Probabilistic Programming

Lecture #14: Proving Almost-Sure Termination

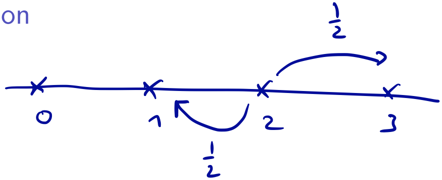
Joost-Pieter Katoen

Software Modeling and Verification Chair | RWTH AACHEN UNIVERSITY

RWTH Lecture Series on Probabilistic Programming 2018

Overview

1. Motivation
2. Proving termination of ordinary programs
3. Variant (aka: ranking) functions
4. Proving almost-sure termination



Proving almost-sure termination

- What? Termination with probability one.
- Why?
  - Termination is an elementary liveness property
  - Reachability can be encoded as termination
  - Often a prerequisite for proving correctness
- Why is it hard in practice?
  - Requires proving lower bound 1 for termination probability
  - $\underbrace{\text{Lower bounds}}_{\text{AST}}$ are harder to prove than $\underbrace{\text{upper bounds}}_{\text{positive AST}}$
  - This is especially true for null-terminating programs

Our aim

A powerful proof rule at the source code level.

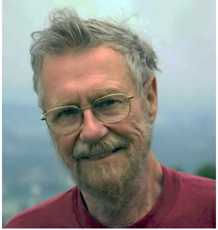
No “descend” into the underlying $\underbrace{\text{probabilistic model}}_{\text{Markov chains}}$.

Overview

1. Motivation
2. Proving termination of ordinary programs
3. Variant (aka: ranking) functions
4. Proving almost-sure termination

Termination by weakest preconditions

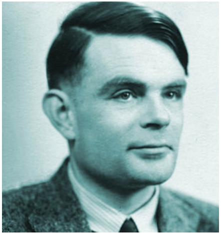
Determine $wp(P, \text{true})$ for program P and postcondition true.



Edsger Wybe Dijkstra
A Discipline of Programming
1976

How to prove termination?

Use a variant function on the program's state space
whose value — on each loop iteration — is monotonically decreasing
with respect to a (strict) well-founded relation.



Alan Mathison Turing
Checking a large routine
1949

Overview

Well-founded relation

or: Noetherian

Well-founded relation

Let $(D, \sqsubset)$ be a strict partial order. The relation $\sqsubset$ is well-founded if there is no infinite sequence $d_1, d_2, d_3, \ldots$ with $d_i \in D$ such that $d_{i+1} \sqsubset d_i$ for all $i \in \mathbb{N}$.

Examples

- $(\mathbb{N}, <)$
- $(\mathbb{R}^+, <_\varepsilon)$ for $\varepsilon > 0$ where $x <_\varepsilon y$ iff $x \leq y - \varepsilon$
- $(\mathbb{L}, <)$ for lists $\mathbb{L}$ where $\ell_1 < \ell_2$ iff $|\ell_1| < |\ell_2|$.

A Noetherian relation is also called terminating.

Variant functions

Variant function

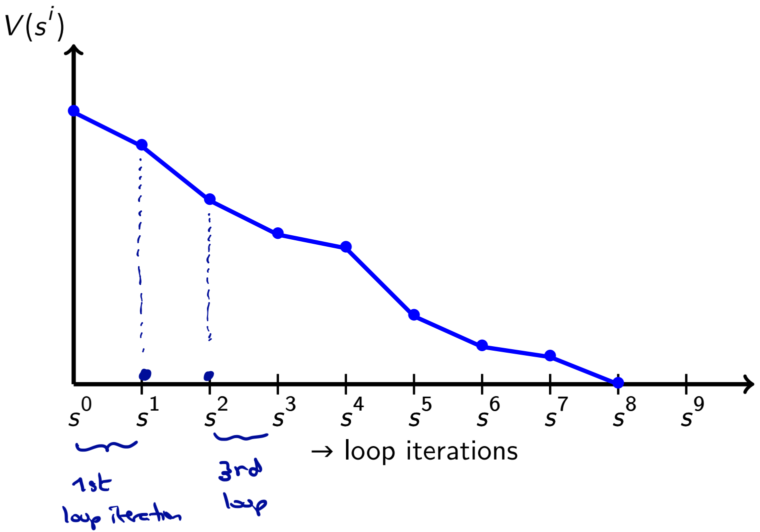
A variant (aka: ranking) function $V : \mathbb{S} \to \mathbb{R}$ for GCL-loop `while`$(G)\,P$ is a function that satisfies for every $s \in \mathbb{S}$:

1. If $s \models G$, then the execution of P on s terminates in a state t with:

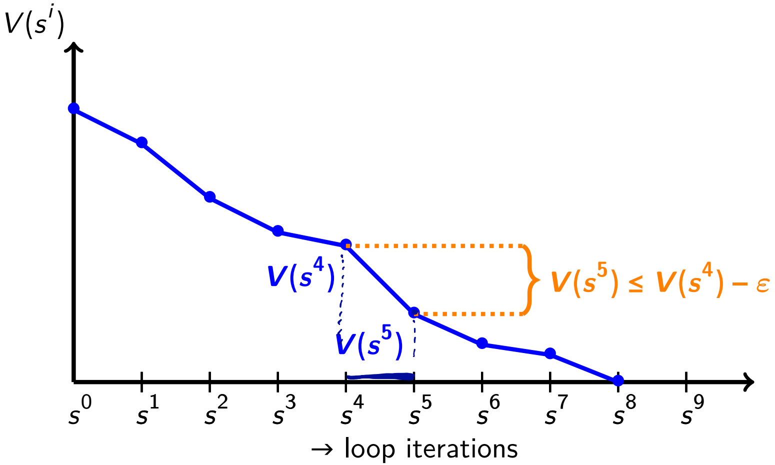
$$V(t) \;\leq\; V(s) - \varepsilon \quad \text{for some fixed } \varepsilon > 0 \text{, and}$$

2. If $V(s) \leq 0$ then $s \not\models G$.

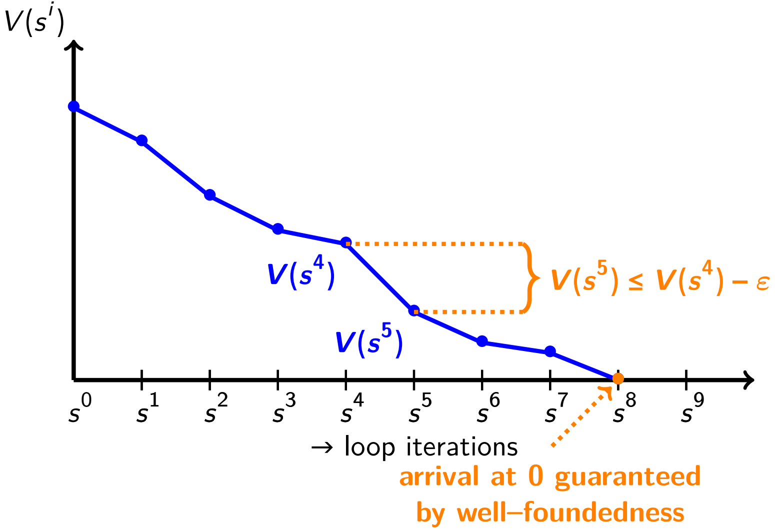
Variant (aka: ranking) functions



Variant (aka: ranking) functions



Variant (aka: ranking) functions



Termination

Every (universally) terminating loop $\texttt{while}(G)\,P$ has a variant function.

Proof.

(Sketch.)

1. As V is a variant function, from every state $s \models G$, the execution of the loop body P reaches a state t whose ranking is at least by ε smaller than s's ranking, and
2. ensures that if the ranking hits 0 or drops below, this falsifies the loop guard G and thus causes the loop to terminate.

Therefore, from every state s, no infinite chain of successor states with ever decreasing ranking can be formed by iterated execution of the loop body P without eventually falsifying the loop guard G. Since the length of such a chain is bounded by $\lceil V(s)/\varepsilon \rceil$, this ensures certain termination of the loop within at most $\lceil V(s)/\varepsilon \rceil$ loop iterations. $\square$

Examples

```
while (x > 0) { x := x-1 }
```

Ranking function $V = x$.

```
x := ... ; y := ... // x and y are positive
while (x != y) {
   if (x > y) { x := x-y } else { y := y-x }
}
```

Ranking function $V = x + y$.

McCarthy 91 function: $n \in \mathbb{N}_{>0}$

$$f(n) = \begin{cases} f(f(n+11)) & \text{if } n \leq 100 \\ n-10 & \text{if } n > 100 \end{cases}$$

$$\begin{aligned} f(99) &= f(f(110)) \\ &= f(100) \\ &= f(f(111)) \\ &= f(101) \\ &= 91 \end{aligned}$$

let

$$h(n) = \begin{cases} 91 & \text{if } n \leq 100 \\ n-10 & \text{if } n > 100 \end{cases}$$

Claim: $\boxed{\forall n: \quad f(n) = h(n)}$

imperative program

$$f(n) = g(n,1)$$

$$g(n,c) = \begin{cases} n & \text{if } c = 0 \\ g(n-10, c-1) & \text{if } c \neq 0 \land n > 100 \\ g(n+11, c+1) & \text{if } c \neq 0 \land n \leq 100 \end{cases}$$

lexigraphic well-founded order:

let $(D_1, \sqsubset_1)$ $(D_2, \sqsubset_2)$ well-founded

let $\sqsubset \subseteq (D_1 \times D_2) \times (D_1 \times D_2)$

$(d_1, d_2) \sqsubset (e_1, e_2)$ iff

$(\exists i \in \{1,2\}.\ d_i \sqsubset_i e_i \wedge$

$\forall j < i.\ d_j = e_j)$

Claim: $(10c - n + 90, n)$ is a lexicographic order for M91 program (imperative)

Theorem:

If a program has a lexicographic order, then it terminates (on all inputs).

Ranking functions for probabilistic programs

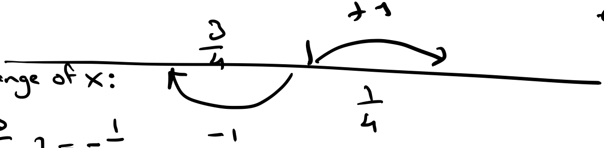
```
while (x > 0) {
    { x := x-1 } [1/2] { skip }

}
```

Ranking function $V = x$ does not guarantee to decrease x.

But every loop iteration decreases x "in expectation".

expected change of x is 0

biased rw:



expected change of x:

$\frac{1}{4} \cdot 1 - \frac{3}{4} \cdot 1 = -\frac{1}{2}$

A proof rule for positive almost-sure termination

Proving positive almost-sure termination **[Chakarov *et al.*, 2013]**

Let $\mathtt{while}(G)\, P$ be a loop where P terminates universally certainly (e.g., P is loop-free), and let $I \in \mathbb{E}$ be a ranking super-invariant of the loop w.r.t. expectation $\mathbf{0}$, i.e., $I \leq \infty$ and for some constants ε and K with $0 < \varepsilon < K$ it holds:

$$[\neg G] \cdot I \leq K \quad \text{and} \quad [G] \cdot K \leq [G] \cdot I + [\neg G] \quad \text{and} \quad \Phi(I) \leq [G] \cdot (I - \varepsilon).$$

loop iteration terminates

characteristic wp-function of the loop

$$\phi(X) = [G] \cdot wp(P, X) + [\neg G] \cdot 0$$

A proof rule for positive almost-sure termination

Proving positive almost-sure termination [Chakarov *et al.*, 2013]

Let $\texttt{while}(G)\,P$ be a loop where P terminates universally certainly (e.g., P is loop-free), and let $I \in \mathbb{E}$ be a ranking super-invariant of the loop w.r.t. expectation $\mathbf{0}$, i.e., $I \preccurlyeq \infty$ and for some constants ε and K with $0 < \varepsilon < K$ it holds:

$$\underbrace{[\neg G] \cdot I \leq K}_{1} \quad \text{and} \quad \underbrace{[G] \cdot K \leq [G] \cdot I + [\neg G]}_{2} \quad \text{and} \quad \underbrace{\Phi(I) \leq [G] \cdot (I - \varepsilon)}_{3}.$$

Then: $\texttt{while}(G)\,P$ terminates universally positively almost surely.

Example

On the black board.

P :: while $(x>0)$ { x-- [$\frac{1}{2}$] skip }

$$\Phi_0(X) = [x>0] \cdot \frac{1}{2}\left(X(x := x-1) + X\right)$$

Claim: $I = [x \geq -1] \cdot x + 1$ is a ranking superinvariant.

Proof:

① $\underbrace{[x \leq 0]}_{\neg G} \cdot I = [x \leq 0]\left([x \geq -1] \cdot x + 1\right)$

$\leq 1 = k$ — choose e.g. $k = 1$

② $[G] \cdot k \leq [G] \cdot I + [\neg G]$?

$\Leftrightarrow [x>0] \cdot 1 \leq [x>0](x+1) + [x \leq 0]$

$\Leftrightarrow \leq [x>0]\left([x \geq -1] \cdot x + 1\right) + [x \leq 0]$

$\Leftrightarrow = [x>0] \cdot I + [x \leq 0]$

(3) $\Phi_0(I) \leq [G] \cdot (I - \varepsilon)$?

$\Phi_0(I) =$
$$[x > 0] \cdot \tfrac{1}{2} \left(I(x := x-1) + I \right)$$

$$= \quad (* \ I = [x \geq -1] \cdot x + 1 \ *)$$

$$\ldots$$

$$[x>0] \cdot \Big(\underbrace{[x>0] \cdot x + 1}_{= I} \ \underbrace{- \tfrac{1}{2}}_{= \varepsilon} \Big)$$

$$= [x>0] \cdot (I - \varepsilon)$$

for $\varepsilon = \frac{1}{2}$

Overview

AST by weakest preconditions

Determine $wp(P, \mathbf{1})$ for program P and postcondition $\mathbf{1}$.

Dexter Kozen
A probabilistic PDL
1983

A zero-one law for termination

A zero-one law for termination

$[I] \leq \Phi([I])$

Zero-one law for probabilistic termination

Let $I \in \mathbb{P}$ such that $[I]$ is a wp-subinvariant of $\mathtt{while}(G)\,P$ with respect to post-expectation $[I]$. Furthermore, let $\varepsilon > 0$ a constant such that:

$$\varepsilon \cdot [I] \leq \underbrace{wp(\mathtt{while}(G)\,P, \mathbf{1})}_{\text{termination probability of while}(G)\,P} .$$

A zero-one law for termination

Zero-one law for probabilistic termination

Let $I \in \mathbb{P}$ such that $[I]$ is a wp-subinvariant of $\texttt{while}(G)\, P$ with respect to post-expectation $[I]$. Furthermore, let $\varepsilon > 0$ a constant such that:

$$\varepsilon \cdot [I] \;\leq\; wp(\texttt{while}(G)\, P, \mathbf{1}) \;.$$

Then:

$$\boxed{[I] \;\leq\; wp(\texttt{while}(G)\, P, (\neg G \wedge I)) \;.}$$

A zero-one law for termination

Zero-one law for probabilistic termination

Let $I \in \mathbb{P}$ such that $[I]$ is a wp-subinvariant of $\texttt{while}(G)\,P$ with respect to post-expectation $[I]$. Furthermore, let $\varepsilon > 0$ a constant such that:

$$\epsilon \cdot [I] \;\leq\; wp(\texttt{while}(G)\,P, \mathbf{1})\;.$$

Then:

$$[I] \;\leq\; wp(\texttt{while}(G)\,P, (\neg G \wedge I))\;.$$

Proof.

On the black board. □

related to "total correctness rule"
in lecture 8+9

Slide 27, lec 8+9:

let $f \in \mathbb{E}$ with $f \leq k$ for some $k \in \mathbb{N}$

$J \in \mathbb{E}$, k-bounded

$$I = [\neg G] \cdot f + [G] \cdot J$$

and I is a wp-subinvariant of while (G) P
w.r.t. f

Then:

$\varepsilon \cdot I \leq wp(\text{while}(G)P, 1)$ for some $\varepsilon > 0$

$$\Longrightarrow \quad I \leq wp(\text{While}(G)P, f).$$

Proof of 0-1 law for termination:

instantiate the theorem above with:

$$f = [\neg G \wedge I]$$

$$J = [I]$$

then $[\neg G] \cdot f + [G] \cdot [I]$ is a
wp-subinvariant of while (G) P wrt f.

A zero-one law for termination

Zero-one law for probabilistic termination

Let $I \in \mathbb{P}$ such that $[I]$ is a wp-subinvariant of $\texttt{while}(G)\,P$ with respect to post-expectation $[I]$. Furthermore, let $\varepsilon > 0$ a constant such that:

$$\epsilon \cdot \cancel{[I]} \leq wp(\texttt{while}(G)\,P, \mathbf{1}) .$$

how to find this termination probability?

Then:

$$1 \quad \cancel{[I]} \overset{=}{\leq} wp(\texttt{while}(G)\,P, (\neg G \land \cancel{I})) .$$

Proof.

On the black board. □

A special case is obtained for invariant I equals true.

A large body of existing works

Hart/Sharir/Pnueli: Termination of Probabilistic Concurrent Programs. POPL 1982

Bournez/Garnier: Proving Positive Almost-Sure Termination. RTA 2005

McIver/Morgan: Abstraction, Refinement and Proof for Probabilistic Systems. 2005

Esparza *et al.*: Proving Termination of Probabilistic Programs Using Patterns. CAV 2012

Chakarov/Sankaranarayanan: Probabilistic Program Analysis w. Martingales. CAV 2013

Fioriti/Hermanns: Probabilistic Termination: Soundness, Completeness, and Compositionality. POPL 2015

Chatterjee *et al.*: Algorithmic Termination of Affine Probabilistic Programs. POPL 2016

Agrawal/Chatterjee/Novotný: Lexicographic Ranking Supermartingales. POPL 2018

. . . . . .

A large body of existing works

Hart/Sharir/Pnueli: Termination of Probabilistic Concurrent Programs. POPL 1982

Bournez/Garnier: Proving Positive Almost-Sure Termination. RTA 2005

McIver/Morgan: Abstraction, Refinement and Proof for Probabilistic Systems. 2005

Esparza *et al.*: Proving Termination of Probabilistic Programs Using Patterns. CAV 2012

Chakarov/Sankaranarayanan: Probabilistic Program Analysis w. Martingales. CAV 2013

Fioriti/Hermanns: Probabilistic Termination: Soundness, Completeness, and Compositionality. POPL 2015

Chatterjee *et al.*: Algorithmic Termination of Affine Probabilistic Programs. POPL 2016

Agrawal/Chatterjee/Novotný: Lexicographic Ranking Supermartingales. POPL 2018

. . . . . .

Key ingredient: super- (or some form of) martingales

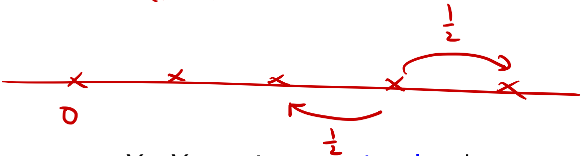
On super-martingales

while $(x>0)$ $\{x-- \; [\frac{1}{2}] \; x++\}$

ranking function

$V = x$

(is a random variable!)



A stochastic process $X_1, X_2, \ldots$ is a martingale whenever:

$$\mathbb{E}(X_{n+1} \mid X_1, \ldots, X_n) \;=\; X_n$$

It is a super-martingale whenever:

$$\mathbb{E}(X_{n+1} \mid X_1, \ldots, X_n) \;\leq\; X_n$$

$X_1, X_2, X_3 \ldots$

$1 \quad \frac{1}{2} \quad \frac{1}{4} \quad \frac{1}{8} \quad \frac{1}{16} \quad \frac{1}{32} \ldots$

A historical perspective

A countable Markov process is "non-dissipative"
if almost every infinite path eventually enters
— and remains in — positive recurrent states.

A sufficient condition for being non-dissipative is:

$$\sum_{j \geq 0} j \cdot p_{ij} \;\leq\; i \qquad \text{for all states } i$$

F. Gordon Foster	
Born	24 February 1921 Belfast, United Kingdom
Died	20 December 2010 (aged 89) Dublin, Ireland
Nationality	Irish
Known for	Foster's theorem
Scientific career	
Doctoral advisor	David George Kendall

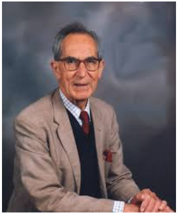
Frederic Gordon Foster
Markoff chains with an enumerable number of states
and a class of cascade processes
1951

Kendall's variation

A Markov process is non-dissipative if for some function $V : \Sigma \to \mathbb{R}$:

$$\sum_{j \geq 0} V(j) \cdot p_{ij} \;\leq\; V(i) \qquad \text{for all states } i$$

and for each r there are finitely many states i with $V(i) \leq r$



David George Kendall
On non-dissipative Markoff chains
with an enumerable infinity of states
1951

On positive recurrence

Every irreducible positive recurrent Markov chain is non-dissipative.

A Markov process is positive recurrent iff there is a Lyapunov function $V : \Sigma \to \mathbb{R}_{\geq 0}$ with for finite $F \subseteq \Sigma$ and $\varepsilon > 0$:

$$
\begin{array}{lcll}
\sum_j V(j) \cdot p_{ij} & < & \infty & \text{for } i \in F\text{, and} \\
\sum_j V(j) \cdot p_{ij} & < & V(j) - \varepsilon & \text{for } i \notin F.
\end{array}
$$

Markov Chains pp 167-193 | Cite as

Lyapunov Functions and Martingales

Authors   Authors and affiliations

Pierre Brémaud

Pierre Brémaud 1999

Frederic Gordon Foster
On the stochastic matrices associated with certain queuing processes
1953

Proving almost-sure termination

variant function

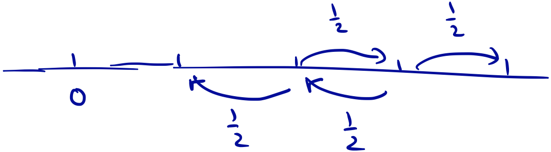
$V : S \longrightarrow \mathbb{R}_{\geq 0}$

The symmetric random walk:

```
while (x > 0) { x := x-1 [0.5] x := x+1 }
```

$V = x$

random variable



expected decrease of V on each iteration

$$\mathbb{E}(\Delta V) = \frac{1}{2} \cdot -1 + \frac{1}{2} \cdot 1$$
$$= 0$$

Proving almost-sure termination

The symmetric random walk:

```
while (x > 0) { x := x-1 [0.5] x := x+1 }
```

Is out-of-reach for many proof rules.

A loop iteration decreases x by one with probability $1/2$

V decrease

= 1

Proving almost-sure termination

The symmetric random walk:

```
while (x > 0) { x := x-1 [0.5] x := x+1 }
```

Is out-of-reach for many proof rules.

A loop iteration decreases x by one with probability $1/2$

This observation is enough to witness almost-sure termination!

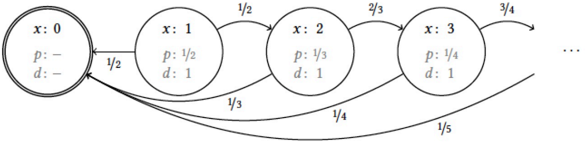
random variable $V = y$

decrease $d(y)$

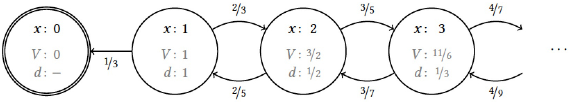
probability $p(y)$

Do these programs almost surely terminate?

```
while (x > 0) {
  p := 1/(x+1);
  x := 0 [p] x++}
```




```
while (x > 0) {
  p:= x/(2*x+1);
  x-- [p] x++}
```



Proving almost-sure termination

Goal: prove a.s.–termination of `while(G) P`

Proving almost-sure termination

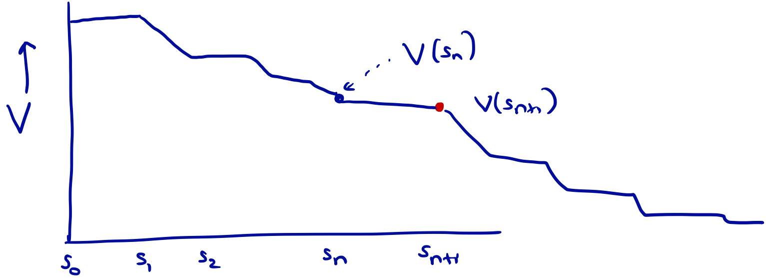
V is a random variable

$\$ \longrightarrow \mathbb{R}_{\geq 0}$

Goal: prove a.s.–termination of `while(G) P`

Ingredients:

- A supermartingale V mapping states onto non-negative reals
  - $\mathbb{E}\{V(s_{n+1}) \mid V(s_0), \ldots, V(s_n)\} \leq V(s_n)$ supermartingale
  - Running body `P` on state $s \models$ `G` does not increase $\mathbb{E}(V(s))$
  - Loop iteration ceases if $V(s) = 0$



Proving almost-sure termination

two ingredients

$p: \mathbb{R}_{\geq 0} \to [0,1]$

$d: \mathbb{R}_{\geq 0} \to \mathbb{R}_{>0}$

value of V

Goal: prove a.s.–termination of `while(G) P`

Ingredients:

- A supermartingale V mapping states onto non-negative reals
  - $\mathbb{E}\{V(s_{n+1}) \mid V(s_0), \ldots, V(s_n)\} \leq V(s_n)$
  - Running body `P` on state $s \models$ `G` does not increase $\mathbb{E}(V(s))$
  - Loop iteration ceases if $V(s) = 0$
- ...... and a progress condition: on each loop iteration in s^i
  - $V(s^i) = v$ decreases by $\geq d(v)$ with probability $\geq p(v)$
  - with antitone p ("probability") and d ("decrease") on V's values

$v \leq w$ implies $p(w) \leq p(v)$

$d(w) \leq d(v)$

Proving almost-sure termination

$d: \mathbb{R}_{\geq 0} \to \mathbb{R}_{>0}$

$V: \mathbb{S} \to \mathbb{R}_{\geq 0}$

$p: \mathbb{R}_{\geq 0} \to (0,1]$

Goal: prove a.s.–termination of `while(G) P`

Ingredients:

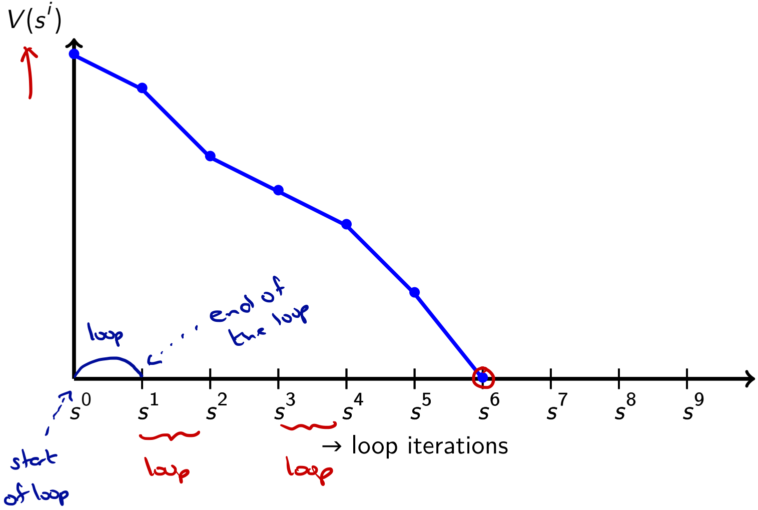
- A supermartingale V mapping states onto non-negative reals
  - $\mathbb{E}\{V(s_{n+1}) \mid V(s_0), \ldots, V(s_n)\} \leq V(s_n)$
  - Running body `P` on state $s \models$ `G` does not increase $\mathbb{E}(V(s))$
  - Loop iteration ceases if $V(s) = 0$
- ...... and a progress condition: on each loop iteration in s^i
  - $V(s^i) = v$ decreases by $\geq d(v)$ with probability $\geq p(v)$
  - with antitone p (“probability”) and d (“decrease”) on V's values

Then: `while(G) P` **a.s.-terminates on every input**

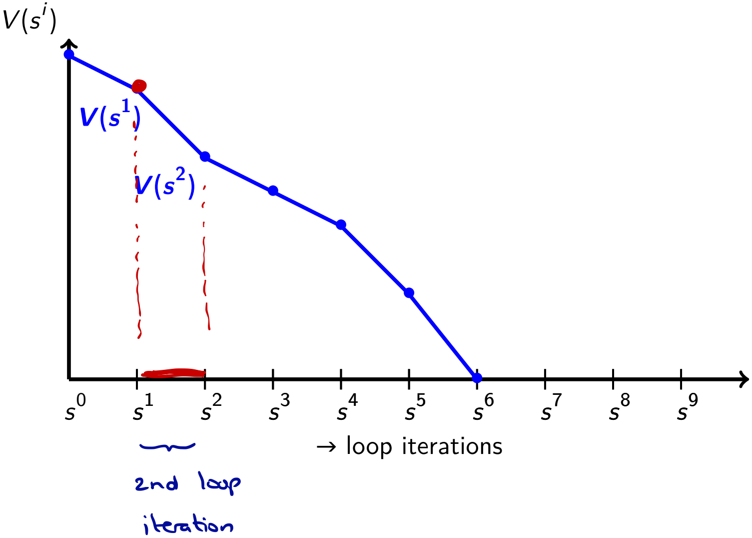
monotone $x \leq y \longrightarrow f(x) \leq f(y)$

antitone $x \leq y \longrightarrow f(x) \geq f(y)$

Proving almost-sure termination



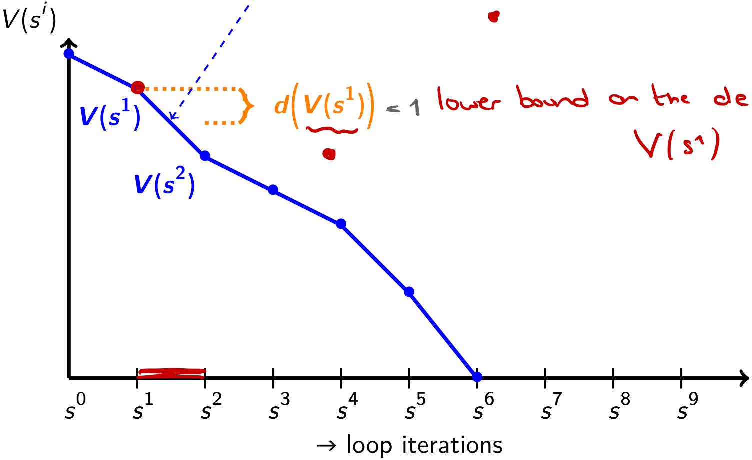
Proving almost-sure termination



random walk

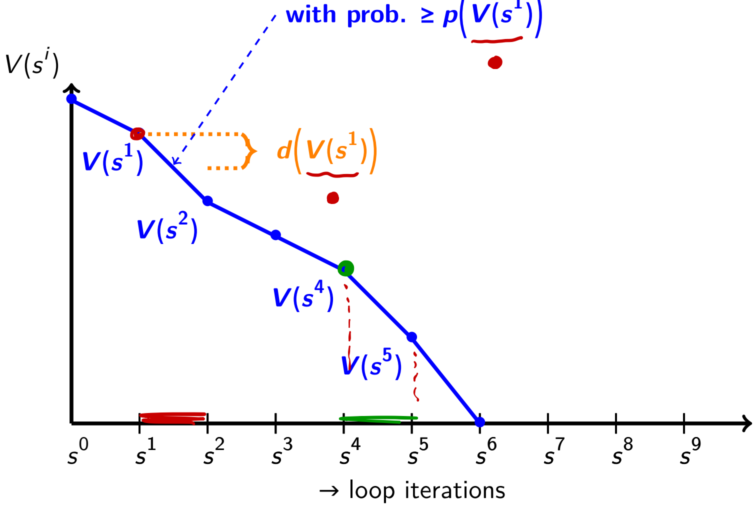
Proving almost-sure termination

with prob. $\geq p(\underbrace{V(s^1)}_{\bullet}) = \frac{1}{2}$

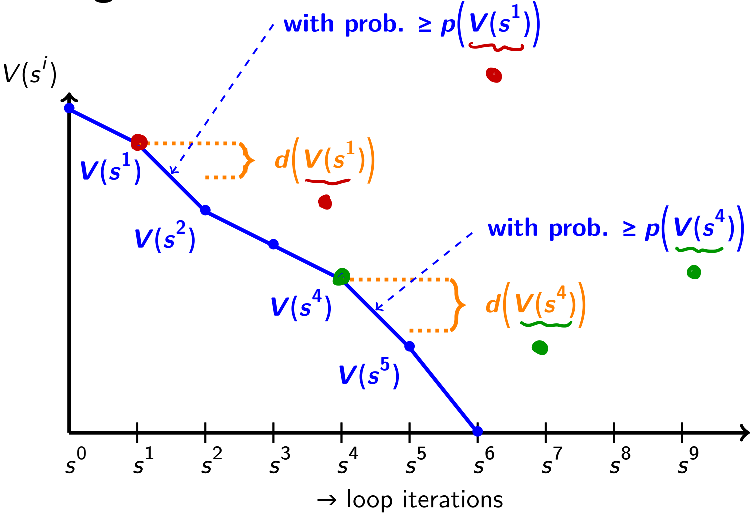


lower bound on the decrease of $V(s^1)$

Proving almost-sure termination

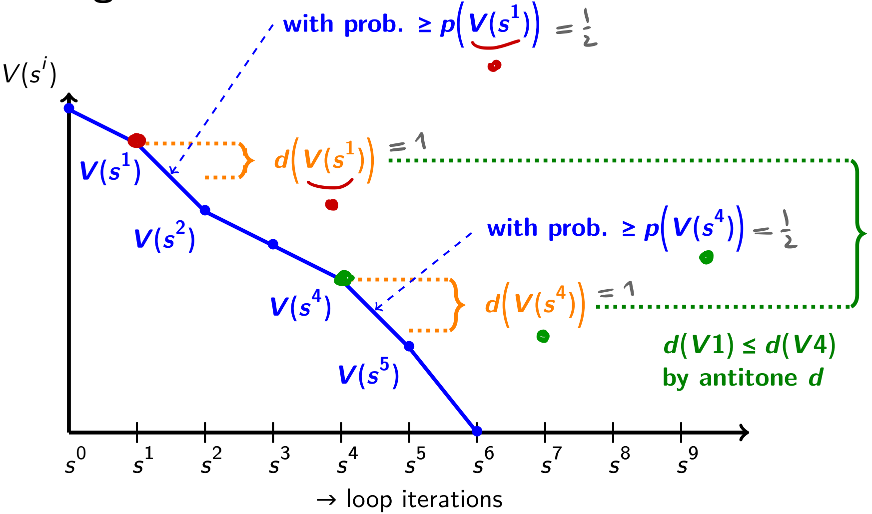


Proving almost-sure termination

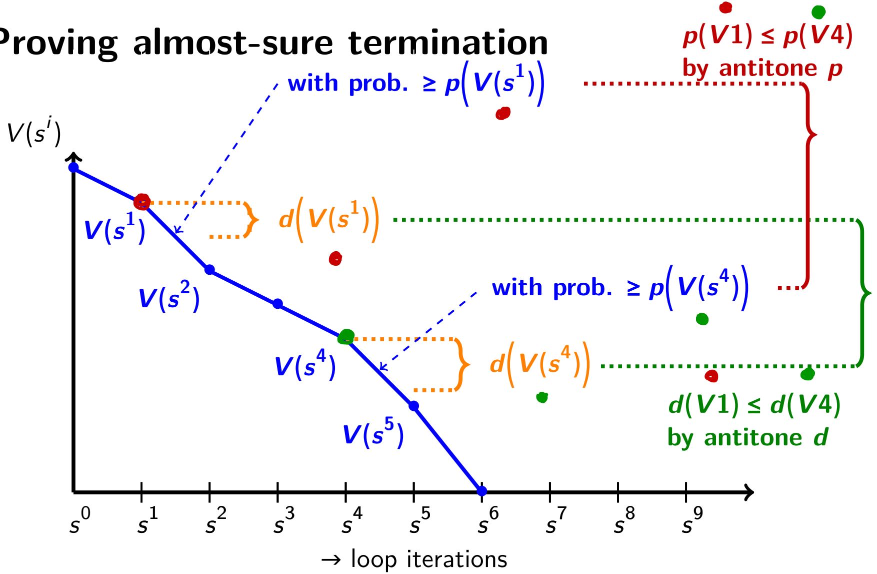


random walk

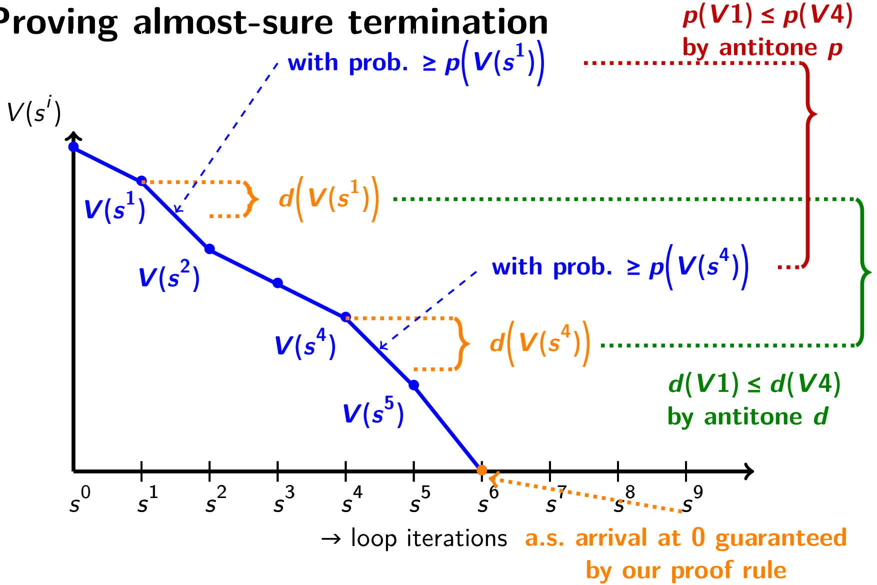
Proving almost-sure termination



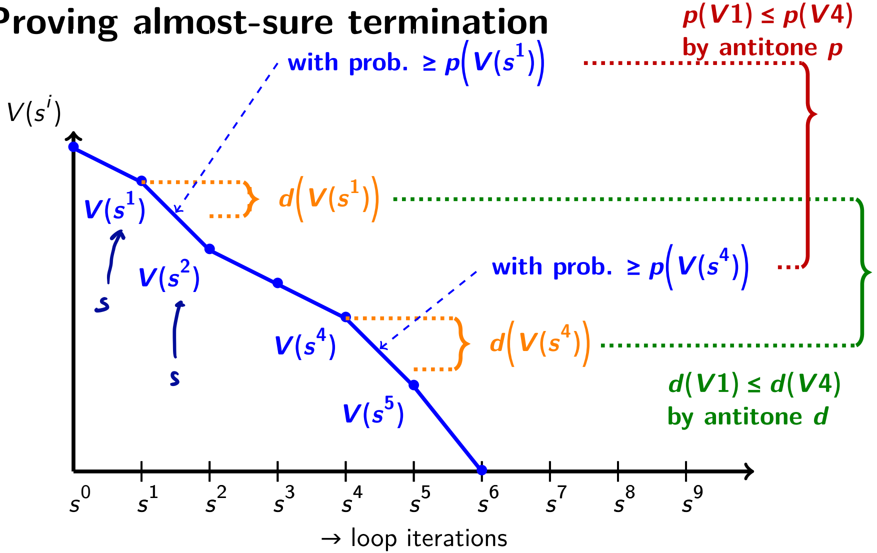
Proving almost-sure termination



Proving almost-sure termination



Proving almost-sure termination



The closer to termination, the more V decreases and this becomes more likely

I = true

The formal proof rule for almost-sure termination

Proof rule for almost-sure termination [McIver *et al.*, 2018]

Let $I \in \mathbb{P}$, (variant) function $V : \mathbb{S} \to \mathbb{R}_{\geq 0}$, (probability) function $p : \mathbb{R}_{\geq 0} \to (0, 1]$ be antitone, (decrease) function $d : \mathbb{R}_{\geq 0} \to \mathbb{R}_{>0}$ be antitone. If:

1. $[I]$ is a wp-subinvariant of $\texttt{while}(G)\, P$ w.r.t. $[I]$
2. $V = 0$ indicates termination, i.e. $[\neg G] = [V = 0]$
3. V is a super-invariant of $\texttt{while}(G)\, P$ w.r.t. V
4. V satisfies the progress condition: start state of P

wp-characteristic function of the loop

$\Phi(V) \leq V$

function composition

$$(p \circ V) \cdot [G] \cdot [I] \;\leq\; \lambda s.\, wp(P, [V \leq V(s) - d(V(s))])(s)$$

Then: the loop $\texttt{while}(G)\, P$ terminates from any state s satisfying the invariant I, i.e.,

$$\underbrace{[I]}_{=1} \;\leq\; wp(\texttt{while}(G)\, P, \mathbf{1})\ .$$

if I = true

The symmetric random walk

- Recall:

```
while (x > 0) { x := x-1 [0.5] x := x+1 }
```

The symmetric random walk

- Recall:

```
while (x > 0) { x := x-1 [0.5] x := x+1 }
```

- Witnesses of almost-sure termination:
  - $V = x$
  - $p(v) = 1/2$ and $d(v) = 1$

I = true

The symmetric random walk

- Recall:

```
while (x > 0) { x := x-1 [0.5] x := x+1 }
```

- Witnesses of almost-sure termination:
  - $V = x$
  - $p(v) = 1/2$ and $d(v) = 1$

That's all you need to prove almost-sure termination!

$I = \text{true} \qquad V = x \qquad p = \frac{1}{2} \qquad d = 1$

$\text{while } (x > 0) \ \{ x{-}{-} \ [\tfrac{1}{2}] \ x{+}{+} \}$

(0) p and d are antitone. Trivial.

(1) I is a wp-subinvariant. Trivial.

(2) $[\neg G] = [V = 0]$ Trivial.

(3) $\Phi(V) \leq V$? $\qquad V = x$

iff

$$[x \leq 0] \cdot \overset{V}{x} + [x > 0] \cdot wp(\text{body}, \overset{V}{x}) \leq x$$

iff

$$[x \leq 0] \cdot x + [x > 0] \cdot \frac{1}{2}(x - 1 + x + 1) \leq x$$

iff

$$\underbrace{[x \leq 0] \cdot x} + \underbrace{[x > 0]\, x} \leq x$$

iff

$x \leq x$. True.

④ $(p \circ V) \cdot [G] \leq \lambda s.\ wp(body, [V \leq V(s) - \underbrace{d(V(s))}_{1}])(s)$

$\Leftrightarrow \underbrace{\left(\frac{1}{2} \circ x\right)}_{=\frac{1}{2}} \cdot [x > 0] \leq \lambda s.\ wp(body, [x \leq x(s) - 1])(s)$

$\Leftrightarrow \frac{1}{2} \cdot [x > 0] \leq$

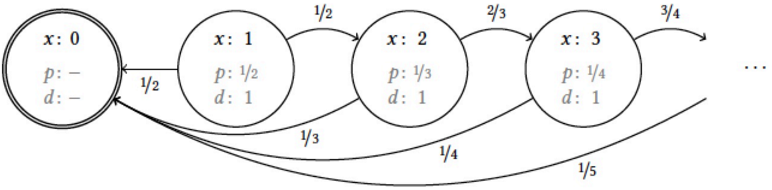
$\lambda s. \left(\frac{1}{2} \cdot \left([x-1 \leq \overset{= x}{x(s)} - 1] + [x+1 \leq \overset{= x}{x(s)} - 1] \right) \right)(s)$

$\Leftrightarrow \frac{1}{2} \cdot [x > 0] \leq \frac{1}{2} \left(\underbrace{[x-1 \leq x-1]}_{1} + \underbrace{[x+1 \leq x-1]}_{0} \right)$

$\Leftrightarrow \frac{1}{2} \cdot [x > 0] \leq \frac{1}{2}(1 + 0)$

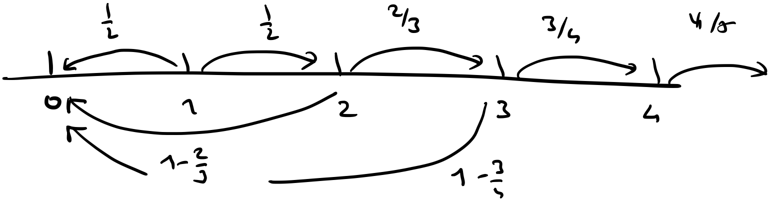
$\Leftrightarrow \frac{1}{2} \cdot [x > 0] \leq \frac{1}{2}$.

The escaping spline

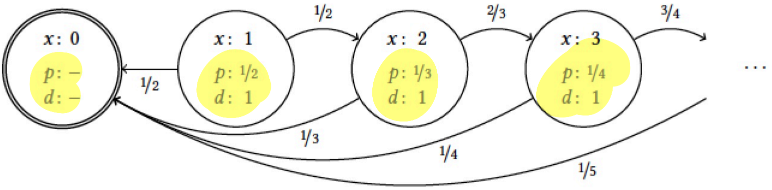


- Consider the program:

```
while (x > 0) { p := 1/(x+1); x := 0 [p] x++}
```



The escaping spline

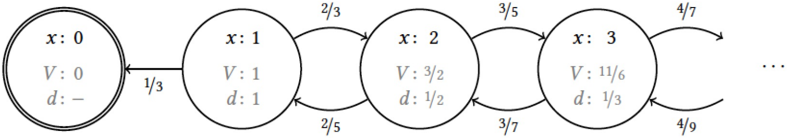


- Consider the program:

```
while (x > 0) { p := 1/(x+1); x := 0 [p] x++}
```

- Witnesses of almost-sure termination:
  - $V = x$
  - $p(v) = \frac{1}{v+1}$ and $d(v) = 1$

A symmetric-in-the-limit random walk



- Consider the program:

```
while (x > 0) { p := x/(2*x+1) ; x-- [p] x++ }
```

$I = \text{true}$ $\quad V = x$ $\quad d(v) = 1$ $\quad p(v) = \frac{1}{v+1}$

⓪ p and d are antitone. Trivial

while $(x>0)$ {
$x := 0$ [...] $\frac{1}{x+1}$
$x{+}{+}$

① true is wp-subinv. Trivial

② $[\neg G] = [V=0]$. Trivial

③ $\Phi(v) \leq V$

$$\Leftarrow \underbrace{[x \leq 0]}_{\neg G} \cdot x + [x>0] \; wp(\text{body}, x) \leq x$$

$$\Leftrightarrow [x \leq 0] \cdot x + [x>0] \cdot \Big(\underbrace{\frac{1}{x+1}}_{\text{"escape"}} \cdot 0 + \Big(1 - \frac{1}{x+1}\Big)(x+1) \Big) \leq x$$

....

$x \leq x$

4 progress condition

$$(p \circ V) \cdot [G] \le \lambda s.\, wp(body, [V \le V(s) - d(V(s))])(s)$$

$$\Leftrightarrow \; (\underbrace{\lambda v. \frac{1}{v+1}}_{=p} \circ \underbrace{x}_{=V}) \cdot \underbrace{[x>0]}_{G} \le$$

$$\lambda s. (body, [\overset{x}{V} \le V(s) - 1])(s)$$

$$\Leftrightarrow \; \frac{1}{x+1} \cdot [x>0] \le$$

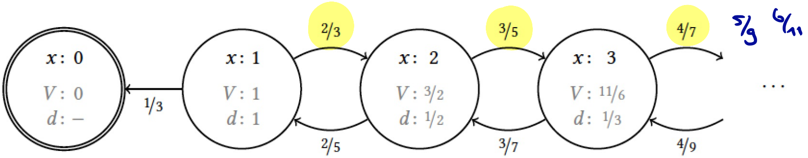
$$\lambda s \left(\frac{1}{x+1} [0 \le x(s) - 1] + \frac{x}{x+1} [x+1 \le x(s) - 1] \right)(s)$$

$$\Leftrightarrow$$

$$\frac{1}{x+1} \cdot [x>0] \le \frac{1}{x+1} \cdot \underbrace{[0 \le x-1]}_{x>0} + \underbrace{\frac{x}{x+1} \cdot \underbrace{[x+1 \le x-1]}_{=0}}_{=0}$$

$$\Leftrightarrow \; \frac{1}{x+1} \cdot [x>0] \le \frac{1}{x+1} [x>0].$$ True.

A symmetric-in-the-limit random walk



- Consider the program:

```
while (x > 0) { p := x/(2*x+1) ; x-- [p] x++ }
```

- Witnesses of almost-sure termination:
  - $V = H_x$, where H_x is x-th Harmonic number $1 + 1/2 + \ldots + 1/x$
  - $p(v) = 1/3$ and $d(v) = \begin{cases} 1/x & \text{if } v > 0 \text{ and } H_{x-1} < v \leq H_x \\ 1 & \text{if } v = 0 \end{cases}$

P :: while $(x>0)$ { $x--$ $\left[\frac{x}{2x+1}\right]$ $x++$ }

$I =$ true , $V = H_x$ $\quad d(v) = \begin{cases} \frac{1}{x} & \text{if } v>0 \text{ and } v \in (H_{x-1}, H_x] \\ 1 & \text{if } v=0 \end{cases}$

$p = \frac{1}{3}$

(0) p, d are antitone . Trivial.

(1) I . Trivial

(2) $[V=0] = [x \leq 0]$. Trivial.

(3) $\Phi(V) \leq V$

$\Leftarrow [x\leq 0]\cdot H_x + [x>0]\cdot wp(\text{body}, H_x) \leq H_x$

$\Leftarrow [x\leq 0]\cdot H_x + [x>0]\cdot\left(\frac{x}{2x+1}\cdot H_{x-1} + \left(1-\frac{x}{2x+1}\right)\cdot H_{x+1}\right) \leq H_x$

$\Leftarrow [x\leq 0]\cdot H_x + [x>0]\cdot\left(\frac{x}{2x+1}\cdot\left(H_x - \frac{1}{x}\right) + (\ldots)\cdot\left(H_x + \frac{1}{x+1}\right)\right)$

$\leq H_x$

.....

$\Leftarrow \underbrace{[x\leq 0]\cdot H_x + [x>0]\cdot H_x}_{= H_x} \leq H_x$

(4) $(p \circ V)\cdot[G] \leq \lambda s. \ldots [V \leq V(s) - \underbrace{d(V(s))}_{\frac{1}{H_{x(s)}}}]$

$\left(\frac{1}{3} \circ H_x\right)\cdot[x>0] \leq \lambda s.\ wp(\text{body}$

Expressiveness

This proof rule covers many a.s.-terminating programs
that are out-of-reach for almost all existing proof rules