PROBABILISTIC TERMINATION 6

Termination is one of the most fundamental liveness properties of probabilistic programs and is naturally an active area of research [HSP83; SPH84; APZ03; BG05; BG06; SS11; EGK12; CS13; FH15; KK15b; CFG16; Cha+16; CNZ17; CF17; LG17; ACN18; McI+18]. Already the very notion of *termination* is much more nuanced and subtle for probabilistic programs than it is for nonprobabilistic ones. Whereas a deterministic program either terminates on a given input with *certainty* or not at all, the following two forms of *probabilistic termination* are mainly considered in the literature:

- ✧ *Almost–sure termination:* Termination with probability 1.
- ✧ *Positive almost–sure termination:* Termination in finite expected time.

In this chapter, we survey and discuss proof rules for proving the different forms of probabilistic termination. In particular, we present a more recent proof rule for proving almost–sure termination of loops that do not necessarily terminate in finite expected time — a notoriously difficult task in probabilistic program verification.

Let us first develop the differences between different forms of termination. As a first example, consider the probabilistic program

$$\begin{array}{l}\texttt{while}(x>0)\{\\ \quad \{x:=x-1\}\,[1/2]\,\{x:=x-2\}\\ \}\,.\end{array}$$

This program terminates *universally certainly*, meaning that every possible computation path of the program terminates. And indeed, even though there are probabilistic choices and the time until termination depends on the outcome of the coin tosses, *every* possible computation path of this program on a given input terminates after at most $\max\{\lceil x\rceil, 0\}$, thus finitely many, loop iterations. The probabilistic nature of the program has thus no effect on termination itself, but only on the time until termination.

As a second example, consider the program

$$\begin{array}{l}\texttt{while}(x>0)\{\\ \quad \{x:=x-1\}\,[1/2]\,\{\texttt{skip}\}\\ \}\,.\end{array}$$

This program admits a single diverging run (namely the one in which infinitely often `skip` is executed). Even though the diverging path has proba-

bility 0, this path does exist and because of this, the program does not terminate certainly. The program does, however, terminate universally almost–surely, i.e. with probability 1. Moreover, the program terminates *universally positively almost–surely* as it needs on average $\max\{2\lceil x\rceil, 0\}$ loop iterations until it terminates, which for a given input x is a finite number. If we were to execute the program on an initial state with $x = 10$, we could thus expect to witness termination of the program within 20 loop iterations. Formally, positive almost–sure termination is defined as follows:

Definition 6.1 (Expected Runtimes and Positive A.–s. Termination):

A. *Let $C \in$ pGCL and let $\sigma \in \Sigma$ be a program state. Then the worst–case expected runtime of C on input σ is given by*[1]

$$\mathsf{ERT}\,[\![C]\!]_\sigma \;=\; \sup_{\mathfrak{s}\in\mathsf{Scheds}} \sum_{i=1}^{\omega} \left(1 \;-\; \sum_{\langle\downarrow,\tau,n,\theta,\eta,q\rangle\in K_{\mathfrak{s}}^{<i}} q\right), \qquad \text{where}$$

$$K_{\mathfrak{s}}^{<i} \;=\; \left\{ \langle\downarrow,\tau,n,\theta,\eta,q\rangle \;\middle|\; \langle C,\sigma,0,\varepsilon,\varepsilon,1\rangle \;\vdash_{\mathfrak{s}}^{*}\; \langle\downarrow,\tau,n,\theta,\eta,q\rangle,\; n<i \right\}.$$

B. *C terminates positively almost–surely on input σ iff its expected runtime on input σ is finite, i.e.* $\mathsf{ERT}\,[\![C]\!]_\sigma < \infty$.

C. *C terminates universally positively almost–surely iff C terminates positively almost–surely on* all *inputs, i.e.* $\forall\, \sigma \in \Sigma\colon\ \mathsf{ERT}\,[\![C]\!]_\sigma < \infty$.

The intuition for the formula for $\mathsf{ERT}\,[\![C]\!]_\sigma$ above is that we can express the expected value of a non–negative $\big(\mathbb{N}\cup\{\infty\}\big)$–valued random variable X as

$$\mathsf{EV}(X) \;=\; \sum_{i=1}^{\omega} \Pr(X \geq i)\,.$$

As we have no direct access to the probability that a probabilistic program runs for at least i steps, we compute 1 minus the probability that the program runs for less than i steps.

The terminology *positive almost–sure termination* was introduced by Bournez & Garnier [BG05]. Their inspiration for the term „positive“ came from Markov chain theory, more specifically from the distinction between *positively recurrent* states (states that are revisited with probability one and the expected time until a revisit is finite) and *null recurrent* states (states that are revisited with probability one but the expected time to revisit is infinite) [Put05, Section A.2, p. 588]. Adapting this line of thought, almost–surely terminating programs that do not terminate positively almost–surely could be called *null almost–surely terminating*. We consider such cases next.

As our third example, consider the program

1 Recall Definition 3.4 and Definition 3.7.

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

This program admits infinitely many diverging runs but their aggregated probability is 0. In contrast to the second example, however, this third program does *not* terminate within an expected finite number of loop iterations. Its expected runtime is infinite. Thus, the notion under which we can speak of termination of the above program is *weaker*: It terminates almost–surely, i.e. with probability 1. Formally, almost–sure termination of programs is defined as follows:

Definition 6.2 (Almost–sure Termination):
Let C be a pGCL *program and let $\sigma \in \Sigma$ be an initial program state. Then C terminates almost–surely on input σ iff*

$$\mathsf{wp}\,[\![C]\!]\,(1)(\sigma) \;=\; 1\,.$$

C terminates universally almost–surely iff C terminates almost–surely on all *inputs, i.e.*

$$\mathsf{wp}\,[\![C]\!]\,(1) \;=\; 1\,.^{2}$$

C terminates (universally) null almost–surely iff C terminates (universally) almost–surely but not (universally) positively almost–surely.

The example program above terminates *universally null almost–surely*, since it terminates with probability 1 but requiring infinite expected runtime. Intuitively, if we were to execute the program on a state with $x = 10$, we would expect the program to terminate, but we cannot expect to witness its termination within our lifespan.

Proving universal almost–sure termination of a program C amounts to proving that 1 is a (non–strict) *lower bound* on the termination probability of C, i.e. proving $1 \preceq \mathsf{wp}\,[\![C]\!]\,(1)$. Proving universal positive almost–sure termination of C amounts to proving a finite *upper bound* on the expected runtime of C (for a calculus for reasoning about expected runtimes, see Chapter 7). From our experience in Section 5.2 and in particular from our considerations in Section 5.2.6 we can expect positive almost–sure termination proofs to be easier in practice, since they constitute an upper bound proof. And indeed, we will see that the methodology for positive almost–sure termination is easier than the one for almost–sure termination proofs.

Besides certain, positive almost–sure, and almost–sure termination, another notion that is sometimes considered are so–called *tail bounds* or *tail*

2 Notice that the two 1's on the right hand sides of the two equations in this definition are of different type. The first 1 is the real number 1, whereas the second 1 is an expectation, namely $\lambda\sigma.\ 1$.

probabilities [CF17; CNZ17]. For a given program and input, tail bounds map each number $n \in \mathbb{N}$ to the probability that the program performs at least n computation steps on the given input. We will, however, not consider tail bounds in this thesis but instead focus on positive almost–sure and almost–sure termination, starting with the former.

6.1 POSITIVE ALMOST–SURE TERMINATION

For a nonprobabilistic loop $\texttt{while}(\varphi)\{C\}$, one way to prove termination is by use of *loop variants* [Flo67a, p. 30 et seqq.]. A loop variant is a mapping from program states to a well–founded set, i.e. a set together with an order relation in which no infinite descend is possible, such that iteration of the loop body strictly decreases the value of the variant. Existence of a loop variant then proves termination of the loop.

A particular form of loop variants are *ranking functions* [Dij75, p. 455]. A ranking function R maps program states to real numbers and satisfies the following two constraints for every state σ:

A. If $\sigma \models \varphi$, then execution of C on σ terminates in a state τ such that

$$R(\tau) \;\leq\; R(\sigma) - \epsilon\,,$$

for some fixed $\epsilon > 0$, and

B. if $R(\sigma) \leq 0$, then $\sigma \not\models \varphi$.

Constraint A. ensures that, from any state σ satisfying the loop guard, the execution of the loop body reaches a successor state whose ranking is at least by ϵ smaller than σ's ranking, thus ensuring a strict descent. Constraint B. ensures that if the ranking hits 0 or drops below, this falsifies the loop guard and thus causes the loop to terminate. Therefore, from any state σ, no infinite chain of successor states with ever decreasing ranking can be formed by iterated execution of the loop body without eventually falsifying the loop guard and thus terminating the loop, since the length of such a chain is bounded by $\lceil R(\sigma)/\epsilon \rceil$. This ensures certain termination of the loop within at most $\lceil R(\sigma)/\epsilon \rceil$ loop iterations.

For instance, for the program

$$\begin{array}{l}\texttt{while}(x > 0)\{\\ \quad x := x - 1\\ \}\end{array}$$

we can choose the ranking function $R = x$ or more formally

$$R \;=\; \lambda\sigma.\; \sigma(x)\,.$$

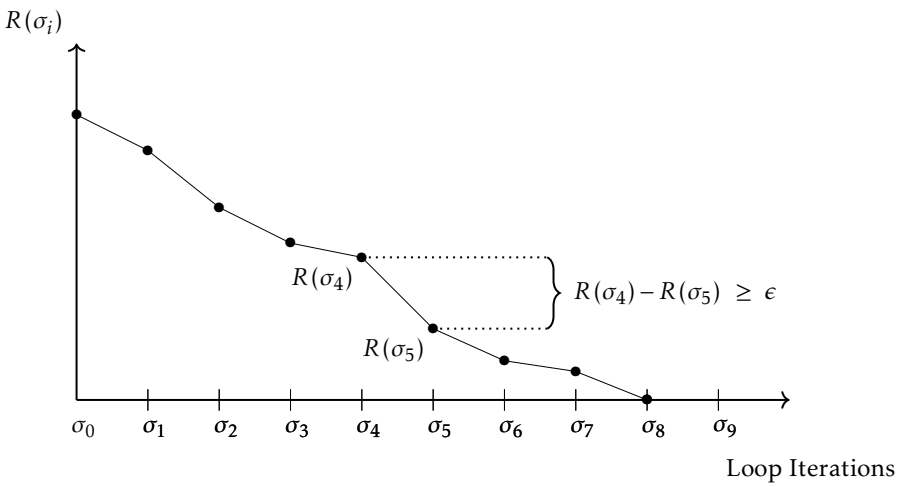

Figure 6.1: Evolution of the values of a ranking function R over the iterations of a loop. σ_0 is the initial state and $\sigma_1, \sigma_2, \sigma_3, \ldots$ are the states reached after $1, 2, 3, \ldots$ loop iterations, respectively. One iteration decreases the ranking by at least ϵ which guarantees eventually hitting 0 (or dropping below).

Then R is a ranking function as every iteration of the loop body decreases x by $\epsilon = 1$ and the loop body will not be executed again once $x \leq 0$.

For probabilistic programs, this reasoning fails. The loop body of

$$\texttt{while}(x > 0)\{ \quad \{x := x - 1\}\,[1/2]\,\{\texttt{skip}\} \quad \},$$

for instance, is not guaranteed to decrease x due to the possibility of executing `skip` instead of $x := x - 1$. However, every iteration of the loop body decreases x by $1/2$ *in expectation* and thus x is *ranking in expectation*.

Existence of a function that is ranking in expectation indeed suffices to prove positive almost–sure termination. Translated into our weakest preexpectation setting, we have the following theorem:

Theorem 6.3 (PAST from Ranking Superinvariants [CS13; FH15]): *Let* $\texttt{while}(\varphi)\{C\}$ *be a loop where the loop body* C *itself terminates universally* certainly.[3] *Furthermore, let* $I \in \mathbb{E}$ *be a ranking superinvariant*[4]

3 E.g. let C be loop–free.

4 Ranking superinvariants correspond to *ranking super martingales* in the terminology of [CS13].

of $\texttt{while}(\varphi)\{C\}$ *with respect to postexpectation 0, i.e.* $I \ll \infty$ *and there exist constants* ϵ *and* K *with* $0 < \epsilon < K$*, such that*

$$[\neg\varphi]\cdot I \;\leq\; K \quad \text{and} \quad [\varphi]\cdot K \;\ll\; [\varphi]\cdot I + [\neg\varphi]$$
$$\text{and} \quad \Phi_0(I) \;\leq\; [\varphi]\cdot(I-\epsilon)\,,$$

where Φ_0 *is the* awp*–characteristic function of* $\texttt{while}(\varphi)\{C\}$ *with respect to postexpectation* 0*.*

Then $\texttt{while}(\varphi)\{C\}$ *terminates universally positively almost–surely.*

Notice that we use awp because we want to *guarantee* that I is decreased in expectation by at least ϵ through one iteration of the loop body.

The two extra conditions involving the constant K are a technical necessity in order to avoid the need for our ranking superinvariants to map to negative values (as ranking functions do): The loop body should decrease I by ϵ in expectation, so I can drop by at most ϵ into the negative. We mitigate this by pulling everything up by $K > \epsilon$ and let a drop below K (instead of 0) indicate termination.

Theorem 6.3 is basically a reformulation of [CS13, Theorem 4] or [FH15, Theorem 5.6] but translated into our weakest preexpectation setting. It is also very similar and basically equivalent to Theorem 3 of [Kam+16], which we present in Chapter 7. The main difference is that [Kam+16] needs less preconditions and always uses $\epsilon = 1$, while still being complete.

Example 6.4 (PAST from Ranking Superinvariants):
Reconsider the program

$$\begin{array}{l}\texttt{while}(x>0)\{\\ \quad \{x := x-1\}\,[1/2]\,\{\texttt{skip}\}\\ \}\,,\end{array}$$

for which the awp–characteristic function with respect to 0 is given by

$$\begin{aligned}\Phi_0(X) \;&=\; [x\leq 0]\cdot 0 \;+\; [x>0]\cdot \mathsf{wp}\,[\![\{x := x-1\}\,[1/2]\,\{\texttt{skip}\}]\!]\,(X)\\ &=\; [x>0]\cdot\frac{1}{2}\Big(X[x/x-1]+X\Big)\end{aligned}$$

Then $I = [x \geq -1]\cdot x + 1$ is a ranking superinvariant with $K = 1$ and $\epsilon = 1/2$. To see that I is indeed a ranking superinvariant, consider

$$[x\leq 0]\cdot I \;=\; [x\leq 0]\cdot\Big([x\geq -1]\cdot x+1\Big) \;\leq\; 1 \;=\; K$$

and

$$\begin{aligned}
[x>0]\cdot K &= [x>0]\cdot 1\\
&\ll [x>0]\cdot(x+1)+[x\leq 0]\\
&\ll [x>0]\cdot\Big([x\geq -1]\cdot x+1\Big)+[x\leq 0]\\
&= [x>0]\cdot I+[x\leq 0]
\end{aligned}$$

and

$$\begin{aligned}
\Phi_0(I) &= [x>0]\cdot\frac{1}{2}\Big(I\,[x/x-1]+I\Big)\\
&= [x>0]\cdot\frac{1}{2}\Big([x-1\geq -1]\cdot(x-1)+1+[x\geq -1]\cdot x+1\Big)\\
&= [x>0]\cdot\frac{1}{2}\Big([x\geq 0]\cdot(x-1)+1+[x\geq -1]\cdot x+1\Big)\\
&= [x>0]\cdot\frac{1}{2}\Big(x-1+1+x+1\Big)\\
&= [x>0]\cdot\frac{1}{2}\Big(x-1+1+x+1\Big)\\
&= [x>0]\cdot\Big(x+1-\frac{1}{2}\Big)\\
&= [x>0]\cdot\Big([x>0]\cdot x+1-\frac{1}{2}\Big)\\
&= [x>0]\cdot(I-\epsilon)\,.
\end{aligned}$$

This proves that I is a ranking superinvariant which by Theorem 6.3 proves universal positive almost–sure termination of the loop under consideration.

A technically less involved, yet complete, method (no need for choosing K or ϵ) for proving a finite expected runtime (and thereby positive almost–sure termination) is presented in Chapter 7.

6.2 ALMOST–SURE TERMINATION

As mentioned earlier, proving almost–sure termination of null almost–surely terminating programs (i.e. programs that terminate with probability 1 but with infinite expected time until termination, cf. Definition 6.2), appears notoriously difficult, because it requires proving a lower bound on a least fixed point, namely that 1 is a (non–strict) lower bound on the termination probability. The lack of a finite upper bound on the expected runtime renders the coinductive proof technique of ranking supermartingales (Theorem 6.3) unavailable.

A new proof rule that does allow for proving almost–sure termination, even of null almost–surely terminating loops, is presented in Section 6.2.3. Although this method will clearly appear to be more involved than the rank-

ing supermartingale approach of Theorem 6.3, it often allows for relatively easy (sometimes even surprisingly easy) proofs of almost–sure termination.

Before we present the new proof rule, we recap some earlier rules by McIver & Morgan for proving almost–sure termination. These theorems, in particular a zero–one law for probabilistic termination, will form the bedrock on which the new proof rule is built.

6.2.1 *The Zero–one Law*

Zero–one laws in probability theory typically state that under certain conditions certain events occur either with probability 0 or 1, but this probability cannot lie properly in–between. Notable examples include the Borel–Cantelli Lemma [Bor09; Can17; Wikb], Kolmogorov's zero–one law [Wikh], or the Hewitt–Savage zero–one law [HS55; Wikf]. The law considered here is due to McIver & Morgan and is a zero–one law on the termination probability of probabilistic while loops. It reads as follows:

> **Theorem 6.5 (Zero–One Law of Probabilistic Termination[5]):**
> *Let I be a predicate such that $[I]$ is a* wp*–subinvariant of* $\texttt{while}(\varphi)\{C\}$ *with respect to postexpectation $[I]$. Furthermore, let $\epsilon > 0$ be a fixed constant such that*
>
> $$\epsilon \cdot [I] \;\preceq\; \mathsf{wp}\,[\![\texttt{while}(\varphi)\{C\}]\!]\,(1)\;.$$
>
> *Then*
>
> $$[I] \;\preceq\; \mathsf{wp}\,[\![\texttt{while}(\varphi)\{C\}]\!]\,\Big([\neg\varphi \wedge I]\Big)\;.$$

Proof. We invoke Theorem 5.12 for obtaining lower bounds on preexpectations: For that, let $I' = [I]$ and $f = [\neg\varphi \wedge I]$. Then $[\neg\varphi]\cdot f + [\varphi]\cdot I'$ is a wp–subinvariant of $\texttt{while}(\varphi)\{C\}$ with respect to postexpectation f, since

$$\begin{aligned}
[I] \;&\preceq\; \Phi_0([I]) && \text{(by } [I] \text{ being a subinvariant with respect to 0)}\\
&=\; [\neg\varphi]\cdot 0 + [\varphi]\cdot \mathsf{wp}\,[\![C]\!]\,([I])\\
&\preceq\; [\neg\varphi]\cdot f + [\varphi]\cdot \mathsf{wp}\,[\![C]\!]\,([I]) && \text{(by } 0 \preceq f\text{)}\\
&=\; \Phi_f([I]) && \text{(by definition of } \Phi_f\text{)}
\end{aligned}$$

By assumption $\epsilon\cdot[I] \preceq \mathsf{wp}\,[\![\texttt{while}(\varphi)\{C\}]\!]\,(1)$, we have that

$$\epsilon\cdot\Big([\neg\varphi]\cdot f + [\varphi]\cdot I'\Big) \;=\; \epsilon\cdot[I] \;\preceq\; \mathsf{wp}\,[\![\texttt{while}(\varphi)\{C\}]\!]\,(1)$$

holds, so all preconditions of Theorem 5.12 c. are met and the theorem yields

$$[I] \;=\; [\neg\varphi]\cdot f + [\varphi]\cdot I'$$

5 This theorem subsumes [MM05, pp. 53 and 54] and [Hur03, Theorem 41].

$$\preceq \mathsf{wp}\,[\![\texttt{while}(\varphi)\{C\}]\!]\,(f) \qquad \text{(by Theorem 5.12 c.)}$$
$$= \mathsf{wp}\,[\![\texttt{while}(\varphi)\{C\}]\!]\,([\neg\varphi \wedge I])\,. \qquad \boxed{\text{Q.E.D.}}$$

While the zero–one law of Theorem 6.5 allows for proving almost–sure termination relative to an invariant, we obtain as a special case (choose true as invariant) the following corollary for universal almost–sure termination:

COROLLARY 6.6:
Let $C \in \mathsf{pGCL}$ terminate universally almost–surely. Furthermore, let $\epsilon > 0$ be a fixed constant such that

$$\epsilon \preceq \mathsf{wp}\,[\![\texttt{while}(\varphi)\{C\}]\!]\,(1)\,.$$

Then $\texttt{while}(\varphi)\{C\}$ terminates universally almost–surely, i.e.

$$\mathsf{wp}\,[\![\texttt{while}(\varphi)\{C\}]\!]\,(1) = 1\,.$$

6.2.2 *An Old Rule*

Building on the zero–one law for probabilistic termination (Theorem 6.5), McIver & Morgan have formulated a more practically oriented proof rule for proving almost–sure termination. Whereas the zero–one law needed as a precondition a lower bound ϵ on the *overall termination probability of a loop* (which is potentially as difficult to establish as almost–sure termination itself), the following rule makes use of a ranking function that is decreased with at least some constant probability by *one iteration* of the loop body. This fact is potentially much easier to check.

THEOREM 6.7 (AST from Bounded Integer Variants [MM05][6]):
Let I be a predicate such that $[I]$ is a wp*–subinvariant of $\texttt{while}(\psi)\{C\}$ with respect to postexpectation $[I]$. Furthermore, let $Z\colon \Sigma \to \mathbb{Z}$ such that*

A. *there exist constants $L, H \in \mathbb{Z}$ such that*

$$[\psi \wedge I] \preceq [L \leq Z \leq H], \qquad \text{and}$$

B. *there exists a constant $\epsilon \in (0, 1]$ such that*

$$\epsilon \cdot [\psi \wedge I] \preceq \lambda\sigma.\ \mathsf{wp}\,[\![C]\!]\,\Big([Z < Z(\sigma)]\Big)(\sigma)\,.$$

Then the loop $\texttt{while}(\psi)\{C\}$ terminates almost–surely from any initial state satisfying the invariant I, i.e.

$$[I] \preceq \mathsf{wp}\,[\![\texttt{while}(\psi)\{C\}]\!]\,(1)\,.$$

6 This theorem combines Lemma 2.7.1 on p. 55 and Lemma 7.5.1 on p. 191 in [MM05].

Proof. The full proof of Theorem 6.7 can be found in [MM05, p. 191 *et seq.*, proof of Lemma 7.5.1]. The key idea to exploit the zero–one law of probabilistic termination (Theorem 6.5). In order to understand the importance of that law for this rule, we rephrase here McIver & Morgan's sketch of the proof of Theorem 6.7 [MM05, p. 55 et seq., proof of Lemma 2.7.1]:

Recall that the variant Z is integer–valued, bounded from below by L, and bounded from above by H. Furthermore, the probability to *strictly* decrease Z (by at least 1, as Z is integer–valued) through one iteration of the loop body is at least ϵ from any starting state. Then after at most $H - L$ loop iterations, the value of the variant Z will have dropped to L or below with probability at least ϵ^{H-L}. This in turn implies falsification of the loop guard or violation of the invariant. But since satisfaction of the invariant is invariant under guarded iteration of the loop, violation of the invariant can be ruled out and so the loop terminates by falsification of the loop guard with probability at least ϵ^{H-L} from any initial state.

Since ϵ^{H-L} is a constant strictly larger than 0, we can appeal to the zero–one law of probabilistic termination (Theorem 6.5) which asserts that if the loop terminates from any state with at least some (universally) constant non–zero probability, then the loop terminates in fact almost–surely. We can thus conclude that the loop terminates not only with probability at least ϵ^{H-L} but in fact almost–surely from any initial state satisfying invariant I. Q.E.D.

While Theorem 6.7 allows for proving almost–sure termination by relatively simple means, its disadvantages are also evident: Integer–valuedness together with boundedness of the variant function clearly restricts its use cases. For instance, in order to prove almost–sure termination of a symmetric 1–dimensional random walk using Theorem 6.7, a substantial number of ad–hoc arguments are necessary and the termination proof becomes somewhat involved [MM05, Section 3.3]. Nevertheless, Theorem 6.7 can arguably be seen as an important precursor to the new rule which we present next.

6.2.3 *A New Rule*

I like your result.
Let's make it a joint paper
and I'll write the next one.

— Stefan Bergmann

Reconsider the symmetric 1–dimensional random walk modeled by the loop

$$\texttt{while}(x > 0)\{\ \{x := x - 1\}\,[1/2]\,\{x := x + 1\}\ \}.$$

We can easily convince ourselves that x is indeed a superinvariant of the loop, although it is *not ranking*.[7] In fact, the expected value of x is precisely x itself — in expectation the particle does not move. However, we can also easily convince ourselves that the probability that the particle moves a distance of 1 closer to 0 is $1/2$. As we will see, witnessing this fact indeed already suffices in order to prove almost–sure termination by our new proof rule.

Just like the proof rule of Theorem 6.7, the new rule involves a variant function which decreases by some amount with some probability through one iteration of the loop body. In contrast to Theorem 6.7, however, the variant function need neither be bounded nor integer–valued. In addition and also in contrast to Theorem 6.7, the minimum amount and probability of the variant's decrease need not be lower–bounded by some constants (for Theorem 6.7, those constants were 1 and some $\epsilon > 0$).

Before we state the new proof rule and give a detailed proof, I would sincerely like to acknowledge that the core idea of the new rule is entirely due to Annabelle McIver and Carroll Morgan, see [MM16] for their early sketch. My contribution was (a) to formalize the proof rule in terms of weakest pre-expectations and (b) give a rigorous soundness proof of the new proof rule. The version of the proof rule provided here differs slightly from the published version ([McI+18, Theorem 4.1]) both in its formulation as well as in its proof as I personally find the presentation at hand more natural.

THEOREM 6.8 (AST from Progressing Variants [McI+18]):
Let I be a predicate and moreover let

- $V : \Sigma \to \mathbb{R}_{\geq 0}$ *(for **v**ariant),*
- $p : \mathbb{R}_{\geq 0} \to (0, 1]$ *(for **p**robability) be antitone*[8]*,*
- $d : \mathbb{R}_{\geq 0} \to \mathbb{R}_{>0}$ *(for **d**ecrease) be antitone.*

Suppose further that the following conditions hold:

A. $[I]$ *is a* wp*–subinvariant of* `while(φ){C}` *with respect to* $[I]$*, i.e.*

$$[I] \;\leq\; {}^{\mathsf{wp}}\Phi_{[I]}\big([I]\big) \quad = \; [\neg\varphi]\cdot[I] \;+\; [\varphi]\cdot \mathsf{wp}\,[\![C]\!]\,([I])\,.$$

B. $V = 0$ *indicates termination, i.e.*

$$[\neg\varphi] \;=\; [V = 0]\,.$$

7 As mentioned earlier, this loop terminates *null* almost–surely. Thus, there cannot exist a ranking supermartingale for this loop as this would by Theorem 6.3 imply positive almost–sure termination of this loop.

8 Antitonicity is the dual notion to monotonicity [Wiki]: A function f is called antitone iff

$$a \leq b \quad \text{implies} \quad f(a) \geq f(b)\,.$$

c. *V is a* awp–*superinvariant of* `while`$(\varphi)\{C\}$ *with respect to* V*, i.e.*

$$V \geq \underset{\langle \varphi, C \rangle}{\mathsf{awp}} \Phi_V(V) \quad = [\neg\varphi] \cdot V + [\varphi] \cdot \mathsf{wp}\,[\![C]\!]\,(V)\,.$$

d. *V satisfies a progress condition, namely*[9]

$$p \circ V \cdot [\varphi] \cdot [I] \preceq \lambda\sigma.\ \mathsf{wp}\,[\![C]\!] \left(\left[V \leq V(\sigma) - d\Big(V(\sigma)\Big) \right] \right)(\sigma)\,.$$

Then the loop `while`$(\varphi)\{C\}$ *terminates almost–surely from any initial state satisfying the invariant I, i.e.*

$$[I] \preceq \mathsf{wp}\,[\![\texttt{while}(\varphi)\{C\}]\!]\,(1)\,.$$

The intuitive mechanics of the new proof rule is illustrated in Figure 6.2. Amount and probability of the variant V's decrease are neither fixed nor bounded bounded by the progress condition, but instead adjustable by *antitone* functions d and p, which take as inputs *not* the current state, but rather *the value of the variant in the current state*. The progress condition now ensures that if the current state is σ and the loop body will be iterated once more, then the probability to decrease V by at least $d(V(\sigma))$ is at least $(p \circ V)(\sigma) = p(V(\sigma))$. For any successor state in which the value of V has *decreased*, the amount and probability of decrease for the *next iteration* will both have *increased* due to antitonicity of p and d. In a nutshell and to put it very simply:

> The closer the loop comes to termination ($V = 0$),
> the more V is decreased by iteration of the loop body (antitone d)
> and the more likely becomes this decrease (antitone p).

Antitonicity of p and d rule out a sort of *Zeno behavior* where the variant does indeed strictly decrease but by an ever decreasing amount. This would allow for V to „converge" to a value strictly larger than 0, making it less and less likely to terminate and thus causing the loop to diverge.

Example 6.9 (Almost–sure Termination of the Random Walk):
Consider the symmetric 1–dimensional random walk, modeled by

```
while(x > 0){
    {x := x − 1} [1/2] {x := x + 1}
}.
```

For reasons of readability, let us suppose that x is of type $\mathbb{N}$. We choose

9 $p \circ V$ denotes functional composition (read: p after V), i.e. $p \circ V = \lambda\sigma.\ p\Big(V(\sigma)\Big)$, and binds stronger than multiplication.

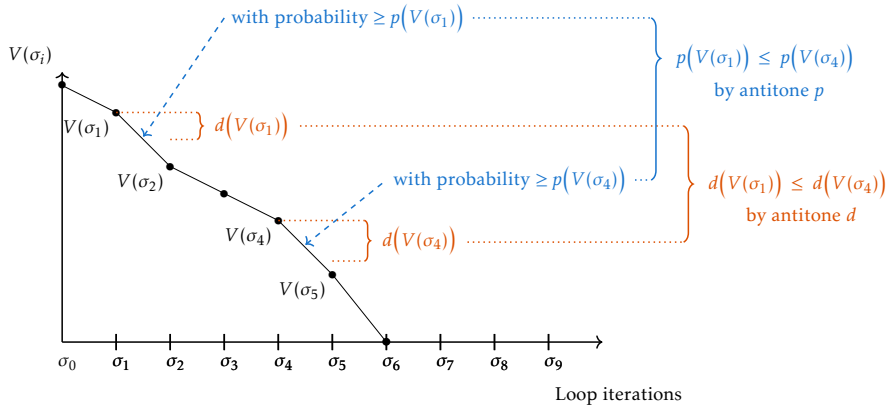

Figure 6.2: Evolution of the values of a variant V over the iterations of a probabilistic loop. σ_0 is the initial state and $\sigma_1, \sigma_2, \sigma_3, \ldots$ are states reached with non–zero probability after 1, 2, 3, … iterations, respectively. Iteration decreases the variant by an ever increasing (or constant) amount ($d(V(\sigma_i))$) with with ever increasing (or constant) probability ($p(V(\sigma_i))$).

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

as witnesses of almost–sure termination. p and d are constant and thus obviously antitone. true is a wp–subinvariant of any loop that terminates almost–surely. This is especially the case when the loop body itself is loop–free. $V = 0$ indicates termination since $V = 0$ iff $x \leq 0$ (because x is of type $\mathbb{N}$).

Next, we provide a detailed check that x is an awp–supermartingale:

$$\begin{aligned}
& {}^{\mathsf{awp}}_{\langle x>0, body\rangle}\Phi_x \preceq x \\
\text{iff}\quad & [x \leq 0]\cdot x + [x > 0]\cdot \mathsf{wp}\,[\![body]\!]\,(x) \preceq x \\
\text{iff}\quad & [x \leq 0]\cdot x + [x > 0]\cdot \frac{1}{2}\cdot(x-1+x+1) \preceq x \\
\text{iff}\quad & [x \leq 0]\cdot x + [x > 0]\cdot x \preceq x \\
\text{iff}\quad & x \preceq x
\end{aligned}$$

Finally, we check that the progress condition is satisfied:

$$\begin{aligned}
& p \circ V \cdot [\varphi]\cdot[I] \preceq \lambda\sigma.\ \mathsf{wp}\,[\![C]\!]\left(\left[V \leq V(\sigma) - d\big(V(\sigma)\big)\right]\right)(\sigma) \\
\text{iff}\quad & \frac{1}{2} \circ x \cdot [x > 0]\cdot[\mathsf{true}]
\end{aligned}$$

$$\leq \lambda\sigma.\ \mathsf{wp}\,[\![body]\!]\left(\left[x \leq x(\sigma) - (\lambda v.\ 1)\big(x(\sigma)\big)\right]\right)(\sigma)$$

$$\text{iff}\quad \frac{1}{2}[x>0] \leq \lambda\sigma.\ \mathsf{wp}\,[\![body]\!]\left([x \leq x(\sigma)-1]\right)(\sigma)$$

$$\text{iff}\quad \frac{1}{2}[x>0] \leq \lambda\sigma.\ \frac{1}{2}\cdot\Big([x-1 \leq x(\sigma)-1] + [x+1 \leq x(\sigma)-1]\Big)$$

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

$$\text{iff}\quad \frac{1}{2}[x>0] \leq \frac{1}{2}\cdot\Big(1+0\Big)$$

$$\text{iff}\quad \frac{1}{2}[x>0] \leq \frac{1}{2}$$

The last line is obviously true, thus concluding our proof, and thus we have proven almost–sure termination.

Notice that for the 1–dimensional symmetric random walk our termination witnesses were very simple functions, namely *constant* functions, and that checking the supermartingale property and the progress condition was quite simple. In particular, we did not have to reason ourselves about any limit whatsoever. *This is different for the book proof of almost–sure termination of the random walk* (see e.g. [Dur10, Theorem 4.2.3, p. 163]): There, one finds a formula for the termination probability and then proves ad–hoc that the *limit* is in fact 1.

Now that we have some intuition on the mechanics and we have seen an example on how to use the new rule in practice, we give a rigorous proof. In this proof, we will show precisely why we need a superinvariant and how the progress condition is used.

Proof (Theorem 6.8). Because the proof of Theorem 6.8 is somewhat involved, we will first give an outline of our proof strategy:

1. We fix an arbitrary constant $h \in \mathbb{R}_{>0}$ and prove that the modified loop $\texttt{while}(0 < V \leq h)\{C\}$ terminates almost–surely from any state satisfying I by exploiting Theorem 6.7.

   Notice that only the loop guard is changed from φ to $0 < V \leq h$. We have merely introduced a *cap* h on V and if V exceeds h, we force termination. Condition B. states that the original loop $\texttt{while}(\varphi)\{C\}$ terminates when V hits 0. Thus, if V hits 0, the modified loop terminates for the same reason as the original loop $\texttt{while}(\varphi)\{C\}$ would have terminated. Only if V exceeds h, then the modified loop *prematurely* terminates, whereas the original loop would still continue to be executed.

2. We prove that the supermartingale property on V implies that the modified loop $\texttt{while}(0 < V \leq h)\{C\}$ does not increase V in expectation, i.e. the expected value of V after execution of the modified loop on initial

state σ is bounded by $V(\sigma)$. Intuitively, the consequence of this is that the modified loop is more likely to terminate because of V hitting 0 than because of V exceeding h.

3. Using 1., we prove that the *non*termination probability of the original loop is bounded from above by the probability that execution of the modified loop terminates because of V exceeding h. By Markov's Inequality, the latter probability is bounded from above by the expected value of V divided by h. By 2., we then get that this fraction is itself bounded by V/h. Finally, we take the limit $h \to \infty$ to conclude that the nontermination probability of the original loop is bounded from above by 0 and thus the original loop terminates almost–surely.

Let us now conduct the proof. Let $h \in \mathbb{R}_{>0}$ be arbitrary but fixed, and let

$$\texttt{while}(0 < V \leq h)\{C\}$$

be the *modified loop*. Then we perform the proof steps we described above.

1. ***The modified loop*** $\texttt{while}(0 < V \leq h)\{C\}$ ***term. almost–surely.*** We prove that the modified loop with guard

$$\psi \;=\; (0 < V \leq h)$$

terminates almost–surely by applying Theorem 6.7 to that loop. Let us first prove that $[I]$ is a wp–subinvariant of $\texttt{while}(\psi)\{C\}$ with respect to $[I]$. We start our reasoning from condition A.:

$$\begin{aligned}
& [I] \text{ is a wp–subinvariant of } \texttt{while}(\varphi)\{C\} \text{ w.r.t. } [I] \\
\text{iff}\quad & [I] \;\preceq\; {}^{\mathsf{wp}}_{\langle \varphi, C\rangle}\Phi_{[I]}([I]) \\
& \qquad \text{(by definition of wp–subinvariance, Definition 5.1 B.)} \\
\text{iff}\quad & [I] \;\preceq\; [\neg\varphi]\cdot[I] + [\varphi]\cdot \mathsf{wp}\,[\![C]\!]\,([I]) \\
& \qquad \big(\text{by definition of } {}^{\mathsf{wp}}_{\langle \varphi, C\rangle}\Phi_{[I]}, \text{ Definition 4.5 E.}\big) \\
\text{implies}\quad & [\varphi]\cdot[I] \;\preceq\; [\varphi]\cdot \mathsf{wp}\,[\![C]\!]\,([I]) \qquad \text{(multiply both sides by } [\varphi]) \\
\text{iff}\quad & [V > 0]\cdot[I] \;\preceq\; [V > 0]\cdot \mathsf{wp}\,[\![C]\!]\,([I]) \\
& \qquad \text{(by } V = 0 \text{ indicating termination, condition B.)} \\
\text{implies}\quad & [V > 0]\cdot[V \leq h]\cdot[I] \;\preceq\; [V > 0]\cdot[V \leq h]\cdot \mathsf{wp}\,[\![C]\!]\,([I]) \\
\text{iff}\quad & [0 < V \leq h]\cdot[I] \;\preceq\; [0 < V \leq h]\cdot \mathsf{wp}\,[\![C]\!]\,([I]) \\
\text{iff}\quad & [\psi]\cdot[I] \;\preceq\; [\psi]\cdot \mathsf{wp}\,[\![C]\!]\,([I]) \qquad \text{(by definition of } \psi) \\
\text{iff}\quad & [\neg\psi]\cdot[I] + [\psi]\cdot[I] \;\preceq\; [\neg\psi]\cdot[I] + [\psi]\cdot \mathsf{wp}\,[\![C]\!]\,([I]) \\
\text{iff}\quad & [I] \;\preceq\; [\neg\psi]\cdot[I] + [\psi]\cdot \mathsf{wp}\,[\![C]\!]\,([I]) \\
\text{iff}\quad & [I] \;\preceq\; {}^{\mathsf{wp}}_{\langle \psi, C\rangle}\Phi_{[I]}([I]) \\
& \qquad \big(\text{by definition of } {}^{\mathsf{wp}}_{\langle \psi, C\rangle}\Phi_{[I]}, \text{ Definition 4.5 E.}\big)
\end{aligned}$$

$$\text{iff} \quad [I] \text{ is a wp–subinvariant of } \texttt{while}(\psi)\{C\} \text{ w.r.t. } [I]$$
(by definition of wp–subinvariance, Definition 5.1 B.)

Next, we have to choose for Theorem 6.7 a bounded integer–valued variant Z. Notice that we have with h an upper bound for the value of V. By antitonicity of p and d, we have with $p(h)$ and $d(h)$ *lower bounds* on the probability and the amount of V's decrease. We can thus use as integer variant Z the number of times that we can subtract $d(h)$ from V until we hit 0. The probability to decrease Z by at least 1 is then at least $p(h)$ — just as the probability to decrease V by at least $d(h)$. Formally, we discretize V as follows:

$$Z \;=\; \left\lceil \frac{V}{d(h)} \right\rceil$$

As bounds for Z we choose the lower bound $L = 0$ and upper bound $H = \lceil h/d(h) \rceil$. To see that Z is appropriately bounded (i.e. in the sense of Theorem 6.7), consider that $0 < V \leq h$ implies $0 \geq \lceil V/d(h) \rceil \leq \lceil h/d(h) \rceil$ and thus

$$[0 \leq V \leq h] \;\preceq\; \left[0 \leq \left\lceil \frac{V}{d(h)} \right\rceil \leq \left\lceil \frac{h}{d(h)} \right\rceil\right]$$
$$\text{implies} \quad [0 \leq V \leq h \wedge I] \;\preceq\; \left[0 \leq \left\lceil \frac{V}{d(h)} \right\rceil \leq \left\lceil \frac{h}{d(h)} \right\rceil\right]$$
$$\text{implies} \quad [0 < V \leq h \wedge I] \;\preceq\; \left[0 \leq \left\lceil \frac{V}{d(h)} \right\rceil \leq \left\lceil \frac{h}{d(h)} \right\rceil\right]$$
$$\text{iff} \quad [\psi \wedge I] \;\preceq\; [L \leq Z \leq H] \qquad \text{(by definition of } \psi, Z, L, \text{ and } H)$$

The last precondition we need in order to be able to apply Theorem 6.7 is that there exists an $\epsilon > 0$ such that

$$\epsilon \cdot [\psi \wedge I] \;\preceq\; \lambda\sigma.\ \mathsf{wp}\,[\![C]\!]\,([Z < Z(\sigma)])\ .$$

When choosing $\epsilon = p(h)$, we have by the progress condition D.:

$$p\big(V(\sigma)\big) \cdot [\varphi \wedge I] \;\preceq\; \lambda\sigma.\ \mathsf{wp}\,[\![C]\!]\,\Big(\big[V \leq V(\sigma) - d\big(V(\sigma)\big)\big]\Big)$$
$$\text{iff} \quad p\big(V(\sigma)\big) \cdot [V > 0 \wedge I] \;\preceq\; \lambda\sigma.\ \mathsf{wp}\,[\![C]\!]\,\Big(\big[V \leq V(\sigma) - d\big(V(\sigma)\big)\big]\Big)$$
(by $V = 0$ indicating termination, condition B.)
$$\text{implies} \quad p\big(V(\sigma)\big) \cdot [0 < V \leq h \wedge I]$$
$$\preceq\; \lambda\sigma.\ \mathsf{wp}\,[\![C]\!]\,\Big(\big[V \leq V(\sigma) - d\big(V(\sigma)\big)\big]\Big)$$
$$\text{iff} \quad p\big(V(\sigma)\big) \cdot [\psi \wedge I] \;\preceq\; \lambda\sigma.\ \mathsf{wp}\,[\![C]\!]\,\Big(\big[V \leq V(\sigma) - d\big(V(\sigma)\big)\big]\Big)$$
(by definition of ψ)

Since for all states σ with $V(\sigma) \leq h$ we have $p(h) \leq p(V(\sigma))$, we obtain:

$$\text{implies} \quad p(h) \cdot [\psi \wedge I] \;\preceq\; \lambda\sigma.\ \mathsf{wp}\,[\![C]\!]\,\Big(\big[V \leq V(\sigma) - d\big(V(\sigma)\big)\big]\Big)$$

$$\text{iff}\quad p(h)\cdot[\psi\wedge I]\ \preceq\ \lambda\sigma.\ \mathsf{wp}\,[\![C]\!]\left(\left[\frac{V}{d(h)}\leq\frac{V(\sigma)}{d(h)}-\frac{d(V(\sigma))}{d(h)}\right]\right)$$

Since ${}^{V}\!/_{d(h)}\leq {}^{V(\sigma)}\!/_{d(h)}-{}^{d(V(\sigma))}\!/_{d(h)}$ implies $\lceil {}^{V}\!/_{d(h)}\rceil\leq\lceil {}^{V(\sigma)}\!/_{d(h)}-{}^{d(V(\sigma))}\!/_{d(h)}\rceil$, we obtain by monotonicity of wp, Theorem 4.16:

$$\text{implies}\quad p(h)\cdot[\psi\wedge I]\ \preceq\ \lambda\sigma.\ \mathsf{wp}\,[\![C]\!]\left(\left[\left\lceil\frac{V}{d(h)}\right\rceil\leq\left\lceil\frac{V(\sigma)}{d(h)}-\frac{d(V(\sigma))}{d(h)}\right\rceil\right]\right)$$

For all states σ with $V(\sigma)\leq h$ we have that $d(h)\leq d(V(\sigma))$ by antitonicity of d. Thus $\lceil {}^{V}\!/_{d(h)}\rceil\leq\lceil {}^{V(\sigma)}\!/_{d(h)}-{}^{d(V(\sigma))}\!/_{d(h)}\rceil$ implies $\lceil {}^{V}\!/_{d(h)}\rceil\leq\lceil {}^{V(\sigma)}\!/_{d(h)}-1\rceil$ and we get by monotonicity of wp, Theorem 4.16:

$$\text{implies}\quad p(h)\cdot[\psi\wedge I]\ \preceq\ \lambda\sigma.\ \mathsf{wp}\,[\![C]\!]\left(\left[\left\lceil\frac{V}{d(h)}\right\rceil\leq\left\lceil\frac{V(\sigma)}{d(h)}-1\right\rceil\right]\right)$$

$$p(h)\cdot[\psi\wedge I]\ \preceq\ \lambda\sigma.\ \mathsf{wp}\,[\![C]\!]\left(\left[\left\lceil\frac{V}{d(h)}\right\rceil<\left\lceil\frac{V(\sigma)}{d(h)}\right\rceil\right]\right)$$

(by $\lceil {}^{V(\sigma)}\!/_{d(h)}-1\rceil<\lceil {}^{V(\sigma)}\!/_{d(h)}\rceil$)

$$\text{iff}\quad p(h)\cdot[\psi\wedge I]\ \preceq\ \lambda\sigma.\ \mathsf{wp}\,[\![C]\!]\,([Z<Z(\sigma)])\quad\text{(by definition of } Z)$$

We conclude by Theorem 6.7 that $\texttt{while}(0<V\leq h)\{C\}$ terminates almost–surely from any state satisfying I, i.e.

$$[I]\ \preceq\ \mathsf{wp}\,[\![\texttt{while}(0<V\leq h)\{C\}]\!]\,(1)\ . \tag{†}$$

2. ***The modified loop*** $\texttt{while}(0<V\leq h)\{C\}$ ***does not increase*** V ***in expectation.*** Since, by condition C., V is a awp–superinvariant of $\texttt{while}(\varphi)\{C\}$ with respect to postexpectation V, we know that

$$\begin{aligned}
&{}^{\mathsf{awp}}_{\langle\varphi,C\rangle}\Phi_V(V)\ \preceq\ V\\
\text{iff}\quad&[\neg\varphi]\cdot V\ +\ [\varphi]\cdot\mathsf{awp}\,[\![C]\!]\,(V)\ \preceq\ V\\
&\qquad\qquad\big(\text{by definition of } {}^{\mathsf{awp}}_{\langle\varphi,C\rangle}\Phi_V\text{, Definition 4.5 E.}\big)\\
\text{iff}\quad&[\varphi]\cdot\mathsf{awp}\,[\![C]\!]\,(V)\ \preceq\ V\\
\text{iff}\quad&[0<V]\cdot\mathsf{awp}\,[\![C]\!]\,(V)\ \preceq\ V\\
&\qquad\qquad\text{(by } V=0 \text{ indicating termination, condition B.)}\\
\text{implies}\quad&[0<V\leq h]\cdot\mathsf{awp}\,[\![C]\!]\,(V)\ \preceq\ V\\
\text{implies}\quad&\big([0=V]+[h<V]\big)\cdot V\ +\ [0<V\leq h]\cdot\mathsf{awp}\,[\![C]\!]\,(V)\ \preceq\ V\\
\text{iff}\quad&{}^{\mathsf{awp}}_{\langle 0<V\leq h,C\rangle}\Phi_V\ \preceq\ V\\
&\qquad\qquad\big(\text{by definition of } {}^{\mathsf{awp}}_{\langle 0<V\leq h,C\rangle}\Phi_V\text{, Definition 4.5 E.}\big)\\
\text{implies}\quad&\mathsf{awp}\,[\![\texttt{while}(0<V\leq h)\{C\}]\!]\,(V)\ \preceq\ V\qquad\qquad(\ddagger)\\
&\qquad\qquad\text{(by induction rule, Theorem 5.4)}
\end{aligned}$$

Thus we have concluded that the modified loop $\texttt{while}(0<V\leq h)\{C\}$ does not increase V in expectation.

3. ***The original loop*** $\texttt{while}(\varphi)\{C\}$ ***terminates almost–surely.*** We first prove that the original loop $\texttt{while}(0<V)\{C\}$ is more likely to terminate with $V=0$ than the modified loop $\texttt{while}(0<V\leq h)\{C\}$. This is intuitively clear, because whenever the modified loop exceeds h and thus terminates with $V\neq 0$, the original loop does not terminate and has still a chance of „returning“ and dropping down to 0. For a rigorous proof, consider the following for all $X\in\mathbb{E}$:

$$
\begin{aligned}
& [0<V\leq h] \;\leq\; [0<V] \\
\text{implies}\quad & [V=0] \;+\; [0<V\leq h]\cdot \mathsf{awp}\,[\![C]\!]\,(X) \\
& \qquad \leq\; [V=0] \;+\; [0<V]\cdot \mathsf{awp}\,[\![C]\!]\,(X) \\
\text{iff}\quad & \big([0=V]+[h<V]\big)\cdot[V=0] \;+\; [0<V\leq h]\cdot \mathsf{awp}\,[\![C]\!]\,(X) \\
& \qquad \leq\; [0=V]\cdot[V=0] \;+\; [0<V]\cdot \mathsf{awp}\,[\![C]\!]\,(X) \\
\text{iff}\quad & {}^{\mathsf{wp}}\Phi_{[V=0]}(X) \;\leq\; {}^{\mathsf{wp}}\Phi_{[V=0]}(X) \\
& \big(\text{by definition of } {}^{\mathsf{wp}}\Phi_{[V=0]} \text{ and } {}^{\mathsf{wp}}\Phi_{[V=0]}, \text{ Definition 4.5 E.}\big) \\
\text{implies}\quad & \mathsf{wp}\,[\![\texttt{while}(0<V\leq h)\{C\}]\!]\,([V=0]) \qquad (\ddagger\ddagger) \\
& \qquad \leq\; \mathsf{wp}\,[\![\texttt{while}(0<V)\{C\}]\!]\,([V=0])
\end{aligned}
$$

We are now in a position to gradually develop a lower bound on the termination probability of the original loop. For that, consider the following:

$$
\begin{aligned}
& \mathsf{wp}\,[\![\texttt{while}(\varphi)\{C\}]\!]\,(1) \\
&= \mathsf{wp}\,[\![\texttt{while}(\varphi)\{C\}]\!]\,([\neg\varphi]) \\
&\qquad\qquad \text{(by postexpectation strengthening, Corollary 4.6)} \\
&= \mathsf{wp}\,[\![\texttt{while}(0<V)\{C\}]\!]\,([V=0]) \\
&\qquad\qquad \text{(by } V=0 \text{ indicating termination, condition B.)}
\end{aligned}
$$

Since the original loop $\texttt{while}(0<V)\{C\}$ is more likely to terminate with $V=0$ than the modified loop $\texttt{while}(0<V\leq h)\{C\}$, see ‡‡ above, we can lower–bound the above by:

$$
\begin{aligned}
&\geq \mathsf{wp}\,[\![\texttt{while}(0<V\leq h)\{C\}]\!]\,([V=0]) \\
&= 1-\mathsf{awlp}\,[\![\texttt{while}(0<V\leq h)\{C\}]\!]\,(1-[V=0]) \quad \text{(by Theorem 4.25 A.)} \\
&= 1-\mathsf{awlp}\,[\![\texttt{while}(0<V\leq h)\{C\}]\!]\,([0<V]) \\
&\geq [I]\cdot\big(1-\mathsf{awlp}\,[\![\texttt{while}(0<V\leq h)\{C\}]\!]\,([0<V])\big) \\
&= [I]\cdot\big(1-[I]\cdot\mathsf{awlp}\,[\![\texttt{while}(0<V\leq h)\{C\}]\!]\,([0<V])\big)
\end{aligned}
$$

Since the modified loop $\texttt{while}(0<V\leq h)\{C\}$ terminates from every state satisfying the invariant I, see † in 1., we conclude by Theorem 4.27 B. that $[I]\cdot\mathsf{awlp}\,[\![\texttt{while}\,(\ldots)\}]\!]\,([0<V])\leq \mathsf{awp}\,[\![\texttt{while}\,(\ldots)\}]\!]\,([0<V])$ and we can thus lower–bound the above by:

$$
\begin{aligned}
&\geq [I] \cdot \Big(1 - \mathsf{awp}\,[\![\texttt{while}(0 < V \leq h)\{C\}]\!]\,([0 < V])\Big) \\
&= [I] \cdot \Big(1 - \mathsf{awp}\,[\![\texttt{while}(0 < V \leq h)\{C\}]\!]\,\Big(\big([V = 0] + [V > h]\big) \cdot [0 < V]\Big)\Big) \\
&\qquad\qquad \text{(by postexpectation strengthening, Corollary 4.6)} \\
&= [I] \cdot \Big(1 - \mathsf{awp}\,[\![\texttt{while}(0 < V \leq h)\{C\}]\!]\,([V > h])\Big) \\
&\geq [I] \cdot \Big(1 - \mathsf{awp}\,[\![\texttt{while}(0 < V \leq h)\{C\}]\!]\,([V \geq h])\Big) \\
&\qquad\qquad \text{(by } [V > h] \leq [V \geq h] \text{ and monotonicity, Theorem 4.16)} \\
&\geq [I] \cdot \left(1 - \frac{\mathsf{awp}\,[\![\texttt{while}(0 < V \leq h)\{C\}]\!]\,(V)}{h}\right) \\
&\qquad\qquad \text{(by Markov's inequality, Theorem 4.19)} \\
&\geq [I] \cdot \left(1 - \frac{V}{h}\right) \qquad\qquad \Big(\text{by } \ddagger \text{ in } \boxed{2.}\Big)
\end{aligned}
$$

To summarize, we have until now established

$$[I] \cdot \left(1 - \frac{V}{h}\right) \;\preceq\; \mathsf{wp}\,[\![\texttt{while}(\varphi)\{C\}]\!]\,(1)\;.$$

Since this inequality holds for an arbitrary $h > 0$, we can take the limit $h \to \infty$ and thus obtain

$$
\begin{aligned}
& \lim_{h\to\infty} [I] \cdot \left(1 - \frac{V}{h}\right) \;\preceq\; \mathsf{wp}\,[\![\texttt{while}(\varphi)\{C\}]\!]\,(1) \\
\text{implies}\quad & [I] \cdot (1 - 0) \;\preceq\; \mathsf{wp}\,[\![\texttt{while}(\varphi)\{C\}]\!]\,(1) \\
\text{implies}\quad & [I] \;\preceq\; \mathsf{wp}\,[\![\texttt{while}(\varphi)\{C\}]\!]\,(1)\;,
\end{aligned}
$$

which finally proves that $\texttt{while}(\varphi)\{C\}$ terminates almost–surely from any initial state satisfying the invariant I. Q.E.D.

6.2.4 *Case Studies in Almost–sure Termination*

We now study a few more cases of almost–surely terminating loops and their termination proofs by means of Theorem 6.8 whose correctness we have just proved. We have already seen in Example 6.9 how easy it is to prove almost–sure termination of a symmetric 1–dimensional random walk. For some of the case studies we show in the following, it is much less obvious that they terminate almost–surely.

6.2.4.1 *The Demonically Symmetric Random Walk*

In order to demonstrate the capability of Theorem 6.8 to reason about nondeterminism and take loop invariants into account, we consider a while loop that contains both probabilistic and nondeterministic choice and terminates only from a certain set of states.

$$\texttt{while}(x \neq 0)\{ \quad \Big\{x := x-1\Big\}\,[1/2]\,\Big\{\{x := x+1\} \,\square\, \{\texttt{skip}\}\Big\} \quad \}$$

The execution of the loop is illustrated in Figure 6.3. The difference to the symmetric 1–dimensional random walk is that instead of incrementing x, the while loop above can also do nothing. The demonic behavior (in terms of termination) is of course to perform the increment. Furthermore, the loop guard is $x \neq 0$ instead of $x > 0$. Thus, the particle must hit exactly 0, which is only possible if x was initially an integer.

Apart from the integer issue, the motivation for this loop is the recursive procedure P inspired by an example of [Olm+16]; its definition is

$$P \;\rhd\; \Big\{\texttt{skip}\Big\}\,[1/2]\,\Big\{\,\texttt{call}\ P;\ \{\texttt{call}\ P\} \,\square\, \{\texttt{skip}\}\Big\}\,.$$

Above, we have rewritten this recursive program as a loop by viewing it as a random walk of a particle x whose position represents the height of the call stack. Intuitively, the loop keeps moving x in a random and demonic fashion until the particle hits the origin 0 (empty call stack, all procedure calls have terminated). For that, at each stage it either with probability 1/2 decrements the position of x by one (procedure call terminates after skip; call stack decremented by one), or with probability 1/2 it performs a demonic choice between incrementing the position of x by one (perform two consecutive procedure calls, then terminate; call stack in effect incremented by one ($+2-1=+1$)) or letting x remain at its position (perform one procedure call, then terminate; call stack in effect unchanged ($+1-1=0$)).

Proof of almost–sure termination. We choose the witnesses

$$I = (x \in \mathbb{N}), \quad V \;=\; [x \in \mathbb{N}]\cdot x + [x \notin \mathbb{N}], \quad d \;=\; 1, \quad \text{and} \quad p \;=\; \frac{1}{2}\,.$$

Intuitively, I, V, p, and d tell us that x decreases with probability at least 1/2 by at least 1 through one iteration of the loop body if initially x is an natural number unequal to zero.

Let us now check that all premises of Theorem 6.8 are satisfied: p and d are constant and thus obviously antitone. $V = 0$ indicates termination since $V = 0$ iff $x = 0$.

Next, we check in detail that $[I]$ is a wp–subinvariant with respect to $[I]$:

$$\begin{aligned}
&{}^{\mathsf{wp}}\Phi_{[I]}([I]) \\
&\quad= {}^{\mathsf{wp}}\Phi_{[x\in\mathbb{N}]}([x \in \mathbb{N}]) \\
&\quad= [x=0]\cdot[x\in\mathbb{N}] \;+\; [x\neq 0]\cdot \mathsf{wp}\,[\![body]\!]\,([x\in\mathbb{N}]) \\
&\quad= [x=0]\cdot[x\in\mathbb{N}]
\end{aligned}$$

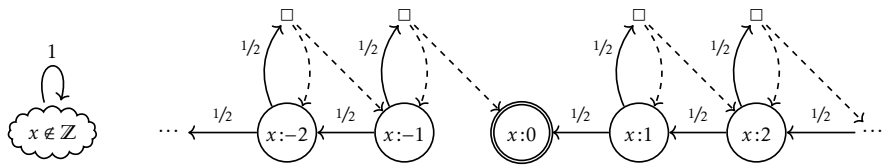

Figure 6.3: Execution of the demonically symmetric random walk. The □ nodes with the dashed arrows represent nondeterministic choices. The values of p and d are constantly 1/2 and 1, respectively. The fact that x is not integer–valued is invariant under iteration of the loop body and thus that set reaches itself with probability 1.

$$
\begin{aligned}
&+\ [x \neq 0] \cdot \tfrac{1}{2} \cdot \Big([x-1 \in \mathbb{N}] + \max\{ [x+1 \in \mathbb{N}],\, [x \in \mathbb{N}] \} \Big) \\
&= [x = 0] \cdot [x \in \mathbb{N}] \ +\ [x \neq 0] \cdot \tfrac{1}{2} \cdot \Big([x \in \mathbb{N}] + [x \in \mathbb{N}] \Big) \\
&= [x = 0] \cdot [x \in \mathbb{N}] \ +\ [x \neq 0] \cdot [x \in \mathbb{N}] \\
&= [x \in \mathbb{N}] \\
&= [I] \ \geq\ [I]
\end{aligned}
$$

We also check that x is an awp–superinvariant with respect to x:

$$
\begin{aligned}
&{}^{\mathsf{awp}}_{\langle x \neq 0, body \rangle} \Phi_V(V) \\
&= [x = 0] \cdot V \ +\ [x \neq 0] \cdot \mathsf{awp}\, [\![body]\!]\, ([x \in \mathbb{N}] \cdot x + [x \notin \mathbb{N}]) \\
&\leq [x = 0] \cdot V \ +\ [x \neq 0] \cdot \mathsf{awp}\, [\![body]\!]\, ([x \in \mathbb{N}] \cdot x) \\
&\qquad +\ [x \neq 0] \cdot \mathsf{awp}\, [\![body]\!]\, ([x \notin \mathbb{N}]) \\
&\qquad\qquad \text{(sublinearity of awp, Theorem 4.21 B.)} \\
&= [x = 0] \cdot V \ +\ [x \neq 0] \cdot \tfrac{1}{2} \Big(\\
&\qquad [x-1 \in \mathbb{N}] \cdot (x-1) + \max\{ [x \in \mathbb{N}] \cdot x,\, [x+1 \in \mathbb{N}] \cdot (x+1) \} \\
&\qquad +\ [x-1 \notin \mathbb{N}] + \max\{ [x \notin \mathbb{N}],\, [x+1 \notin \mathbb{N}] \} \Big) \\
&= [x = 0] \cdot V \ +\ [x \neq 0] \cdot \tfrac{1}{2} \Big([x-1 \in \mathbb{N}] \cdot (x-1) + [x \in \mathbb{N}] \cdot (x+1) \\
&\qquad +\ [x-1 \notin \mathbb{N}] + [x \notin \mathbb{N}] \Big) \\
&= [x = 0] \cdot V \ +\ [x \neq 0] \cdot \tfrac{1}{2} \Big([x \in \mathbb{N}] \cdot (x-1) + [x \in \mathbb{N}] \cdot (x+1) \\
&\qquad +\ [x \notin \mathbb{N}] + [x \notin \mathbb{N}] \Big) \\
&= [x = 0] \cdot V \ +\ [x \neq 0] \cdot \tfrac{1}{2} \Big(2\,[x \in \mathbb{N}] \cdot x + 2\,[x \notin \mathbb{N}] \Big) \\
&= [x = 0] \cdot V \ +\ [x \neq 0] \cdot \Big([x \in \mathbb{N}] \cdot x + [x \notin \mathbb{N}] \Big) \\
&= [x = 0] \cdot V \ +\ [x \neq 0] \cdot V \ =\ V
\end{aligned}
$$

Lastly, we show that V, p, and d satisfy the progress condition:

$$
\begin{aligned}
& p \circ V \cdot [\varphi] \cdot [I] \;\leq\; \lambda\sigma.\ \mathsf{wp}\,[\![body]\!]\left(\left[V \leq V(\sigma) - d\Big(V(\sigma)\Big)\right]\right)(\sigma) \\
\text{iff}\quad & \tfrac{1}{2} \circ \Big(\ \cdots\ \Big) \cdot [x \neq 0] \cdot [x \in \mathbb{N}] \\
& \qquad \leq\; \lambda\sigma.\ \mathsf{wp}\,[\![body]\!]\,([V \leq V(\sigma) - 1])(\sigma) \\
\text{iff}\quad & \tfrac{1}{2} \cdot [x \in \mathbb{N}_{\geq 1}] \;\leq\; \lambda\sigma.\ \mathsf{wp}\,[\![body]\!]\,([V \leq V(\sigma) - 1])(\sigma) \\
\text{iff}\quad & \tfrac{1}{2} \cdot [x \in \mathbb{N}_{\geq 1}] \;\leq\; \frac{1}{2}\Big([V\,[x/x-1] \leq V - 1] + \max\{\ldots\}\Big) \\
\text{implied by}\quad & \tfrac{1}{2} \cdot [x \in \mathbb{N}_{\geq 1}] \;\leq\; \tfrac{1}{2}\,[V\,[x/x-1] \leq V - 1] \\
\text{iff}\quad & \tfrac{1}{2} \cdot [x \in \mathbb{N}_{\geq 1}] \;\leq\; [x \in \mathbb{N}_{\geq 1}] \cdot \tfrac{1}{2}\,[V\,[x/x-1] \leq V - 1] \\
\text{iff}\quad & \tfrac{1}{2} \cdot [x \in \mathbb{N}_{\geq 1}] \;\leq\; [x \in \mathbb{N}_{\geq 1}] \cdot \tfrac{1}{2}\,[x - 1 \leq x - 1] \\
& \qquad \text{(by careful analysis of } V\,[x/x-1] \text{ and } V \text{ given } x \in \mathbb{N}_{\geq 1}) \\
\text{iff}\quad & \tfrac{1}{2} \cdot [x \in \mathbb{N}_{\geq 1}] \;\leq\; [x \in \mathbb{N}_{\geq 1}] \cdot \tfrac{1}{2}
\end{aligned}
$$

The last inequality is obviously true. This shows that all preconditions of Theorem 6.8 are satisfied and as a consequence the demonically symmetric random walk terminates almost–surely from any initial state where x is integer–valued.

Coming back to our motivation, the procedure P' given by

$$P' \;\triangleright\quad \{\mathtt{skip}\}\,[1/2]\,\{\mathtt{call}\ P';\ \mathtt{call}\ P';\ \{\mathtt{call}\ P'\} \,\square\, \{\mathtt{skip}\}\}\ ,$$

i.e. potentially three consecutive procedure calls instead of just two procedure calls, interestingly is not almost–surely terminating: it terminates only with probability $(\sqrt{5}-1)/2 < 1$ [Olm+16].

6.2.4.2 *The Symmetric-in-the-Limit Random Walk*

While so far we have considered only constant probability and decrease functions, we now consider a while loop requiring a *non–constant* decrease function d. For that, consider the following while loop:[10]

$$
\begin{array}{l}
\mathtt{while}\,(x > 0)\,\{ \\
\quad q := x/2x+1; \\
\quad \{x := x - 1\}\,[q]\,\{x := x + 1\} \\
\}
\end{array}
$$

In order not to clutter the reasoning below, we assume that x is of type $\mathbb{N}$. The execution of the loop is illustrated in Figure 6.4.

Intuitively, the loop models an asymmetric random walk of a particle x, terminating when the particle hits the origin 0. In one iteration of the loop

10 This example is due to McIver & Morgan [MM16].

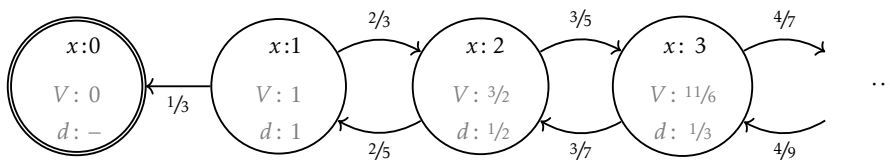

Figure 6.4: Execution of the symmetric-in-the-limit random walk. Inside the nodes we give the valuations of variable x as well as the values of the variant V and the decrease function d. The value of p is constantly 1/3.

body, the program either with probability $x/2x+1$ decrements the position of x by one, or with probability $x+1/2x+1$ increments the position of x by one. The further the particle x is away from 0, the more symmetric becomes the random walk since $x/2x+1$ approaches 1/2 asymptotically. Yet, it is not so obvious that this random walk indeed also terminates with probability 1.

Proof of almost–sure termination. We choose the witnesses

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

$$\text{and} \quad p(v) = \frac{1}{3},$$

where H_x is the x-th harmonic number.[11] Intuitively, these witnesses tell us that the variant V, i.e. the harmonic number of the value of x, decreases with probability at least 1/3 by at least $\frac{1}{x}$ through one loop iteration if initially $x > 0$.

Notice furthermore that while d measures precisely the potential decrease of V, the real probability to decrease V is monotonically *increasing* whereas Theorem 6.8 calls for an *antitone, thus monotonically decreasing*, p. The remedy here is that the decrease probability is globally lower–bounded by the constant 1/3 and thus an antitone probability function exists.

Let us now check that all premises of Theorem 6.8 are met: p is constant and thus obviously antitone. true is a wp–subinvariant of any loop that terminates almost–surely. This is especially the case when the loop body itself is loop–free. $V = 0$ indicates termination since $V = 0$ iff $x \leq 0$ (because x is assumed to be of type $\mathbb{N}$).

Next, we provide a detailed check that V is an awp–supermartingale:

$$\overset{\mathsf{awp}}{\langle x>0, body\rangle}\Phi_V(V)$$

11 Formally, $H_x = \sum_{n=1}^{x} \frac{1}{n}$. Notice that $H_0 = 0$.

$$
\begin{aligned}
&= \overset{\text{awp}}{\langle x>0, body\rangle}\Phi_{H_x}(H_x)\\
&= [x \le 0]\cdot H_x \;+\; [x>0]\cdot \text{awp}\,[\![body]\!]\,(H_x)\\
&= [x \le 0]\cdot H_x \;+\; [x>0]\cdot \left(\frac{x}{2x+1}\cdot H_{x-1} + \left(1-\frac{x}{2x+1}\right)\cdot H_{x+1}\right)\\
&= [x \le 0]\cdot H_x \;+\; [x>0]\cdot \left(\frac{x}{2x+1}\cdot \left(H_x - \frac{1}{x}\right) + \left(\frac{x+1}{2x+1}\right)\cdot \left(H_x + \frac{1}{x+1}\right)\right)\\
&= [x \le 0]\cdot H_x \;+\; [x>0]\cdot \left(\left(\frac{x}{2x+1} + \frac{x+1}{2x+1}\right)\cdot H_x - \frac{1}{2x+1} + \frac{1}{2x+1}\right)\\
&= [x \le 0]\cdot H_x \;+\; [x>0]\cdot H_x\\
&= H_x\\
&= V \;\preceq\; V
\end{aligned}
$$

Lastly, we show that V, p, and d satisfy the progress condition. For that, note that $d(H_n) = 1/n$ and consider the following:

$$
\begin{aligned}
& p \circ V \cdot [\varphi]\cdot[I]\\
&\qquad \le\; \lambda\sigma.\ \text{wp}\,[\![body]\!]\left(\left[V \le V(\sigma) - d\big(V(\sigma)\big)\right]\right)(\sigma)\\
\text{iff}\quad & \frac{1}{3}\circ H_x\cdot[x>0]\cdot[\text{true}]\\
&\qquad \le\; \lambda\sigma.\ \text{wp}\,[\![body]\!]\left(\left[H_x \le H_{x(\sigma)} - d\big(H_{x(\sigma)}\big)\right]\right)(\sigma)\\
\text{iff}\quad & \frac{1}{3}\cdot[x>0] \;\le\; \lambda\sigma.\ \text{wp}\,[\![body]\!]\left(\left[H_x \le H_{x(\sigma)} - \frac{1}{H_{x(\sigma)}}\right]\right)(\sigma)\\
\text{iff}\quad & \frac{1}{3}\cdot[x>0] \;\le\; \lambda\sigma.\ \left(\frac{x}{2x+1}\cdot\left[H_{x-1} \le H_{x(\sigma)} - \frac{1}{H_{x(\sigma)}}\right]\right.\\
&\qquad\qquad\qquad \left. +\;\left(1-\frac{x}{2x+1}\right)\cdot\left[H_{x+1} \le H_{x(\sigma)} - \frac{1}{H_{x(\sigma)}}\right]\right)(\sigma)\\
\text{iff}\quad & \frac{1}{3}\cdot[x>0] \;\le\; \frac{x}{2x+1}\cdot\left[H_{x-1} \le H_x - \frac{1}{H_x}\right]\\
&\qquad\qquad\qquad +\;\frac{x+1}{2x+1}\cdot\left[H_{x+1} \le H_x - \frac{1}{H_x}\right]\\
\text{implied by}\quad & \frac{1}{3}\cdot[x>0] \;\le\; [x>0]\cdot\frac{x}{2x+1}\cdot\left[H_{x-1} \le H_x - \frac{1}{H_x}\right]\\
\text{iff}\quad & \frac{1}{3}\cdot[x>0] \;\le\; [x>0]\cdot\frac{x}{2x+1}\cdot[\text{true}]\\
\text{iff}\quad & \frac{1}{3}\cdot[x>0] \;\le\; [x>0]\cdot\frac{x}{2x+1}
\end{aligned}
$$

The last line is true for all natural numbers $x > 0$. This shows that all preconditions of Theorem 6.8 are satisfied and as a consequence the symmetric-in-the-limit random walk terminates almost–surely.

Non–existence of an affine variant. For this program, note that our variant was *non–affine*, i.e. not of the form $a + bx + cq$. In fact, there exists *no affine variant* that satisfies the superinvariant property. Such affine variants are used e.g. by [CNZ17]. Any affine[12] variant V would be of the form

$$V \;=\; a + bx + cq\,,$$

for some (positive) coefficients a, b, c. [13] Now we attempt to check the superinvariant property for a variant of that form:

$$\begin{aligned}
&{}^{\mathsf{awp}}_{\langle x>0, body\rangle}\Phi_V(V)\\
&= {}^{\mathsf{awp}}_{\langle x>0, body\rangle}\Phi_{a+bx+cq}(a+bx+cq)\\
&= [x \le 0]\cdot x \;+\; [x>0]\cdot \mathsf{awp}\,[\![body]\!]\,(a+bx+cq)\\
&= [x \le 0]\cdot x \;+\; [x>0]\cdot\left(a - 2b\cdot\frac{x}{2x+1} + bx + b + c\cdot\frac{x}{2x+1}\right)\\
&\overset{!}{\le} a + bx + cq \;=\; V
\end{aligned}$$

For $x \le 0$ this is trivially satisfied. For $x > 0$, the above is satisfied iff

$$\begin{aligned}
& a - 2b\cdot\frac{x}{2x+1} + bx + b + c\cdot\frac{x}{2x+1} \;\le\; a + bx + cq\\
\text{iff}\quad & -2b\cdot\frac{x}{2x+1} + b + c\cdot\frac{x}{2x+1} \;\le\; cq\,,
\end{aligned}$$

which is only satisfiable for all possible valuations of q and $x > 0$ iff $b = c = 0$. Thus, if V is required to be affine, then V has to be constantly a, for $a \ge 0$. Indeed, a is a superinvariant. However, it is clear that the constant a cannot possibly indicate termination, i.e. clearly

$$[a = 0] \;\neq\; [x \le 0]\,.$$

Thus, there cannot exist an affine superinvariant that proves termination of symmetric–in–the–limit while loop.

6.2.4.3 *The Escaping Spline*

We now consider a while loop where we will make use of a non–constant probability function p. Consider the following while loop:[14]

$$\begin{aligned}
&\texttt{while}\,(x>0)\,\{\\
&\quad q := 1/_{x+1};\\
&\quad \{x := 0\}\,[q]\,\{x := x+1\}
\end{aligned}$$

12 Some authors call this a *linear* variant.

13 Coefficients need to be positive because otherwise $V \ge 0$ cannot be ensured. However, this is not crucial in this proof.

14 This example is due to McIver & Morgan [MM16].

}

Assume again that $x \in \mathbb{N}$. The execution of the loop is illustrated in Figure 6.5. Intuitively, the loop models a random walk of a particle x that terminates when the particle hits the origin 0. The random walk either with probability $1/x+1$ immediately terminates or with probability $x/x+1$ increments the position of x by one. This means that for each iteration where the loop does not terminate, it becomes even *more likely not to terminate in the next iteration*. Thus, the longer the loop runs, the less likely it will terminate since the probability to continue looping approaches 1 asymptotically. Yet this loop terminates almost–surely, as we will now prove.

Proof of almost–sure termination. We choose witnesses

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

Intuitively this tells us that x decreases with probability at least $1/x+1$ by at least 1 through one loop iteration if initially $x > 0$.

Notice that while the variant function measures precisely the potential decrease in each state, the actual decrease is monotonically *increasing* the further we move away from $x = 0$, whereas Theorem 6.8 calls for an *antitone*, *thus monotonically decreasing* decrease function. The remedy here is that the decrease is globally lower–bounded by 1 and thus a constant — and hence antitone — decrease function exists.

Let us now check that all premises of Theorem 6.8 are met: d is constant and thus obviously antitone. true is a wp–subinvariant of any loop that terminates almost–surely. This is especially the case when the loop body itself is loop–free. $V = 0$ indicates termination since $V = 0$ iff $x \leq 0$ (since $x \in \mathbb{N}$).

Next, we provide a detailed check that V is an awp–supermartingale:

$$\begin{aligned}
&{}^{\mathsf{awp}}_{\langle x>0, body\rangle}\Phi_V(V) \\
&= {}^{\mathsf{awp}}_{\langle x>0, body\rangle}\Phi_x(x) \\
&= [x \leq 0] \cdot x \;+\; [x > 0] \cdot \mathsf{awp}\,[\![body]\!]\,(x) \\
&= [x \leq 0] \cdot x \;+\; [x > 0] \cdot \left(\frac{1}{x+1} \cdot 0 + \left(1 - \frac{1}{x+1}\right) \cdot (x+1)\right) \\
&= [x \leq 0] \cdot x \;+\; [x > 0] \cdot \left(\frac{1}{x+1} \cdot 0 + \frac{x}{x+1} \cdot (x+1)\right) \\
&= [x \leq 0] \cdot x \;+\; [x > 0] \cdot x \\
&= x \\
&= V \;\leq\; V
\end{aligned}$$

Finally, we show that V, p, and d satisfy the progress condition:

$$p \circ V \cdot [\varphi] \cdot [I] \;\leq\; \lambda\sigma.\ \mathsf{wp}\,[\![body]\!]\left(\left[V \leq V(\sigma) - d\Big(V(\sigma)\Big)\right]\right)(\sigma)$$

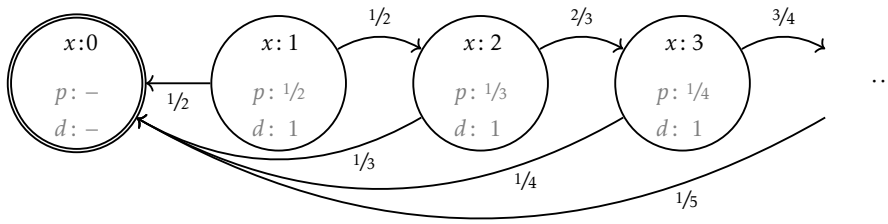

Figure 6.5: Execution of the escaping spline loop. The value of the variant V is equal to the value of the variable x in each state. Inside the nodes we give the valuations of variable x as well as the values of the probability function p and the decrease function d in each state.

$$
\begin{aligned}
\text{iff}\quad & \left(\lambda v.\ \frac{1}{v+1}\right) \circ x \cdot [x > 0] \cdot [\mathsf{true}] \\
& \quad \leq\ \lambda\sigma.\ \mathsf{wp}\,[\![body]\!]\left(\left[x \leq x(\sigma) - (\lambda v.\ 1)\big(x(\sigma)\big)\right]\right)(\sigma) \\
\text{iff}\quad & \frac{1}{x+1} \cdot [x > 0]\ \leq\ \lambda\sigma.\ \mathsf{wp}\,[\![body]\!]\,([x \leq x(\sigma) - 1])\,(\sigma) \\
\text{iff}\quad & \frac{1}{x+1} \cdot [x > 0] \\
& \quad \leq\ \lambda\sigma.\ \left(\frac{1}{x+1} \cdot [0 \leq x(\sigma) - 1] + \frac{x}{x+1} \cdot [x+1 \leq x(\sigma) - 1]\right)(\sigma) \\
\text{iff}\quad & \frac{1}{x+1} \cdot [x > 0]\ \leq\ \frac{1}{x+1} \cdot [0 \leq x - 1] + \frac{x}{x+1} \cdot [x+1 \leq x - 1] \\
\text{iff}\quad & \frac{1}{x+1} \cdot [x > 0]\ \leq\ \frac{1}{x+1} \cdot [x > 0] \cdot [0 \leq x - 1] + \frac{x}{x+1} \cdot [\mathsf{false}] \\
\text{iff}\quad & \frac{1}{x+1} \cdot [x > 0]\ \leq\ \frac{1}{x+1}
\end{aligned}
$$

This shows that all preconditions of Theorem 6.8 are satisfied and as a consequence the escaping spline loop terminates almost–surely.