PROOF RULES FOR LOOPS

5

Reasoning about loops is one of the most — if not *the* most — difficult tasks in verification. For nonprobabilistic programs, this is usually done using loop invariants and loop variants. Roughly speaking, loop invariants allow proving partial correctness, meaning the algorithm is correct if it terminates. Loop variants, on the other hand, enable proving termination. Partial correctness and termination together give total correctness.

For probabilistic programs, neither correctness nor termination are strictly binary properties: Monte Carlo algorithms, for instance, typically trade off 100% correctness for runtime efficiency, thus giving correct answers to otherwise difficult problems only with high probability but make up for it with short expected runtime. In order to account for those quantitative aspects, techniques for reasoning about the correctness of randomized algorithms need to naturally also be of quantitative nature. Amongst others, Kozen, McIver & Morgan, Jones, and also ourselves have provided quantitative analogs to invariant–style reasoning about probabilistic loops. In this chapter, we survey those proof rules.

After recapping how to lift invariant–style reasoning from nonprobabilistic to probabilistic loops, we survey and discuss proof rules for proving bounds (both upper and lower) on weakest preexpectations and weakest liberal preexpectations. In particular, we discuss in some detail the problem of obtaining lower bounds on weakest preexpectations, i.e. lower bounds on least fixed points. All proof rules have been translated into our weakest preexpectation setting so that we can give a unified overview and comparison.

5.1 INVARIANTS

All proof rules we present in this chapter make in one way or another use of a probabilistic, or rather quantitative, notion of invariants. In order to transit from Boolean to quantitative reasoning, let us briefly recap invariant–style reasoning about partial correctness of *nonprobabilistic* while loops: Given a precondition G and a postcondition F, say we want to prove that if executing $\texttt{while}(\varphi)\{C\}$ on an initial state $\sigma \models G$ terminates, then it does so in a final state $\tau \models F$. For that, we have to find a predicate I such that

$$G \implies I \quad \text{and} \quad \neg\varphi \wedge I \implies F \quad \text{and} \quad \langle\, \varphi \wedge I \,\rangle\, C \,\langle\, I \,\rangle \text{ is valid,} \tag{5.1}$$

where we mean validity for partial correctness. Any I for which the Hoare triple $\langle\, \varphi \wedge I \,\rangle\, C \,\langle\, I \,\rangle$ is valid for partial correctness is called a *loop invariant*:

If the loop $\texttt{while}(\varphi)\{C\}$ is started in a state satisfying both loop guard φ and invariant I and one execution of the loop body C terminates from that state, then the execution of C terminates in a state that again satisfies I. Thus, satisfaction of I is *invariant under (guarded) iteration* of the loop body.[1]

Why do invariants do the trick? Because we can now apply the while rule for partial correctness of Hoare logic which reads as follows:

$$\frac{\langle \varphi \wedge I \rangle\, C\, \langle I \rangle}{\langle I \rangle\, \texttt{while}(\varphi)\{C\}\, \langle \neg\varphi \wedge I \rangle} \text{ (while–partial)} \tag{5.2}$$

We can now combine the while–partial rule above with the consequence rule of Hoare logic (see Section 4.2.4, Relation to the consequence rule) into a single proof tree and so obtain the full proof of partial correctness, namely

$$\frac{G \implies I \qquad \dfrac{\langle \varphi \wedge I \rangle\, C\, \langle I \rangle}{\langle I \rangle\, \texttt{while}(\varphi)\{C\}\, \langle \neg\varphi \wedge I \rangle} \qquad \neg\varphi \wedge I \implies F}{\langle G \rangle\, \texttt{while}(\varphi)\{C\}\, \langle F \rangle}\,,$$

which can be stated as a single inference rule:

$$\frac{G \implies I \qquad \langle \varphi \wedge I \rangle\, C\, \langle I \rangle \qquad \neg\varphi \wedge I \implies F}{\langle G \rangle\, \texttt{while}(\varphi)\{C\}\, \langle F \rangle} \text{ (while–partial2)}$$

In the realm of weakest precondition reasoning, the premises $\langle \varphi \wedge I \rangle\, C\, \langle I \rangle$ and $\neg\varphi \wedge I \implies F$ together are equivalent to

$$[I] \;\preceq\; {}^{\mathsf{wlp}}\Phi_{[F]}([I])\,,$$

where ${}^{\mathsf{wlp}}\Phi_{[F]}$ is the wlp–characteristic function of $\texttt{while}(\varphi)\{C\}$ with respect to postcondition $[F]$ (see Definition 4.5 E.). This can be seen by

$$\begin{aligned}
& \neg\varphi \wedge I \implies F \\
\text{iff}\quad & [\neg\varphi]\cdot[I] \;\preceq\; [F] \\
\text{iff}\quad & [\neg\varphi]\cdot[I] \;\preceq\; [\neg\varphi]\cdot[F] && \text{(by case distinction) (†)}
\end{aligned}$$

and

$$\begin{aligned}
& \langle \varphi \wedge I \rangle\, C\, \langle I \rangle \\
\text{iff}\quad & \varphi \wedge I \implies \mathsf{wlp}\,[\![C]\!]\,(I) \\
\text{iff}\quad & [\varphi]\cdot[I] \;\preceq\; \mathsf{wlp}\,[\![C]\!]\,([I]) \\
\text{iff}\quad & [\varphi]\cdot[I] \;\preceq\; [\varphi]\cdot\mathsf{wlp}\,[\![C]\!]\,([I]) && \text{(by case distinction)} \\
\text{iff}\quad & [\neg\varphi]\cdot[I] + [\varphi]\cdot[I] \;\preceq\; [\neg\varphi]\cdot[F] + [\varphi]\cdot\mathsf{wlp}\,[\![C]\!]\,([I]) && \text{(by (†) above)} \\
\text{iff}\quad & [I] \;\preceq\; {}^{\mathsf{wlp}}\Phi_{[F]}([I])\,. && \big(\text{by definition of } {}^{\mathsf{wlp}}\Phi_{[F]}\text{, Definition 4.5 E.}\big)
\end{aligned}$$

1 By "guarded iteration" we mean iterating the loop body only if the loop guard is true.

In the language of our weakest precondition calculi, the (while–partial2)–rule thus reads as follows:

$$\frac{[G] \preceq [I] \preceq {}^{\mathsf{wlp}}_{\langle\varphi,C\rangle}\Phi_{[F]}([I])}{[G] \preceq \mathsf{wlp}\,[\![\texttt{while}(\varphi)\{C\}]\!]\,([F])}$$

For our definition of quantitative invariants, we lift the above rule to weakest preexpectations in a straightforward way. Furthermore, we distinguish between super- and subinvariants.

DEFINITION 5.1 (Invariants):
Let Φ_f be the wp*–characteristic function of* $\texttt{while}(\varphi)\{C\}$ *with respect to postexpectation $f \in \mathbb{E}$ and let $I \in \mathbb{E}$. Then:*

A. *I is called a* wp*–superinvariant of* $\texttt{while}(\varphi)\{C\}$ *with respect to postexpectation f, iff*

$$\Phi_f(I) \preceq I\,.$$

B. *I is called a* wp*–subinvariant of* $\texttt{while}(\varphi)\{C\}$ *with respect to postexpectation f, iff*

$$I \preceq \Phi_f(I)\,.$$

C. *Super- and subinvariants for* wlp, awp, *and* awlp *are defined analogously by means of* wlp–, awp–, *and* awlp*–characteristic functions, respectively. Notice that* wlp– *and* awlp*–invariants are of type $\mathbb{E}_{\leq 1}$ rather than $\mathbb{E}$.*

The I we used to illustrate the while–rule for partial correctness (Rule 5.2 above) would be a wlp–subinvariant in the terminology of Definition 5.1.

Remark 5.2 (On Terminology in Related Literature). Our *subinvariants* correspond to *probabilistic invariants* in the terminology of McIver & Morgan (see [MM05, Definition 2.2.1, p. 39]) up to a slight technical difference: McIver & Morgan call I a probabilistic invariant iff

$$[\varphi]\cdot I \preceq \mathsf{wp}\,[\![C]\!]\,(I)\,,$$

which is implied by $I \preceq \Phi_f(I)$, but the converse implication is not true in general for arbitrary postexpectations f. However, McIver & Morgan do not consider arbitrary postexpectations f, but instead argue only about weakest preexpectations of loops with respect to postexpectation $[\neg\varphi]\cdot I$ and we have

$$[\varphi]\cdot I \preceq \mathsf{wp}\,[\![C]\!]\,(I) \quad \text{iff} \quad I \preceq \Phi_{[\neg\varphi]\cdot I}(I)\,,$$

as the following reasoning shows:

$$
\begin{aligned}
& I \preceq \Phi_{[\neg\varphi]\cdot I}(I) \\
\text{iff}\quad & [\neg\varphi]\cdot I + [\varphi]\cdot I \preceq [\neg\varphi]\cdot[\neg\varphi]\cdot I + [\varphi]\cdot \mathsf{wp}\,[\![C]\!]\,(I) \\
\text{iff}\quad & [\neg\varphi]\cdot I + [\varphi]\cdot I \preceq [\neg\varphi]\cdot I + [\varphi]\cdot \mathsf{wp}\,[\![C]\!]\,(I) \\
\text{iff}\quad & [\neg\varphi]\cdot I \preceq [\neg\varphi]\cdot I \quad \text{and} \quad [\varphi]\cdot I \preceq +[\varphi]\cdot \mathsf{wp}\,[\![C]\!]\,(I) \\
\text{iff}\quad & [\varphi]\cdot I \preceq +[\varphi]\cdot \mathsf{wp}\,[\![C]\!]\,(I)
\end{aligned}
$$

Our definition of subinvariants is therefore not a restriction compared to McIver & Morgan's probabilistic invariants.

Our *superinvariants* correspond to *supermartingales* in the terminology used by Chakarov & Sankaranarayanan [CS14], Fioriti & Hermanns [FH15], and Chatterjee *et al.* [CFG16; Cha+16; CF17; CNZ17; ACN18] with basically the same technical difference as above.

Generally speaking, sub– and superinvariants in our terminology can be conceived of, respectively, as sub– and supermartingales of the stochastic process that can naturally be associated to a probabilistic loop. △

Next, we introduce a concept we call ω–invariants. These are basically sequences of expectations that are invariants relative to each other. We will make use of those for reasoning about lower bounds on least fixed points and dually upper bounds on greatest fixed points.

DEFINITION 5.3 (ω–Invariants):

A. *Let Φ be the* wlp*–characteristic function of* `while`$(\varphi)\{C\}$ *with respect to postexpectation f and let $(I_n)_{n\in\mathbb{N}} \subset \mathbb{E}_{\leq 1}$ be a monotonically decreasing*[2] *sequence with $I_0 = 1$.*

Then $(I_n)_{n\in\mathbb{N}}$ is called a wlp*–ω–superinvariant of* `while`$(\varphi)\{C\}$ *with respect to postexpectation $f \in \mathbb{E}_{\leq 1}$, iff*

$$\forall\, n \in \mathbb{N}\colon \quad \Phi(I_n) \preceq I_{n+1}\,.$$

B. *Let Φ be the* wp*–characteristic function of* `while`$(\varphi)\{C\}$ *with respect to postexpectation f and let $(I_n)_{n\in\mathbb{N}} \subset \mathbb{E}$ be a monotonically increasing*[3] *sequence with $I_0 = 0$.*

Then $(I_n)_{n\in\mathbb{N}}$ is called a wp*–ω–subinvariant of* `while`$(\varphi)\{C\}$ *with respect to postexpectation f, iff*

$$\forall\, n \in \mathbb{N}\colon \quad I_{n+1} \preceq \Phi(I_n)\,.$$

C. awlp*–ω–superinvariants and* awp*–ω–subinvariants are analogously defined by means of* awlp*– and* awp*–characteristic functions.*

2 But not necessarily *strictly* decreasing.
3 But not necessarily *strictly* increasing.

Using such sequences to reason about the correctness of programs is to the best of our knowledge originally due to Jones [Jon90, p. 124]. In her thesis, she basically used what we here call wp–ω–subinvariants for a total–correctness logic. Audebaud & Paulin–Mohring later build upon Jones' ideas and use monotonically increasing sequences to reason about total correctness of randomized algorithms in Coq [APM09, Section 4.4].

5.2 BOUNDS ON EXPECTED VALUES

Bounds on expected values, i.e. bounds on preexpectations, are a key concept in reasoning about probabilistic programs. Several correctness properties can be expressed as either upper or lower bounds on preexpectations. For example, we have already seen that the probability of event A can be coded as the expected value of the event's characteristic function $[A]$. Verifying bounds on probabilities is also the main task of the model checking problem of probabilistic logics like PCTL [HJ94].

Reasoning loop–free programs is mostly straightforward. Weakest preexpectations can be computed in practice.[4] For while loops, the situation is more difficult: Weakest (liberal) preexpectations of loops are defined as fixed points and those are in general non–computable. All non–trivial approximations of the fixed points are non–computable as well (see Part III).

In this section, we thus describe proof rules that can aid in reasoning about weakest (liberal) preexpectations of loops. We first describe inductive proof rules that allow for reasoning about upper bounds on wp and awp and coinductive proof rules that are suitable for lower bounds on wlp and awlp. We also briefly discuss the problem of coinduction for lower bounds on wp. Thereafter, we describe what we call ω–rules for reasoning about lower bounds on wp and awp, and upper bounds on wlp and awlp. We then survey proof rules by McIver & Morgan for lower bounds on wp and finally show how any bound can potentially be tightened.

5.2.1 *Induction for Weakest Preexpectations*

Induction on natural numbers is a well–known proof principle which can be traced back to classical antiquity, e.g. Euclid's proof that the number of primes is infinite. The induction principle states that in order to prove that a predicate F is true for all natural numbers, it suffices to prove that both

A. $0 \models F$, and

B. $n \models F$ implies $n+1 \models F$

are true. We can reformulate induction over the natural numbers in the setting of continuous functions on complete lattices [Rot16, Section 2.1]: We

4 I.e. in case the postexpectation is computable.

choose the complete lattice $(\mathcal{P}(\mathbb{N}), \subseteq)$, the continuous function

$$\Phi(X) \;=\; \{0\} \cup \{n+1 \mid n \in X\}\,, \tag{5.3}$$

and conceive of the predicate F as a set $F \in \mathcal{P}(\mathbb{N})$. We can easily convince ourselves that $\mathbb{N}$ is the least fixed point of Φ and that checking A. and B. above together amounts to checking whether $\Phi(F) \subseteq F$. The induction principle for the natural numbers then tells us that

$$\Phi(F) \;\subseteq\; F \quad \text{implies} \quad \mathsf{lfp}\,\Phi \;\subseteq\; F\,. \tag{5.4}$$

Since $\mathsf{lfp}\,\Phi = \mathbb{N}$, thus $\mathbb{N} \subseteq F$, and $\mathbb{N}$ is the greatest element in $\mathcal{P}(\mathbb{N})$, we can conclude that $F = \mathbb{N}$ and thus F holds for all numbers.

Implication 5.4 above is a special case of a more general principle (see Lemma A.6): Let $(D, \sqsubseteq)$ be any complete lattice and let $\Phi\colon D \to D$ be any continuous self–map on D. Then

$$\forall\, d \in D\colon \quad \Phi(d) \;\sqsubseteq\; d \quad \text{implies} \quad \mathsf{lfp}\,\Phi \;\sqsubseteq\; d\,.$$

The above general principle is called *Park's Lemma*, *Scott induction* or simply *induction* [Rot16, Section 2]. Since weakest preexpectations are defined as least fixed points of continuous functions on complete lattices, we can make use of the induction principle in order to reason about upper bounds on weakest preexpectations:

THEOREM 5.4 (Induction for Upper Bounds on wp and awp[5]):
Let $I \in \mathbb{E}$ be a wp*–superinvariant of* $\texttt{while}(\varphi)\{C\}$ *with respect to post-expectation f (see* Definition 5.1 A.*). Then*

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

The analogous result for awp *holds as well.*

Proof. This is an instance of Park's Lemma (see Lemma A.6): Simply choose complete lattice $(\mathbb{E}, \preceq)$ and continuous function ${}^{\mathsf{wp}}_{\langle\varphi,C\rangle}\Phi_f$. Q.E.D.

EXAMPLE 5.5 (Upper Bounds on wp):
Consider the program C_{geo}, given by

$$\begin{aligned}
&c := 1 \,\fatsemi\\
&\texttt{while}(c = 1)\{\\
&\qquad \{c := 0\}\,[1/2]\,\{x := x+1\}\\
&\}\,,
\end{aligned}$$

5 For induction for tame programs, see [Koz85, the *while rule* on p. 168]

and suppose we want to reason about an upper bound on the expected value of x after execution of C_{geo}. To this end, we propose the wp–superinvariant

$$I \;=\; x + [c = 1]$$

and check its wp–superinvariance by applying the wp–characteristic function

$$\Phi(X) \;=\; [c \neq 1] \cdot x + [c = 1] \cdot \tfrac{1}{2}\Big(X\,[c/0] + X\,[x/x+1]\Big)\,,$$

to I, which gives us

$$\begin{aligned}
\Phi(I) \;&=\; \Phi\Big(x + [c = 1]\Big) \\
&=\; [c \neq 1] \cdot x + [c = 1] \cdot \tfrac{1}{2}\Big(x + [0 = 1] + x + 1 + [c = 1]\Big) \\
&=\; x + [c = 1] \cdot \tfrac{1}{2}\Big(0 + 1 + 1\Big) \\
&=\; x + [c = 1] \\
&=\; I \;\preceq\; I\,.
\end{aligned}$$

Thus the induction rule (Theorem 5.4) gives us that

$$\mathsf{wp}\,[\![\texttt{while}\,(\ldots\}]\!]\,(x) \;\preceq\; x + [c = 1] \tag{†}$$

and hence we get

$$\begin{aligned}
\mathsf{wp}\,[\![C_{geo}]\!]\,(x) \;&=\; \mathsf{wp}\,[\![c := 1 \fatsemi \texttt{while}\,(\ldots\}]\!]\,(x) \\
&=\; \mathsf{wp}\,[\![c := 1]\!]\,(\mathsf{wp}\,[\![\texttt{while}\,(\ldots\}]\!]\,(x)) \\
&\preceq\; \mathsf{wp}\,[\![c := 1]\!]\,(x + [c = 1]) \\
&\qquad\qquad \text{(by † and monotonicity, Theorem 4.16)} \\
&=\; x + [1 = 1] \\
&=\; x + 1
\end{aligned}$$

and therefore $x + 1$ (evaluated in the initial state) is an upper bound on the expected value of x (evaluated in the final states) after executing C_{geo}.

5.2.2 *Coinduction for Weakest Liberal Preexpectations*

The principle of *coinduction* is the dual of the induction principle and reads as follows [Rot16, Section 2]: Let $(D, \sqsubseteq)$ be any complete lattice and let $\Phi\colon D \to D$ be any continuous function. Then

$$\forall\, d \in D\colon \quad d \;\sqsubseteq\; \Phi(d) \quad \text{implies} \quad d \;\sqsubseteq\; \mathsf{gfp}\,\Phi\,.$$

For our example of the natural numbers, coinduction is not very interesting, since $\mathbb{N}$ is not only the least but also the greatest fixed point of Φ as defined

in Equation 5.3. For a predicate $F \in \mathcal{P}(\mathbb{N})$, we thus get by coinduction

$$F \subseteq \Phi(F) \quad \text{implies} \quad F \subseteq \mathbb{N}\,,$$

which, however, does not provide any information on F as the right–hand–side of the implication is vacuously true for any $F \in \mathcal{P}(\mathbb{N})$.

The particular problem we encounter with Φ here is that $\mathbb{N}$ is not only the greatest fixed point of Φ but indeed the greatest element in $\mathcal{P}(\mathbb{N})$ altogether. This is not the situation, however, for weakest liberal preexpectations: Those are defined as greatest fixed points and they may very well be below 1 — the greatest element in $(\mathbb{E}_{\leq 1}, \preceq)$. We may thus make use of the coinduction principle to reason about lower bounds on weakest liberal preexpectations:

Theorem 5.6 (Coinduction for Lower Bounds on wlp[6]):
Let $I \in \mathbb{E}_{\leq 1}$ be a wlp*–subinvariant of* $\texttt{while}(\varphi)\{C\}$ *with respect to post-expectation f (see* Definition 5.1 b.*). Then*

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

The analogous result for awlp *holds as well.*

Proof. This is an instance of Park's Lemma (see Lemma A.6): Simply choose complete lattice $(\mathbb{E}_{\leq 1}, \preceq)$ and continuous function ${}^{\mathsf{wlp}}_{\langle\varphi,C\rangle}\Phi_f$. Q.E.D.

Example 5.7 (Lower Bounds on wlp):
Reconsider the program C, given by

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

and suppose we want to reason about a lower bound on the probability that x is even after execution of C (if C terminates at all). To this end, we propose

$$I \;=\; [c \neq 1]\cdot[x \text{ even}] \;+\; [c = 1]\cdot\left(\frac{2}{3} + \frac{4\cdot[x \text{ odd}]}{15} + \frac{[x \text{ even}]}{15}\right)$$

as wlp–subinvariant and check wlp–subinvariance by applying the wlp–characteristic function

6 See [MM05, Lemma 7.2.2, p. 185].

$$\Phi(X) \;=\; [c \neq 1]\cdot[x \text{ even}] + [c=1]\cdot\left(\frac{1}{2} + \frac{X[x/x+1]}{4} + \frac{X[c,x/0,x+1]}{4}\right),$$

to I, which gives us

$$\begin{aligned}
\Phi(I) \;&=\; [c \neq 1]\cdot[x \text{ even}] + [c=1]\cdot\left(\frac{1}{2} + \frac{I[x/x+1]}{4} + \frac{I[c,x/0,x+1]}{4}\right)\\
&=\; [c \neq 1]\cdot[x \text{ even}] + [c=1]\cdot\left(\frac{1}{2} + [c\neq 1]\cdot\frac{\cdots}{4}\right.\\
&\qquad + [c=1]\cdot\left(\frac{2}{3\cdot 4} + \frac{4\cdot[x+1 \text{ odd}]}{15\cdot 4} + \frac{[x+1 \text{ even}]}{15\cdot 4}\right)\\
&\qquad \left. + [0\neq 1]\cdot\frac{[x+1 \text{ even}]}{4} + [0=1]\cdot(\ldots)\right)\\
&=\; [c \neq 1]\cdot[x \text{ even}]\\
&\qquad + [c=1]\cdot\left(\frac{1}{2} + \frac{2}{3\cdot 4} + \frac{4\cdot[x \text{ even}]}{15\cdot 4} + \frac{[x \text{ odd}]}{15\cdot 4} + \frac{[x \text{ odd}]}{4}\right)\\
&=\; [c \neq 1]\cdot[x \text{ even}] + [c=1]\cdot\left(\frac{2}{3} + \frac{[x \text{ even}]}{15} + \frac{4\cdot[x \text{ odd}]}{15}\right)\\
&=\; I \;\preceq\; I\,.
\end{aligned}$$

Thus the coinduction rule (Theorem 5.6) gives us that

$$\begin{aligned}
&[c \neq 1]\cdot[x \text{ even}] \;+\; [c=1]\cdot\left(\frac{2}{3} + \frac{4\cdot[x \text{ odd}]}{15} + \frac{[x \text{ even}]}{15}\right) \qquad (\dagger)\\
&\qquad \preceq\; \mathsf{wp}\,[\![\texttt{while}\ (\ldots)\}]\!]\,([x \text{ even}])
\end{aligned}$$

and hence we get

$$\begin{aligned}
&\mathsf{wp}\,[\![C]\!]\,([x \text{ even}])\\
&\;=\; \mathsf{wp}\,[\![c := 1\,;\,\texttt{while}\ (\ldots)\}]\!]\,([x \text{ even}])\\
&\;=\; \mathsf{wp}\,[\![c := 1]\!]\,(\mathsf{wp}\,[\![\texttt{while}\ (\ldots)\}]\!]\,([x \text{ even}]))\\
&\;\geq\; \mathsf{wp}\,[\![c := 1]\!]\left([c \neq 1]\cdot[x \text{ even}] + [c=1]\cdot\left(\frac{2}{3} + \frac{4\cdot[x \text{ odd}]}{15} + \frac{[x \text{ even}]}{15}\right)\right)\\
&\qquad\qquad \text{(by } \dagger \text{ above and monotonicity, Theorem 4.16)}\\
&\;=\; [1 \neq 1]\cdot[\ldots] \;+\; [1=1]\cdot\left(\frac{2}{3} + \frac{4\cdot[x \text{ odd}]}{15} + \frac{[x \text{ even}]}{15}\right)\\
&\;=\; \frac{2}{3} + \frac{4\cdot[x \text{ odd}]}{15} + \frac{[x \text{ even}]}{15}
\end{aligned}$$

and therefore $2/3 + 4\cdot[x \text{ odd}]/15 + [x \text{ even}]/15$ (evaluated in the initial state) is a lower

bound on the probability that C either diverges or terminates in a state where x is even.

5.2.3 *No Coinduction for Weakest Preexpectations*

We have seen in the previous subsection that induction allows us to *get above* a least fixed point whereas coinduction allows to *get below* a greatest fixed point. Unfortunately, *getting below a least fixed point* — and dually: *getting above a greatest fixed point* — is not associated with such elegant proof principles as induction or coinduction. In particular, for a complete lattice $(D, \sqsubseteq)$ and a continuous function $\Phi\colon D \to D$, the supposedly evident rules

$$\forall\, d \in D\colon \quad d \sqsubseteq \Phi(d) \quad \text{implies} \quad d \sqsubseteq \mathsf{lfp}\,\Phi\,, \qquad \lightning$$

and

$$\forall\, d \in D\colon \quad \Phi(d) \sqsubseteq d \quad \text{implies} \quad \mathsf{gfp}\,\Phi \sqsubseteq d \qquad \lightning$$

are both *unsound*, not only in general but also in our particular use case of preexpectations as the following counterexample demonstrates:

Counterexample 5.8 (Unsoundness of Coinduction for wp):
Consider the program C, given by

$$\begin{aligned}&\texttt{while}(c = 1)\{\\ &\quad \{c := 0\}\,[1/2]\,\{x := x+1\}^{\circ}_{\circ}\\ &\quad k := k+1\\ &\}\,,\end{aligned}$$

and suppose we want to incorrectly reason about a lower bound on the expected value of x after execution of C by coinduction. The wp–characteristic function of the while loop with respect to postexpectation x is given by

$$\Phi(X) \;=\; [c \neq 1]\cdot x + [c=1]\cdot \tfrac{1}{2}\Big(X\,[k, c/k+1, 0] + X\,[k, x/k+1, x+1]\Big)\,.$$

We now propose *infinitely many* fixed points of Φ, namely for every $a > 0$

$$I_a \;=\; x + [c=1]\left(2^{k+a}+1\right)$$

is a fixed point of Φ, as one can easily check. However, for any $d < b$, we clearly have $I_d \prec I_b$. Thus, if we prove $I_b \preceq \Phi(I_b)$ we cannot have proven that I_b is a lower bound on the least fixed point of Φ, since I_d is a fixed point strictly smaller than I_b. In fact, none of the I_a's are the least fixed point of Φ. The intuitive reason is that the expected value of x is completely independent of k but k has an influence on the value that the I_a's assume. $\boxed{\lightning}$

It is important to note that *unsoundness of coinductive premises in order to obtain lower bounds on* wp *is absolutely not evident*. We will see later in Chapter 7, that for *deterministic* programs Frohn *et al.* have shown that one *can* prove *lower bounds on runtimes of programs* from wp–subinvariants, which Frohn *et al.* call *metering functions* [Fro+16b]. This allows to lower bound a least fixed point from a coinductive premise (i.e. from a premise of the form $d \sqsubseteq \Phi(d)$). Transferring the metering function method to probabilistic programs, however, unfortunately fails in a way similar to the above counterexample, as we will see later in this thesis.

5.2.4 *ω–Rules*

In light of our just described inability to obtain lower bounds on weakest preexpectations, and dually upper bounds on weakest liberal preexpectations, by simple means such as coinduction or induction, we now present two alternative proof rules for obtaining precisely such desired bounds. These proof rules will be conceptually less elegant and consequently more difficult to apply, as they make use of ω–invariants. In particular, it will be necessary to find the limit of such ω–invariants in order to actually gain some insights from applying these rules. That basically just shifts the problem of obtaining bounds into the realm of real analysis. The rule for lower bounds on weakest preexpectations (*getting below a least fixed point*) reads as follows:

THEOREM 5.9 (Lower Bounds on wp and awp from ω–Invariants[7]):

A. *Let $(I_n)_{n\in\mathbb{N}}$ be a* wp*–ω–subinvariant of* $\texttt{while}(\varphi)\{C\}$ *with respect to postexpectation f (see* Definition 5.3 B.*). Then*

$$\sup_{n\in\mathbb{N}} I_n \preceq \mathsf{wp}\,[\![\texttt{while}(\varphi)\{C\}]\!]\,(f)\,.$$

B. *Let $(I_n)_{n\in\mathbb{N}}$ be a* wlp*–ω–superinvariant of* $\texttt{while}(\varphi)\{C\}$ *with respect to postexpectation f (see* Definition 5.3 A.*). Then*

$$\mathsf{wlp}\,[\![\texttt{while}(\varphi)\{C\}]\!]\,(f) \preceq \inf_{n\in\mathbb{N}} I_n\,.$$

C. *Analogous results for* awp *and* awlp *hold as well.*

Proof. We only prove A., because the proofs for B. and C. are analogous. Let Φ be the wp–characteristic function of $\texttt{while}(\varphi)\{C\}$ with respect to postexpectation f. We first prove by induction that

$$\forall\, n \in \mathbb{N}\colon \quad I_n \preceq \Phi^{n+1}(0)\,.$$

7 See also [Jon90, p. 124] and [APM09, Section 4.4].

For the induction base we have

$$I_0 \;=\; 0 \;\preceq\; \Phi(0)$$

trivially, since 0 is the least element in $\mathbb{E}$. For the induction step we assume induction hypothesis $I_n \preceq \Phi^{n+1}(0)$ and prove

$$\begin{aligned} I_{n+1} &\preceq \Phi(I_n) && \text{(by } (I_n)_{n\in\mathbb{N}} \text{ being a wp–}\omega\text{–subinv., Definition 5.3 B.)} \\ &\preceq \Phi\left(\Phi^{n+1}(0)\right) && \text{(by I.H. and monotonicity of } \Phi\text{, Theorem 4.16)} \\ &= \Phi^{n+2}(0)\,. \end{aligned}$$

Since $I_n \preceq \Phi^{n+1}(0)$ holds for all n and $\Phi^0(0) = 0$, we may take the supremum on both sides and conclude:

$$\begin{aligned} \sup_{n\in\mathbb{N}} I_n &\preceq \sup_{n\in\mathbb{N}} \Phi^{n+1}(0) \\ &= \sup_{n\in\mathbb{N}} \Phi^{n}(0) && \left(\text{by } \Phi^0(0) = 0 \text{ being the least element in } \mathbb{E}\right) \\ &= \mathsf{lfp}\,\Phi \\ &= \mathsf{wp}\,[\![\texttt{while}(\varphi)\{C\}]\!]\,(f) && \boxed{\text{Q.E.D.}} \end{aligned}$$

EXAMPLE 5.10 (Bounds from ω–rules):
Recall Example 2.6, Example 2.9, Example 2.11 B., and Example 4.10. In all of those examples we performed a fixed point iteration. The „patterns“ — as we called them — which we learned by inspecting the evolution of the first few iterations were in fact ω–invariants.

Proving the pattern correct would correspond to the induction on n in the ω–rule. Finding the limit of a pattern would correspond to finding a closed form for a sup or an inf, accordingly.

Let us briefly reflect on the usability of ω–rules. Recall that verification of loops by means of the induction and the coinduction rule (Theorem 5.4 and Theorem 5.6) was conceptually very simple. Informally, the steps we had to take are the following:

1. Find an appropriate invariant I.
2. Push I through the characteristic function of the loop once.
3. Check whether Step 2. took us down (for induction) or up (for coinduction) in the partial order $\preceq$.

Often, the „only“ difficulty that we encounter in practice is with Step 1: Finding an appropriate invariant (even though this can admittedly be *very* difficult in practice).

Verification of loops using ω–rules (Theorem 5.9) on the other hand is much more involved. In summary, the steps we have to take are as follows:

1. Find an appropriate ω–invariant, i.e. a *sequence* $(I_n)_{n\in\mathbb{N}}$.
2. Check that $(I_n)_{n\in\mathbb{N}}$ is indeed an ω–invariant, e.g. by *induction on n*:
   a) Push I_n through the characteristic function.
   b) Check whether performing Step a) took us above I_{n+1} (for wp) or below I_{n+1} (for wlp) in the partial order $\preceq$.
3. *Find the supremum* (for wp) or the *infimum* (for wlp) of $(I_n)_{n\in\mathbb{N}}$.

Steps 2.a) and 2.b) for the ω–rules basically correspond to Steps 2. and 3. for (co)induction. However, for ω–rules we have to perform an additional induction on the natural numbers.

The second — and probably more significant — extra effort we have to take is reasoning about the limits of the ω–invariants. For wp, for instance, one might very well argue that we may then just as well directly infer the supremum sequence $\Phi^n(0)$ in order to obtain the exact expected value. As a matter of fact, in my personal experience, we have never encountered a case where we found a wp–ω–subinvariant I_n that *truly underapproximated* $\Phi^n(0)$. Instead, we were always able to prove $I_n = \Phi^n(0)$. The difficulty with finding the supremum of the sequence, however, remains. Personally, I therefore believe that both the usability as well as the gain of ω–rules is very limited in practice.

Despite the extra difficulties that come with using ω–rules, a natural question that arises is whether an ω–rule for upper bounds on weakest preexpectations, and dually an ω–rule for lower bounds on weakest liberal preexpectations, could be of any advantage. Luckily, the following remark gives a negative answer to this question.

Remark 5.11 (Expendability of ω–rules for upper bounds on wp*).* Let us formulate the ω–rule for wp–reasoning: Let Φ be the wp–characteristic function of $\texttt{while}(\varphi)\{C\}$ with respect to postexpectation f and let $(I_n)_{n\in\mathbb{N}} \subset \mathbb{E}$ be a monotonically decreasing sequence. Then

$$\Phi(I_n) \preceq I_{n+1} \qquad \text{implies} \qquad \mathsf{wp}\,[\![\texttt{while}(\varphi)\{C\}]\!]\,(f) \preceq \inf_{n\in\mathbb{N}} I_n\,.$$

The soundness proof for this rule goes as follows:

$$\begin{aligned}
& \forall\, n \in \mathbb{N}\colon \quad \Phi(I_n) \preceq I_{n+1} \\
\text{implies} \quad & \inf_{n\in\mathbb{N}} \Phi(I_n) \preceq \inf_{n\in\mathbb{N}} I_{n+1} \\
\text{implies} \quad & \inf_{n\in\mathbb{N}} \Phi(I_n) \preceq \inf_{n\in\mathbb{N}} I_n \\
\text{implies} \quad & \Phi\Big(\inf_{n\in\mathbb{N}} I_n\Big) \preceq \inf_{n\in\mathbb{N}} I_n \qquad \text{(by continuity, Theorem 4.12)}
\end{aligned}$$

$$\text{implies} \qquad \mathsf{wp}\,[\![\texttt{while}(\varphi)\{C\}]\!]\,(f) \;\preceq\; \inf_{n\in\mathbb{N}} I_n$$

(by induction rule, Theorem 5.4)

As a byproduct of our proof, we have shown that $\inf_{n\in\mathbb{N}} I_n$ itself is a wp–superinvariant. Since, ultimately, we have to find the infimum $\check{I} = \inf_{n\in\mathbb{N}} I_n$ anyway in order to gain some insights from the ω–rule, we could have just as well applied the induction rule immediately to $\check{I}$ and could therefore have dispensed with the extra induction on n imposed by the ω–rule.

Dually to the above, an ω–rule for lower bounds on weakest liberal preexpectations is expendable as well. △

5.2.5 *Lower Bounds on* wp

There is a genuine and legitimate interest in reasoning about lower bounds on weakest preexpectations, namely when it comes to giving total correctness guarantees which amounts to *lower–bounding* the probability of total correctness. Yet, we saw that applying ω–rules is quite involved. McIver & Morgan came up with interesting total correctness rules that mitigate this unpleasant situation to the extent that their rules do not rely on ω–invariants. One of the most important rules on which a larger part of their oeuvre on proof rules for probabilistic loops builds upon reads as follows:

Theorem 5.12 ([MM05][8]):
Let $f \in \mathbb{E}_{\leq \exists b}$ be a ***bounded*** *postexpectation. Furthermore, let $I' \in \mathbb{E}_{\leq \exists b}$ be a bounded expectation such that expectation $I \in \mathbb{E}$ given by*

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

is a wp*–subinvariant of* $\texttt{while}(\varphi)\{C\}$ *with respect to f. Finally, let*

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

be the termination probability of $\texttt{while}(\varphi)\{C\}$*. Then:*

A. *If $I = [G]$ for some predicate G, then*

$$T\cdot I \;\preceq\; \mathsf{wp}\,[\![\texttt{while}(\varphi)\{C\}]\!]\,(f)\;.$$

B. *If $[G] \preceq T$ for some predicate G, then*

$$[G]\cdot I \;\preceq\; \mathsf{wp}\,[\![\texttt{while}(\varphi)\{C\}]\!]\,(f)\;.$$

C. *If $\epsilon\cdot I \preceq T$ for some $\epsilon > 0$, then*

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

8 More specifically, this theorem combines Lemma 2.4.1 on p. 43, its relaxation described on p. 54, Lemma 7.7.6 on p. 203, Theorem 7.3.3 on p. 188, and Theorem B.2.2 on p. 329 in [MM05].

Intuitively, Theorem 5.12 provides lower bounds on $\mathsf{wp}\,[\![\texttt{while}(\varphi)\{C\}]\!]\,(f)$ in the following scenarios:

1. If the invariant I is the indicator function of a predicate G, then I multiplied by the termination probability T is a lower bound.
2. If the termination probability T is lower–bounded by the indicator function of some predicate G, then the invariant I multiplied by that indicator function $[G]$ is a lower bound.
3. If the termination probability T is lower–bounded by some non–zero constant fraction ϵ of the invariant I, then the invariant I itself is a lower bound.

While at first glance Theorem 5.12 seems easier to apply than ω–rules, it has several drawbacks of its own: For one, it is only applicable to *bounded* expectations which renders reasoning about general expected values (as opposed to reasoning e.g. about probabilities) difficult, if not impossible.

Another major drawback of Theorem 5.12 is that it requires substantial knowledge about the termination probability $\mathsf{wp}\,[\![\texttt{while}(\varphi)\{C\}]\!]\,(1)$. Reasoning about this probability is quite involved too, although we will later present proof rules (some more, some less involved) that can render reasoning about probabilistic termination feasible (see Chapter 6).

Despite the just mentioned difficulties of applying Theorem 5.12 in practice, expecially Theorem 5.12 c. is an important theoretical device for proving the correctness of several other proof rules. In particular, several of the termination rules in Chapter 6 ultimately build upon Theorem 5.12 c.

If by some means we already known that $\texttt{while}(\varphi)\{C\}$ terminates universally almost–surely, then for one–bounded expectations $f \in \mathbb{E}_{\leq 1}$ we know by Corollary 4.28 that $\mathsf{wp}\,[\![\texttt{while}(\varphi)\{C\}]\!]\,(f)$ and $\mathsf{wlp}\,[\![\texttt{while}(\varphi)\{C\}]\!]\,(f)$ coincide. Thus, in that case there exists only one fixed point and we hence obtain the following corollary:

COROLLARY 5.13 (Bounds on Almost–surely Terminating Loops): *Let the loop* $\texttt{while}(\varphi)\{C\}$ *terminate universally almost–surely, i.e.*

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

and let $I \in \mathbb{E}_{\leq 1}$. *Then:*

A. *If* I *is a* wp*–subinvariant of* $\texttt{while}(\varphi)\{C\}$ *with respect to postexpectation* f, *then*

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

B. *If* I *is a* wlp*–superinvariant of* $\texttt{while}(\varphi)\{C\}$ *with respect to postexpectation* f, *then*

$$\mathsf{wlp}\,[\![\texttt{while}(\varphi)\{C\}]\!]\,(f) \;\preceq\; I\,.$$

Another rule by McIver & Morgan allows — interestingly — for reasoning about weakest preexpectations by means of wlp–subinvariants:

Theorem 5.14 ([MM05, Lemma 7.3.1 on p. 186])**:**
*Let $I' \in \mathbb{E}_{\leq 1}$ be a **one–bounded** expectation such that $I \in \mathbb{E}_{\leq 1}$ given by*

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

is a wlp*–subinvariant of* `while(`φ`){`C`}` *with respect to postexpectation f. Furthermore, let*

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

and let $g \ominus h$ be defined as $\max\{g-h,\,0\}$, for any $g,h \in \mathbb{E}$. Then

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

While this rule is methodologically interesting since it derives a total correctness property (a weakest preexpectation) from a partial correctness invariant (a wlp–invariant), it still has the potentially severe drawback that we need substantial knowledge about the termination probability of the loop at hand.

5.2.6 *Upper Bounds vs. Lower Bounds*

Generally speaking (and perhaps slightly over–simplified), we saw that reasoning about upper bounds of least fixed point (and dually reasoning about lower bounds of greatest fixed points) is easy, whereas reasoning about lower bounds of least fixed points (and dually reasoning about upper bounds of greatest fixed points) is more involved.

We will learn later in Part III that from a computational hardness perspective, the exact *opposite* to what we just stated should be expected. This constitutes a seemingly paradoxical situation to which to the best of our knowledge no *good* explanation is known.

An *unsatisfactory* explanation why lower bounds for weakest preexpectations are in fact computationally tractable is the following: Suppose we want to reason about a lower bound for $\mathsf{wp}\,[\![\texttt{while}(\varphi)\{C\}]\!]\,(f)$ and Φ is the associated characteristic function. Then $(\Phi^n(0))_{n\in\mathbb{N}}$ is trivially an ω–invariant. But then for some fixed $k \geq 2$, the sequence

$$\left(0, \Phi(0), \Phi^2(0), \ldots, \Phi^{k-1}(0), \Phi^k(0), \Phi^k(0), \Phi^k(0), \ldots\right)_{n\in\mathbb{N}}\;,$$

i.e. the so to speak *forced stabilization* of $(\Phi^n(0))_{n\in\mathbb{N}}$ after k iterations, is also an ω–invariant with an easy–to–find (i.e. computable) limit: $\Phi^k(0)$.

This method is of course unsatisfactory, since we had to perform k iterations, i.e. applications of Φ, in order to obtain *some* lower bound. In fact, the

tighter a bound we want to obtain, the more effort we have to invest. *This is not the case for induction or coinduction.* So while the sequence $(\Phi^n(0))_{n\in\mathbb{N}}$ successively indeed enumerates all lower bounds, a major problem in probabilistic program verification remains open:

> **OPEN PROBLEM 1 (One–shot Verification of Lower Bounds on wp):** *Find a „one–shot" method as elegant as the induction or coinduction rule (*Theorems 5.4 *and* 5.6*), which, given a loop* $\texttt{while}(\varphi)\{C\}$*, a post-expectation* $f \in \mathbb{E}$*, and a* specific *hypothesis* $L \in \mathbb{E}$*, allows for checking whether* L *is in fact a lower bound on* $\mathsf{wp}\,[\![\texttt{while}(\varphi)\{C\}]\!]\,(f)$.

In Section 6.2, we will present a rule that can be regarded as a partial solution to the above problem, namely for the special case of almost–sure termination, which amounts to proving that 1 is a (non–strict) lower bound on the termination probability. However, for lower bounds on arbitrary preexpectations, to the best of our knowledge, no sufficiently elegant method is known.

5.2.7 *Bound Refinement*

We saw that obtaining a bound on a weakest (liberal) preexpectation of a loop can be quite difficult. However, once we have obtained some bound — be it upper or lower — by any means (e.g. by application of one of the proof rules presented in the previous sections), we have a chance of refining and thereby tightening this bound fairly easily:

> **THEOREM 5.15 (Bound Refinement):** *Let* Φ *be the* wp*–characteristic function of* $\texttt{while}(\varphi)\{C\}$ *with respect to* f *and let* I *be an upper bound on* $\mathsf{wp}\,[\![\texttt{while}(\varphi)\{C\}]\!]\,(f)$*, such that* $\Phi(I) \preceq I$.
>
> *Then* $\Phi(I)$ *is also an upper bound on* $\mathsf{wp}\,[\![\texttt{while}(\varphi)\{C\}]\!]\,(f)$*. Moreover, whenever* $\Phi(I) \neq I$*, then* $\Phi(I)$ *is an even tighter upper bound on* $\mathsf{wp}\,[\![\texttt{while}(\varphi)\{C\}]\!]\,(f)$ *than* I.
>
> *Dually, if* I *is a lower bound, such that* $I \preceq \Phi(I)$*, then* $\Phi(I)$ *is also a lower bound; and whenever* $\Phi(I) \neq I$*, then* $\Phi(I)$ *is an even tighter lower bound than* I.
>
> *Analogous results hold for* awp, wlp, *and* awlp *as well.*

Proof. Let I be an upper bound on $\mathsf{wp}\,[\![\texttt{while}(\varphi)\{C\}]\!]\,(f)$. To see that $\Phi(I)$ is also an upper bound on $\mathsf{wp}\,[\![\texttt{while}(\varphi)\{C\}]\!]\,(f)$, consider the following:

$$
\begin{aligned}
& \mathsf{wp}\,[\![\texttt{while}(\varphi)\{C\}]\!]\,(f) \;\preceq\; I \\
\text{iff}\quad & \mathsf{lfp}\;\Phi \;\preceq\; I \\
\text{implies}\quad & \Phi(\mathsf{lfp}\;\Phi) \;\preceq\; \Phi(I) \qquad \text{(by monotonicity, Theorem 4.16)}
\end{aligned}
$$

$$\begin{aligned} &\text{implies} && \mathsf{lfp}\ \Phi \preceq \Phi(I) && (\mathsf{lfp}\ \Phi \text{ is a fixed point of } \Phi)\\ &\text{iff} && \mathsf{wp}\,[\![\texttt{while}(\varphi)\{C\}]\!]\,(f) \preceq \Phi(I) \end{aligned}$$

By the assumption $\Phi(I) \preceq I$, $\Phi(I)$ is at least as tight an upper bound as I. Thus if $\Phi(I) \neq I$, $\Phi(I)$ must be an even tighter upper bound.

The reasoning for awp, wlp, awlp, and lower bounds is analogous. Q.E.D.

The particular bound refinement of Theorem 5.15 can of course be continued ad infinitum: For instance, if I is an upper bound on $\mathsf{wp}\,[\![\texttt{while}(\varphi)\{C\}]\!]\,(f)$ with $\Phi(I) \preceq I$, then so is $\Phi(I)$ but also $\Phi^2(I)$, $\Phi^3(I)$, and so on. In fact, for increasing n, the sequence $\Phi^n(I)$ is decreasing and converges to a fixed point, more precisely the *greatest fixed point that is below (or equal to) I*. This is called the Tarski–Kantorovich principle [JGP00]. The so–obtained fixed point itself is then also an upper bound, thus

$$\mathsf{wp}\,[\![\texttt{while}(\varphi)\{C\}]\!]\,(f) \preceq \inf_{n\in\mathbb{N}} \Phi^n(I)\,.$$

Dually, if I is a lower bound on $\mathsf{wp}\,[\![\texttt{while}(\varphi)\{C\}]\!]\,(f)$ with $I \preceq \Phi(I)$, then so are $\Phi(I)$, $\Phi^2(I)$, $\Phi^3(I)$, and so on, and moreover

$$\sup_{n\in\mathbb{N}} \Phi^n(I) \preceq \mathsf{wp}\,[\![\texttt{while}(\varphi)\{C\}]\!]\,(f)\,.$$

5.2.8 *Independent and Identically Distributed Loops*

We have learned in the previous sections that obtaining bounds — especially lower bounds —, on weakest preexpectations of while loops can be a very difficult task. Obtaining exact weakest preexpectations obviously cannot be any easier in principle. Under certain conditions, however, we are able to derive the *exact* weakest preexpectation of a while loop with respect to a given postexpectation. Informally, these conditions can be described as follows:

1. For each loop iteration, the probability to immediately terminate after that iteration is equal.

2. There is *no information* flow across different loop iterations with respect to any program variable that has an influence on the value of the postexpectation f.

In the following, we will make the above two conditions more formal. A central notion for achieving this formalization is the concept of a loop being f–independent identically distributed (f–i.i.d. for short):

DEFINITION 5.16 (f–i.i.d. Loops [Bat+18b]):
Let $f \in \mathbb{E}$ and $C \in \mathsf{pGCL}$.

A. *The set of variables occurring in f, denoted $\mathsf{Vars}(f)$, is defined as*

$$\mathsf{Vars}(f) \;=\; \{x \in \mathsf{Vars} \mid \exists v, v' \in \mathsf{Vals}\colon\; f[x/v] \;\neq\; f[x/v']\}\,.$$

B. *The set of variables modified by C, denoted $\mathsf{Mod}(C)$, is defined as the set of all variables $x \in \mathsf{Vars}$, such that x appears on the left–hand–side of an assignment occurring in C.*

C. *We say that C cannot influence f, denoted $C \not\Rightarrow f$, if the set of variables occurring in f is disjoint from the set of variables modified by C, i.e.*

$$C \not\Rightarrow f \qquad \text{iff} \qquad \mathsf{Mod}(C) \cap \mathsf{Vars}(f) \;=\; \emptyset\,.$$

D. *A loop $\texttt{while}(\varphi)\{C\}$ is called f–independent identically distributed (f–i.i.d. for short), iff*

$$C \not\Rightarrow \mathsf{wp}\,[\![C]\!]\,([\varphi]) \qquad \text{and} \qquad C \not\Rightarrow \mathsf{wp}\,[\![C]\!]\,([\neg\varphi]\cdot f)\,.$$

Notice that $\mathsf{Mod}(\ldots)$ is a *purely syntactic* notion. On the other hand, the definition of $\mathsf{Vars}(\ldots)$ has more of a *semantic flavor* as it speaks about a property of a potentially arbitrary function of type $\Sigma \to \mathbb{R}^{\infty}_{\geq 0}$. However, if we are given a closed form syntactic expression for the expectation f, we can at least overapproximate $\mathsf{Vars} f$ by the set of all variables that actually occurr in f, syntactically. Nevertheless, because of the semantic flavor of $\mathsf{Vars}(\ldots)$, the relation $\not\Rightarrow$ and the notion of f–i.i.d.–ness is not purely syntactic

The definition of f–i.i.d.–ness is very technical and providing an intuition for it is not an easy task. A more pleasant aspect about the definition is that in practice it can often be checked in a quite straightforward and even *automatable* manner, despite not being a purely syntactic notion [Bat+18b]. The most important aspect, however, is that for f–independent identically distributed loops we can obtain *exact* weakest preexpectations:

THEOREM 5.17 (Weakest Preexpectations of f–i.i.d. Loops [Bat+18b]):
Let $\texttt{while}(\varphi)\{C\}$ be f–i.i.d. Then the weakest preexpectation of the loop with respect to f is given by

$$\mathsf{wp}\,[\![\texttt{while}(\varphi)\{C\}]\!]\,(f) \;=\; [\neg\varphi]\cdot f \;+\; [\varphi]\cdot \frac{\mathsf{wp}\,[\![C]\!]\,([\neg\varphi]\cdot f)}{1 - \mathsf{wp}\,[\![C]\!]\,([\varphi])}\,,$$

where we define $\%/0 = 0$.

Intuitively, as the expected value of f can be determined by just a single iteration of the loop body, the fraction appearing in Theorem 5.17 can be understood as the *conditional expected value* of f given that the loop terminates.

It is worthwhile to note that in order to apply Theorem 5.17 it is *not required* to find or guess in any way an invariant, ω–invariant, martingale, or alike. Instead, only f–i.i.d.–ness of f — the very postexpectation one is interested in — needs to be checked. Our theorem then immediately yields the *exact* sought–after preexpectation — not just a bound.

Finally, we would like to mention that Theorem 5.17 is obviously not a free–lunch–theorem: Checking f–i.i.d.–ness can potentially become a non–trivial and in general undecidable task. Also, once the expected value of postexpectation f depends in some way on the number of iterations a loop makes, i.e. once the loop performs some sort of *counting* and the value of the counter influences the value of f, the theorem fails to be applicable altogether. On the other hand, Theorem 5.17 has been successfully applied to reason about massively large Bayesian networks from the *Bayesian Network Repository* [Scu] with more than a thousand nodes [Bat+18b].