightarrow{\tau_1} (\ell_1, \mathbf{x}_1) \xrightarrow{\tau_2} \dots \xrightarrow{\tau_n} (\ell_n, \mathbf{x}_n) \dots$, such that (a) (ℓ_0, \mathbf{x}_0) is the unique initial state. (b) The state $s_j : (\ell_j, \mathbf{x}_j)$ for $j \geq 0$ satisfies the guard for the transition τ_{j+1} . Note that by the no demonic restriction, τ_{j+1} is uniquely defined for each s_j . (c) Each state $s_{j+1} : (\ell_{j+1}, \mathbf{x}_{j+1})$ is a sample from $\text{POST-DISTRIB}(s_j)$.

Example



Almost Sure Termination

Definition (Termination)

Let Π be a PTS with a special *final location* l_F . l_F has only one outgoing transition id . A sampled execution σ of Π *terminates* if it eventually reaches a state (l_F, \mathbf{x}) .

Probability of terminating paths:

- ▶ For a finite syntactic path $\pi : l_0 \xrightarrow{\tau_1} l_1 \xrightarrow{\tau_2} l_2 \dots l_F$, there is a well-defined probability $\mu(\pi) \in [0, 1]$ that characterizes the probability of the path going through the locations.
- ▶ The overall probability of termination can be obtained as the sum of probability of all such finite syntactic paths.

Almost Sure Termination

The main idea to show μ on the infinite space is well-defined:

Let $\Omega = \prod_{j=1}^{\infty} \Omega_j$ and $\mathcal{F} = \prod_{j=1}^{\infty} \mathcal{F}_j$.

- ▶ At each location l_i , there is a probability space $(\Omega_i, \mathcal{F}_i, \mu_i)$.
- ▶ For a given n , a measurable cylinder can be constructed by $B_n = \{\omega \in \Omega \mid (\omega_1, \dots, \omega_n) \in B^n\}$, where $B^n = \prod_{j=1}^n A_j$, $A_j \in \mathcal{F}_j$. Assume the measure is P_n .
- ▶ Theorem of cylinder construction, a probability measure space (Ω, \mathcal{F}, P) such that $P\{\omega \in \Omega \mid (\omega_1, \dots, \omega_n) \in B^n\} = P_n(B^n)$.

Almost Sure Termination

Definition (a.s. Termination)

A PTS is said to be almost sure terminating iff the sum of probabilities of all terminating syntactic paths is 1.

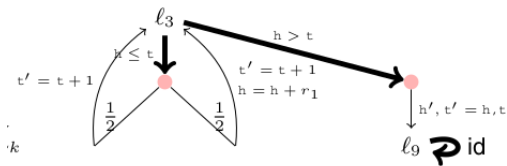
Pre-Expectation

Definition (Pre-expectation of an expression)

Let state $s : (l, \mathbf{x})$ be a state and τ be the enabled transition on s . The pre-expectation $\mathbb{E}(\mathbf{e}'|s)$ is defined as the conditional expected value of \mathbf{e}' over $\text{Post} - \text{Distrib}(s)$ as

$$\mathbb{E}_{\tau}(\mathbf{e}'|s) = \sum_{j=1}^k p_j \mathbb{E}_R(\text{pre}(\mathbf{e}', F_j))$$

Pre-Expectation



Example

$$\mathbb{E}(5t - 2h | (l_3, h, t))$$

Martingale and Supermartingale Expression

A discrete-time stochastic process $\{M_n\}$ is a countable sequence of random variables M_0, M_1, M_2, \dots where M_n is distributed based on the samples drawn from M_0, \dots, M_{n-1} . By convention, M_n denotes the random variable and m_n its sample.

Definition 4 (Martingales and Super Martingales). A process $\{M_n\}$ is a martingale iff for each $n > 0$, $\mathbb{E}(M_n | m_{n-1}, \dots, m_0) = m_{n-1}$. In other words, at each step the expected value at the next step is equal to the current value. Likewise $\{M_n\}$ is a super-martingale iff for each $n > 0$, $\mathbb{E}(M_n | m_{n-1}, \dots, m_0) \leq m_{n-1}$.

Adapting the original definition to PTS:

Definition 5 (Martingale Expressions). An expression $e[X]$ over program variables X is a martingale for the PTS Π iff for every transition $\tau : (\ell, \varphi, f_1, \dots, f_k)$ in Π and for every state $s : (\ell, \mathbf{x})$ for which τ is enabled, the pre-expectation of e equals its current state value: $\forall \mathbf{x}. \varphi[\mathbf{x}] \Rightarrow \mathbb{E}_\tau(e' | \ell, \mathbf{x}) = e$. Likewise, an expression is a super-martingale iff for each transition τ , $\forall \mathbf{x}. \varphi[\mathbf{x}] \Rightarrow \mathbb{E}_\tau(e' | \ell, \mathbf{x}) \leq e$.

From Martingale to Probabilistic Assertion

Theorem 1 (Azuma-Hoeffding Theorem). *Let $\{M_n\}$ be a super martingale such that $|m_n - m_{n-1}| < c$ over all sample paths for constant c . Then for all $n \in \mathbb{N}$ and $t \in \mathbb{R}$ such that $t \geq 0$, it follows that $\Pr(M_n - M_0 \geq t) \leq \exp\left(\frac{-t^2}{2nc^2}\right)$. Moreover, if $\{M_n\}$ is a martingale the symmetric bound holds as well: $\Pr(M_n - M_0 \leq -t) \leq \exp\left(\frac{-t^2}{2nc^2}\right)$. Combining both bounds, we conclude that for a martingale $\{M_n\}$ we obtain $\Pr(|M_n - M_0| \geq t) \leq 2 \exp\left(\frac{-t^2}{2nc^2}\right)$.*

Almost-Sure Termination

Definition (Ranking Super Martingale(RSM))

A supermartingale $\{M_n\}$ is ranking iff

- ▶ There exists $\epsilon > 0$ s.t. for all sampled paths,
 $\mathbb{E}(M_{n+1}|m_n) \leq m_n - \epsilon.$
- ▶ For all $n \geq 0$, $M_n \geq -K$ for some $K > 0$.
(Equiv. Def. For all $n \geq 0$, $M_n \geq 0$).

How a.s. Termination is Proved?

Ranking function: will finally become negative.

Ranking Supermartingale: will almost surely become negative.

How a.s. Termination is Proved?

Ranking function: will finally become negative.

Ranking Supermartingale: will almost surely become negative.

Theorem (Main result)

A ranking supermartingale with a positive initial value will a.s. become negative.

How a.s. Termination is Proved?

Ranking function: will finally become negative.

Ranking Supermartingale: will almost surely become negative.

Theorem (Main result)

A ranking supermartingale with a positive initial value will a.s. become negative.