15-414: Bug Catching: Automated Program Verification

Lecture Notes on Loop Variants and Convergence

Matt Fredrikson

Carnegie Mellon University
Lecture 10

1 Introduction

The move to total correctness by investigating diamond modalities worked quite well in the previous lecture, except that our understanding of loops is still lagging behind. Unwinding of loops is all we were able to do so far:

$$(\langle\text{unwind}\rangle)\quad \langle \texttt{while}(Q)\,\alpha\rangle P \leftrightarrow \langle \texttt{if}(Q)\,\{\alpha;\texttt{while}(Q)\,\alpha\}\rangle P$$

Since not all loops have a fixed finite number of rounds, this axiom isn't quite sufficient. But that's similar to the case of box modalities, where we also first understood the elementary axioms reducing programs and later went for a study of loop invariants for while loops with unbounded repetitions. Our key to understanding what to do with $[\texttt{while}(Q)\,\alpha]P$ formulas is to first understand induction principles for $[\alpha^*]P$ with more general nondeterministic repetitions α^* of program α, under complete ignorance of the loop guard. We will proceed in similar ways again for diamond properties of while loops.

2 Recap: Nondeterministic Repetitions

Recall the nondeterministic repetition α^* which expresses that the program α repeats any arbitrary unspecified nondeterministic number of times:

6. $[\![\alpha^*]\!] = \{(\omega,\nu) : \text{ there are an } n \text{ and states } \mu_0 = \omega, \mu_1, \mu_2, \ldots, \mu_n = \nu \text{ such that } (\mu_i,\mu_{i+1}) \in [\![\alpha]\!] \text{ for all } 0 \leq i < n\}$
   That is, state μ_{i+1} is reachable from state μ_i by running α for all i.

Recall its core induction principle for $[\alpha^*]P$.

Lemma 1. *The induction axiom I is sound:*

$$(I)\ [\alpha^*]P \leftrightarrow P \wedge [\alpha^*](P \rightarrow [\alpha]P)$$

The loop invariant rule for nondeterministic repetitions derives from this axiom:

$$\text{(loop)}\ \frac{\Gamma \vdash J, \Delta \quad J \vdash [\alpha]J \quad J \vdash P}{\Gamma \vdash [\alpha^*]P, \Delta}$$

3 Diamonds for Nondeterministic Repetitions

The induction axiom I led to a study of loop invariants, which can prove box properties of loops using loop invariants. As the name suggests, loop *invariants* are about properties that do *not* change as the loop runs. But if nothing ever changes, then how would that argue that the loop also makes progress toward eventually terminating? Of course, it wouldn't.

Lemma 2. *The convergence axiom is sound for programs with integer arithmetic:*

$$(C)\ \begin{array}{l}[\alpha^*]\forall n{>}0\,(\varphi(n) \rightarrow \langle\alpha\rangle\varphi(n-1)) \\ \rightarrow \big((\exists n.n{\geq}0 \wedge \varphi(n)) \rightarrow \langle\alpha^*\rangle\varphi(0)\big)\end{array} \quad (n \notin \alpha)$$

The proof of the soundness of the convergence axiom C is based on the observation that the value of n for which $\varphi(n)$ is true will eventually decrease down to 0 after repeating α^* sufficiently often if it initially starts from a nonnegative $n \geq 0$, provided that after any number of repetitions of α^* and for any positive $n > 0$ for which $\varphi(n)$ holds it is the case that there is a way of running one round of α to make $\varphi(n-1)$ true. We refer to the literature for detail [HKT00, Pla12, Pla17].

A program that does not terminate is also sometimes referred to as a diverging program.

Lemma 3. *The loop convergence proof rule con derives from axiom C:*

$$(con)\ \frac{\Gamma \vdash \exists n{\geq}0\,\varphi(n), \Delta \quad \varphi(n), n{>}0 \vdash \langle\alpha\rangle\varphi(n-1) \quad \varphi(0) \vdash P}{\Gamma \vdash \langle\alpha^*\rangle P, \Delta}\ (n \textit{ fresh})$$

Proof. From the loop convergence axiom C, we derive

$$\dfrac{\dfrac{\Gamma \vdash \exists n{\geq}0\,\varphi(n), \Delta \qquad \dfrac{\dfrac{\varphi(n), n{>}0 \vdash \langle\alpha\rangle\varphi(n-1)}{\vdash \forall n{>}0\,(\varphi(n) \rightarrow \langle\alpha\rangle\varphi(n-1))}\,{\scriptstyle \forall R,\rightarrow R}}{\Gamma \vdash [\alpha^*]\forall n{>}0\,(\varphi(n) \rightarrow \langle\alpha\rangle\varphi(n-1)), \Delta}\,{\scriptstyle G}}{\Gamma \vdash \exists n{\geq}0\,\varphi(n) \wedge [\alpha^*]\forall n{>}0\,(\varphi(n) \rightarrow \langle\alpha\rangle\varphi(n-1)), \Delta}\,{\scriptstyle \wedge R}}{\Gamma \vdash \langle\alpha^*\rangle\varphi(0), \Delta}\,{\scriptstyle C} \qquad \varphi(0) \vdash P}{\Gamma \vdash \langle\alpha^*\rangle P, \Delta}\,{\scriptstyle M}$$

□

In order to get to know this proof rule better, let's do a few example proofs.

$$\text{con}\,\frac{\text{$\to$R}\,\dfrac{\mathbb{Z}\dfrac{*}{x\geq 0 \vdash \exists n{\geq}0\, x=n}\langle{:=}\rangle\dfrac{\mathbb{Z}\dfrac{*}{x=n, n>0 \vdash x-1=n-1}\quad \mathbb{Z}\dfrac{*}{x=0\vdash x=0}}{x=n, n{>}0 \vdash \langle x:=x-1\rangle x=n-1}}{x\geq 0 \vdash \langle (x:=x-1)^*\rangle x=0}}{\vdash x\geq 0 \to \langle (x:=x-1)^*\rangle x=0}$$

If the loop body decrements x by 2, of course, we cannot know that the value of x will eventually be 0 but merely that it will be between 0 (inclusive) and 2 (exclusive). The loop variant $\varphi(n) \overset{\text{def}}{\equiv} 2n \leq x < 2n+2$ relates the program variable x to the loop progress variable n appropriately.

$$\text{con}\,\frac{\text{$\to$R}\,\dfrac{\mathbb{Z}\dfrac{*}{x\geq 0 \vdash \exists n{\geq}0\, 2n{\leq}x{<}2n{+}2}\langle{:=}\rangle\dfrac{\mathbb{Z}\dfrac{*}{2n{\leq}x{<}2n{+}2, n>0 \vdash 2n{-}2{\leq}x{-}2{<}2n}\quad \mathbb{Z}\dfrac{*}{0{\leq}x{<}2\vdash 0{\leq}x{<}2}}{2n{\leq}x{<}2n{+}2, n{>}0 \vdash \langle x:=x-2\rangle 2n{-}2{\leq}x{<}2n}}{x\geq 0 \vdash \langle (x:=x-2)^*\rangle 0\leq x<2}}{\vdash x\geq 0 \to \langle (x:=x-2)^*\rangle 0\leq x<2}$$

Suppose the loop body still decrements by 2 but we also know that the value of x starts out even (written $2|x$) then we can prove that x is eventually 0 by a minor modification of the above proof, using evenness as an additional conjunct in the loop variant $\varphi(n) \equiv 2|x \wedge 2n \leq x < 2n+2$:

$$\text{con}\,\frac{\text{$\to$R,$\wedge$L}\,\dfrac{\mathbb{Z}\dfrac{*}{x\geq 0, 2|x \vdash \exists n{\geq}0\,(2|x{\wedge}2n{\leq}x{<}2n{+}2)}\langle{:=}\rangle\dfrac{\mathbb{Z}\dfrac{*}{2|x{\wedge}2n{\leq}x{<}2n{+}2, n{>}0 \vdash 2|x{-}2\wedge 2n{-}2{\leq}x{-}2{<}2n}\quad \mathbb{Z}\dfrac{*}{2|x{\wedge}0{\leq}x{<}2\vdash x{=}0}}{2|x{\wedge}2n{\leq}x{<}2n{+}2, n{>}0 \vdash \langle x:=x-2\rangle(2|x{\wedge}2n{-}2{\leq}x{<}2n)}}{x\geq 0, 2|x \vdash \langle (x:=x-2)^*\rangle x=0}}{\vdash x\geq 0\wedge 2|x \to \langle (x:=x-2)^*\rangle x=0}$$

Note that the loop variant $\varphi(n) \equiv 2|x \wedge 2n \leq x < 2n+2$ has a part that does not actually depend on the progress counter n. That's peculiar. What does it mean?

Some loop variants such as $\varphi(n) \equiv q \wedge p(n)$ that consist of some conjuncts q that are independent of the loop progress counter n together with other conjuncts $p(n)$ that do depend on n. In that case, the n-independent part q plays a similar role as a loop invariant ass something that does not change, while only the the n-dependent part $p(n)$ is a proper progress condition that does change toward the eventual goal.

In the above example, it, indeed, was an invariant of the loop that x always remains even. The proper progress condition expressed that x is between $2n$ and $2n+2$ as a function of n, so making progress toward $0 \leq x < 2$ as n decreases.

4 Variants of Mixed Invariants and Variants

Using loop variants $\varphi(n)$ with parts that depend on n (progress condition) and parts that do not (invariants) is one approach. And a perfectly reasonable and well-defined

one, too. A fair number of program verification tools, however, instead expect separate declarations of loop invariants and loop variants. What could that possibly mean? How is it reasonable to worry separately about loop invariants and loop variants?

It does make some intuitive sense to worry separately first about partial correctness (if a program terminates then its result will have the correct outcome) and second about termination (the program indeed terminates) to finally show total correctness (the program always terminates and gives the correct answer, too). But how can such informal arguments be made rigorous, in order to make sure there's no flaw in our reasoning?

A partial correctness property of a loop shows that if formula A holds in the initial state then formula B always holds after running the loop α^*:

$$A \to [\alpha^*]B$$

A total correctness property of a loop is of the form:

$$C \to \langle\alpha^*\rangle D$$

How can we meaningfully combine two properties of total and partial correctness leading to mixed box and diamond modalities? Never minding the fact that we generally might need some preconditions A or C, respectively, to make the above partial or total correctness true, let's assume we have some way of justifying that a box property $[\alpha^*]B$ as well as a diamond property $\langle\alpha^*\rangle D$ are true in some state.

If $[\alpha^*]B$ and $\langle\alpha^*\rangle D$ are both true, then what do we know?

If B holds after all runs of α^* and D holds after at least one run of α^*, then the conjunction $B \wedge D$ also holds after at least one run of α^*. Consequently, a variant and an invariant, when established separately, should still hold jointly. We should make that rigorous! But what if an invariant, established separately, is needed during the proof of the variant? How is that a proof? We should make that rigorous, too!

So let's go one step at a time.

If we know that $\langle\alpha^*\rangle B$ and $\langle\alpha^*\rangle D$ then we don't know a whole lot because the first formula says there is a run of α^* to a state where B is true while the second formula says that there also is a run of α^* to a state where D is true. But both B and D could be true after a different number of iterations, so that $B \wedge D$ might never be true. Yet if we know $[\alpha^*]B$ and $\langle\alpha^*\rangle D$, then we know that $B \wedge D$ are true after some number of repetitions, because B is true after any number of iterations while D is true after some appropriate number of iterations, at which point B will also be true and hence their conjunction.

Lemma 4. *Kripke's modal modus ponens axioms are sound:*

$$\textit{(K)}\ \ [\alpha](P \to Q) \to ([\alpha]P \to [\alpha]Q)$$

$$\textit{(K}_{\langle\cdot\rangle}\textit{)}\ \ [\alpha](P \to Q) \to (\langle\alpha\rangle P \to \langle\alpha\rangle Q)$$

Lemma 5. *The invariant to variant conversion is a derived axiom:*

$$\textit{(inv2var)}\ \ [\alpha]J \to (\langle\alpha\rangle(J \to \varphi) \to \langle\alpha\rangle\varphi)$$

Proof. The inv2var axiom proves using axiom $\mathrm{K}_{\langle\cdot\rangle}$ and monotonicity rule M[·]:

$$\dfrac{\dfrac{\dfrac{*}{J \vdash (J \to \varphi) \to \varphi}}{[\alpha]J \vdash [\alpha]\big((J \to \varphi) \to \varphi\big)}\,\mathrm{M}[\cdot]}{[\alpha]J \vdash \langle\alpha\rangle(J \to \varphi) \to \langle\alpha\rangle\varphi}\,\mathrm{K}_{\langle\cdot\rangle}}{\vdash [\alpha]J \to (\langle\alpha\rangle(J \to \varphi) \to \langle\alpha\rangle\varphi)}\,{\to}\mathrm{R}$$

□

The inv2var axiom enables us to assume a proved invariant property during a diamond proof. A common special case of this is when we establish an invariant property and a variant property separately and just want to put them together, which is what the minor variation in derived axiom inv∧var supports.

Lemma 6. *The invariant plus variant conversion is a derived axiom:*

$$\textit{(inv∧var)}\quad [\alpha]P \wedge \langle\alpha\rangle Q \to \langle\alpha\rangle(P \wedge Q)$$

Proof.

$$\dfrac{\dfrac{\dfrac{\dfrac{*}{Q \vdash P \to P \wedge Q}\,{\to}\mathrm{R},{\wedge}\mathrm{R},\mathrm{id}}{\langle\alpha\rangle Q \vdash \langle\alpha\rangle(P \to P \wedge Q)}\,\mathrm{M}}{[\alpha]P, \langle\alpha\rangle Q \vdash \langle\alpha\rangle(P \wedge Q)}\,\mathrm{inv2var}}{\vdash [\alpha]P \wedge \langle\alpha\rangle Q \to \langle\alpha\rangle(P \wedge Q)}\,{\to}\mathrm{R},{\wedge}\mathrm{L}$$

□

This proof uses the diamond formulation of the monotonicity rule, the dual to M[·]:

$$\text{(M)}\ \dfrac{P \vdash Q}{\Gamma, \langle\alpha\rangle P \vdash \langle\alpha\rangle Q, \Delta}$$

5 Total Correctness of While Loops

For nondeterministic repetitions α^*, the proof rule con based on the axiom C predicts the exact number of loop iterations by way of the variable n. This is unnecessarily precise for while loops ,$\texttt{while}(Q)\,\alpha$ where the loop itself already conveys when it stops, namely exactly when the loop guard Q turns false.

For while loops it is, thus, often more convenient to work with a more lenient proof rule that just has a term φ whose value decreases along the repetitions of the loop and stays nonnegative while the loop repeats. This proof rule, var, can be derived from the convergence rule con.

Lemma 7. *The variant proof rule for while loops is a derived rule:*

$$\textit{(var)}\ \dfrac{\Gamma \vdash J, \Delta \quad J, Q, \varphi = n \vdash \langle\alpha\rangle(J \wedge \varphi < n) \quad J, Q \vdash \varphi \geq 0 \quad J, \neg Q \vdash P}{\Gamma \vdash \langle\texttt{while}(Q)\,\alpha\rangle P, \Delta}\ (n \textit{ fresh})$$

Proof. In order to relax the need for an exact loop repetition count in con, this proof uses the following equivalent definition of while loops: $\texttt{while}(Q)\,\alpha \equiv \{\texttt{if}(Q)\,\alpha\}^*;?\neg Q$. It also uses a clever loop variant $\varphi(n) \overset{\text{def}}{\equiv} J \wedge (Q \to \varphi < n)$.

$$\text{con}\;\frac{\Gamma \vdash \exists n{\geq}0\,\varphi(n), \Delta \qquad \varphi(n), n > 0 \vdash \langle \texttt{if}(Q)\,\alpha\rangle\varphi(n-1) \quad \varphi(0) \vdash \neg Q \wedge P}{\dfrac{\dfrac{\Gamma \vdash \langle\{\texttt{if}(Q)\,\alpha\}^*\rangle(\neg Q \wedge P), \Delta}{\Gamma \vdash \langle\{\texttt{if}(Q)\,\alpha\}^*;?\neg Q\rangle P, \Delta}\,\langle;\rangle,\langle?\rangle}{\Gamma \vdash \langle\texttt{while}(Q)\,\alpha\rangle P, \Delta}$$

We consider the three remaining premises separately. The first premise proves as follows, where the bottom step uses validity $\exists n\,(J \wedge p(n)) \leftrightarrow J \wedge \exists n\,p(n)$ since $n \notin J$, and where the right premise uses the witness $\varphi + 1$ for n:

$$\dfrac{\dfrac{\dfrac{\Gamma \vdash J, \Delta \qquad \overset{*}{\overset{\mathbb{Z}}{\Gamma \vdash \exists n{\geq}0\,(Q \to \varphi < n), \Delta}}}{\Gamma \vdash J \wedge \exists n{\geq}0\,(Q \to \varphi < n), \Delta}\,\wedge\text{R}}{\Gamma \vdash \exists n{\geq}0\,(J \wedge (Q \to \varphi < n)), \Delta}}{\Gamma \vdash \exists n{\geq}0\,\varphi(n), \Delta}$$

The second premise proves as follows (the second branch of $\to$L for $Q \to \varphi < n$ is elided, marked by $\triangleright$, and proves since Q is among the assumptions, the top step in the first branch is a monotonicity step choosing the implicitly universally quantified variable n to be $\varphi + 1$):

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{J, Q, \varphi = n \vdash \langle\alpha\rangle(J \wedge \varphi < n)}{J, Q, \varphi < n, n > 0 \vdash \langle\alpha\rangle(J \wedge \varphi < n - 1)}\,\text{M}}{J, Q, \varphi < n, n > 0 \vdash \langle\alpha\rangle\varphi(n-1)}\,\text{M} \qquad \triangleright}{J, Q \to \varphi < n, n > 0, Q \vdash \langle\alpha\rangle\varphi(n-1)}\,\to\text{L} \qquad \dfrac{\dfrac{\overset{*}{J \vdash J}\,\text{id}}{\neg Q, Q \vdash \varphi < n - 1}\,\to\text{R}}{\neg Q \vdash Q \to \varphi < n - 1}\,\neg\text{L,id}}{J, Q \to \varphi < n, n > 0, \neg Q \vdash \varphi(n-1)}\,\wedge\text{R,WL}}{J, Q \to \varphi < n, n > 0 \vdash (Q \to \langle\alpha\rangle\varphi(n-1)) \wedge (\neg Q \to \varphi(n-1))}\,\wedge\text{R},\to\text{R}}{\varphi(n), n > 0 \vdash \langle\texttt{if}(Q)\,\alpha\rangle\varphi(n-1)}\,\langle\text{if}\rangle,\wedge\text{L}$$

The third premise proves as follows (again the second branch of $\to$L for $\varphi \to \varphi < 0$ is elided, marked by $\triangleright$ and proves since Q is among the assumptions):

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{J, Q \vdash \varphi \geq 0 \qquad \overset{*}{\overset{\mathbb{Z}}{\varphi < 0, \varphi \geq 0 \vdash}}}{J, \varphi < 0, Q \vdash}\,\text{cut,WL} \qquad \triangleright}{J, Q \to \varphi < 0, Q \vdash}\,\to\text{L,WR}}{J, Q \to \varphi < 0 \vdash \neg Q}\,\neg\text{R}}{\varphi(0) \vdash \neg Q}\,\wedge\text{L} \qquad \dfrac{\dfrac{\overset{*}{\neg Q \vdash \neg Q}\,\text{id}}{\varphi(0), \neg Q \vdash \neg Q \wedge P}\,\wedge\text{R,WL} \qquad \dfrac{J, \neg Q \vdash P}{\varphi(0), \neg Q \vdash P}\,\wedge\text{L,WL}}{\varphi(0) \vdash \neg Q \wedge P}\,\text{cut}$$

□

As a simple example, the following formula easily proves with rule var using $J \equiv true$ and $x - 5$ for φ:

$$\text{var}\,\frac{\top\text{R}\,\frac{*}{\vdash true} \quad \langle:=\rangle\,\frac{\mathbb{Z}\,\frac{*}{x \geq 5, x-5=n \vdash x-2-5<n}}{x \geq 5, x-5=n \vdash \langle x:=x-2\rangle x-5<n} \quad \mathbb{Z}\,\frac{*}{x \geq 5 \vdash x-5 \geq 0} \quad \mathbb{Z}\,\frac{*}{\neg x \geq 5 \vdash x<5}}{\vdash \langle \texttt{while}(x \geq 5)\, x:=x-2\rangle\, x<5}$$

The respective proof rules for proving the trivial succedent $true$ or proving a sequent with the impossible assumption $false$ are as is to be expected:

$$(\top\text{R})\ \frac{}{\Gamma \vdash true, \Delta}$$

$$(\bot\text{L})\ \frac{}{false, \Gamma \vdash \Delta}$$

6 Example

Recall the proof of the square-by-add program from lecture 5

$$x \geq 0 \rightarrow [s := 0; i := 0; \texttt{while}(i < x)\, \{s := s + 2 * i + 1; i := i + 1\}]\, s = x * x \tag{1}$$

When α denotes the loop body $s := s + 2 * i + 1; i := i + 1$ recall that we proved it using the following loop invariant

$$J \overset{\text{def}}{\equiv} i \leq x \wedge s = i * i \tag{2}$$

$$[;],[:=]=\ \frac{\text{loop}\,\frac{x\geq 0, s=0, i=0 \vdash J \qquad J, i<x \vdash [\alpha]J \quad J, \neg i<x \vdash s=x*x}{x \geq 0, s = 0, i = 0 \vdash [\texttt{while}(i < x)\, \alpha]s = x * x}}{x \geq 0 \vdash [s := 0; i := 0; \texttt{while}(i < x)\, \alpha]s = x * x}$$

This establishes partial correctness of the square-by-add program but does not guarantee that it also always terminates. Changing the modality from a box to a diamond will require us to prove it using the variance rule var instead of invariant rule loop. The variance rule var requires both an invariant J, for which we still use (2), and a variant term φ, for which we use $\varphi \overset{\text{def}}{=} x - i$ since that decreases to 0 when running the square-by-add program. This leads to the following proof start:

$$\langle;\rangle,\langle:=\rangle=\ \frac{\text{var}\,\frac{x\geq 0, s=0, i=0 \vdash J \qquad J, i<x, \varphi=n \vdash \langle\alpha\rangle(J \wedge \varphi<n) \quad J, i<x \vdash \varphi \geq 0 \quad J, \neg i<x \vdash s=x*x}{x\geq 0, s=0, i=0 \vdash \langle\texttt{while}(i < x)\, \alpha\rangle s = x * x}}{\vdash x\geq 0 \rightarrow \langle s := 0; i := 0; \texttt{while}(i < x)\, \alpha\rangle s = x * x}$$

This first and fourth premise are the same as for the proof of (1) and, thus, still prove in the same way. The third premise proves by arithmetic since $i < x$ implies $x - i \geq 0$:

$$\frac{\mathbb{Z}\,\frac{*}{i \leq x \wedge s = i * i, i<x \vdash x - i \geq 0}}{J, i<x \vdash \varphi \geq 0}$$

The only remaining premise, the induction step in the second premise could be proved again, or proved in a clever way reusing the fact that we already established partial correctness for the program. In particular, we already have a proof of $J, i{<}x \vdash [\alpha]J$, which derived axiom inv∧var can exploit.

$$\text{inv}\wedge\text{var}\;\frac{\text{WL}\;\frac{\text{above}\;\frac{}{J, i<x \vdash [\alpha]J}\langle;\rangle,\langle:=\rangle}{J, i<x, \varphi=n \vdash [\alpha]J} \quad \wedge\text{R}\;\frac{\mathbb{Z}\;\frac{*\;\frac{}{J, i<x, x-i=n \vdash x-(i+1)<n}}{J, i<x, x-i=n \vdash \langle s:=s+2*i+1; i:=i+1\rangle x-i<n}}{J, i<x, \varphi=n \vdash \langle\alpha\rangle\varphi<n}}{J, i<x, \varphi=n \vdash [\alpha]J \wedge \langle\alpha\rangle\varphi<n}}{J, i<x, \varphi=n \vdash \langle\alpha\rangle(J \wedge \varphi<n)}$$

7 Summary

A split into a partial correctness argument together with a pure termination analysis is especially helpful when most parts of the behavior of the program are irrelevant for its termination. The other reason to reason like this is that partial correctness and total correctness are often considered separately, at which point it is helpful to reuse the results of the partial correctness analysis for the total correctness analysis. Having said that, a direct analysis with just one single proof that directly targets total correctness is more concise. Today's axioms and proof rules are summarized in Fig. 1.

$$\text{(C)}\quad [\alpha^*]\forall n{>}0\,(\varphi(n) \to \langle\alpha\rangle\varphi(n-1)) \to \big((\exists n.n{\geq}0 \wedge \varphi(n)) \to \langle\alpha^*\rangle\varphi(0)\big) \qquad (n \notin \alpha)$$

$$\text{(con)}\quad \frac{\Gamma \vdash \exists n{\geq}0\,\varphi(n), \Delta \quad \varphi(n), n{>}0 \vdash \langle\alpha\rangle\varphi(n-1) \quad \varphi(0) \vdash P}{\Gamma \vdash \langle\alpha^*\rangle P, \Delta} \qquad \text{(n fresh)}$$

$$\text{(var)}\quad \frac{\Gamma \vdash J, \Delta \quad J, Q, \varphi=n \vdash \langle\alpha\rangle(J \wedge \varphi<n) \quad J, Q \vdash \varphi \geq 0 \quad J, \neg Q \vdash P}{\Gamma \vdash \langle\texttt{while}(Q)\,\alpha\rangle P, \Delta} \text{(n fresh)}$$

$$\text{(K)}\quad [\alpha](P \to Q) \to ([\alpha]P \to [\alpha]Q)$$

$$\text{(K}_{\langle\cdot\rangle}\text{)}\quad [\alpha](P \to Q) \to (\langle\alpha\rangle P \to \langle\alpha\rangle Q)$$

$$\text{(inv2var)}\quad [\alpha]J \to (\langle\alpha\rangle(J \to \varphi) \to \langle\alpha\rangle\varphi)$$

$$\text{(inv}\wedge\text{var)}\quad [\alpha]P \wedge \langle\alpha\rangle Q \to \langle\alpha\rangle(P \wedge Q)$$

$$\text{(M)}\quad \frac{P \vdash Q}{\Gamma, \langle\alpha\rangle P \vdash \langle\alpha\rangle Q, \Delta}$$

Figure 1: Proof rules for diamonds of loops and related axioms

References

[HKT00] David Harel, Dexter Kozen, and Jerzy Tiuryn. *Dynamic Logic*. MIT Press, 2000.

[Pla12] André Platzer. The complete proof theory of hybrid systems. In *LICS*, pages 541–550. IEEE, 2012. doi:10.1109/LICS.2012.64.

[Pla17] André Platzer. *Logical Foundations of Cyber-Physical Systems*. Springer, Switzerland, 2017. URL: http://www.springer.com/978-3-319-63587-3.