15-424: Foundations of Cyber-Physical Systems

Lecture Notes on Proofs & Arithmetic

André Platzer

Carnegie Mellon University
Lecture 9

1 Introduction

Lecture 8 on Events & Delays discussed and developed two models for the ping pong ball whose control was a ping pong paddle. First an event-driven controller and then a time-triggered controller. Invariants have been identified in Lecture 8 but not proved. This lecture will study proofs.

This lecture discusses:

- What is a proof?
- How does arithmetic happen in a proof?
- Arithmetic hiding to weaken arithmetic
- Instantiating arithmetic quantifiers to the extreme
- Updates as delayed substitutions/assignments
- Creative cuts for arithmetic
- Substituting equations
- If-then-else proofs

There are many more interesting things to be discussed about the mysteries of arithmetic and how real arithmetic properties themselves can be proved [PQR09, Pla10, Appendix D]. That is a topic for a later lecture, though. This lecture focuses on how arithmetic interfaces with proofs.

2 Proving Events in Control

$$0 \leq h \leq 5 \land v \leq 0 \land 1 \geq c \geq 0 \land g > 0 \land f \geq 0 \rightarrow \\ \big[\big(((h' = v, v' = -g \,\&\, h \geq 0 \land h \leq 5) \cup (h' = v, v' = -g \,\&\, h \geq 5)); \\ \texttt{if}(h = 0)\, v := -cv \,\texttt{else}\, \texttt{if}(4 \leq h \leq 5 \land v \geq 0)\, v := -fv\big)^*\big](0 \leq h \leq 5) \tag{1}$$

Lecture 8 on Events & Delays identified the following invariant for this system:

$$5 \geq h \geq 0 \land (h = 5 \rightarrow v \leq 0)$$

This invariant is just strong enough to remember the control choice at the event $h = 5$ and that the possible range of h is safe. Recall that (global) invariants need to be augmented with the usual assumptions about the unchanged variables, like $c \geq 0 \land g > 0 \land f \geq 0$.

$$\varphi \overset{\text{def}}{\equiv} 0 \leq h \leq 5 \land (h = 5 \rightarrow v \leq 0) \land 1 \geq c \geq 0 \land g > 0 \land f \geq 0$$

Let's use some (slightly awkward) abbreviations to keep proofs onto one page.

$$\begin{aligned} A_{h,v} &\overset{\text{def}}{\equiv} 2h = 2H - v^2 \land 0 \leq h \land h \leq 5 \land v \leq 0 \land g = 1 \land 1 = c \land 1 = f \\ B_{h,v} &\overset{\text{def}}{\equiv} 0 \leq h \land h \leq H \\ h''{=}..{\leq}5 &\overset{\text{def}}{\equiv} (h' = v, v' = -g \,\&\, h \geq 0 \land h \leq 5) \\ h''{=}..{\geq}5 &\overset{\text{def}}{\equiv} (h' = v, v' = -g \,\&\, h \geq 5) \\ \texttt{if}(h{=}0)\,.. &\overset{\text{def}}{\equiv} \texttt{if}(h = 0)\, v := -cv \,\texttt{else} \\ \texttt{if}(4, h{\leq}5)\,.. &\overset{\text{def}}{\equiv} \texttt{if}(4 \leq h \leq 5 \land v \geq 0)\, v := -fv \end{aligned}$$

With these abbreviations, the event-driven ping pong ball formula (1) turns into:

$$A_{h,v} \rightarrow \big[\big((h''{=}..{\leq}5 \cup h''{=}..{\geq}5); \texttt{if}(h{=}0)\,..\texttt{if}(4, h{\leq}5)\,..\big)^*\big]B_{h,v}$$

Let's set out to prove (1) by converting it into a sequent and applying $\mathsf{d}\mathcal{L}$ proof rules:

$$\textit{ind}'\frac{\land\text{l},\land\text{r},ax\dfrac{*}{A_{h,v} \vdash \varphi} \quad \varphi \vdash \big[(h''{=}..{\leq}5 \cup h''{=}..{\geq}5); \texttt{if}(h{=}0)\,..\texttt{if}(4, h{\leq}5)\,..\big]\varphi \quad \land\text{l},\land\text{r},ax\dfrac{*}{\varphi \vdash B_{h,v}}}{\rightarrow\text{r}\dfrac{A_{h,v} \vdash \big[\big((h''{=}..{\leq}5 \cup h''{=}..{\geq}5); \texttt{if}(h{=}0)\,..\texttt{if}(4, h{\leq}5)\,..\big)^*\big]B_{h,v}}{\vdash A_{h,v} \rightarrow \big[\big((h''{=}..{\leq}5 \cup h''{=}..{\geq}5); \texttt{if}(h{=}0)\,..\texttt{if}(4, h{\leq}5)\,..\big)^*\big]B_{h,v}}}$$

The left premise (initial case) and the right premise (use case) prove directly by splitting the conjunctions with $\land$l,$\land$r and then closing by axiom ax. The middle premise (inductive step for preserving the invariant) requires more work:

$$[;]\mathrm{r}\;\dfrac{[\cup]\mathrm{r}\;\dfrac{\dfrac{\ldots}{\varphi \vdash [h''{=}..{\leq}5][\mathtt{if}(h{=}0)\,..\mathtt{if}(4,h{\leq}5)\,..]\varphi} \quad \dfrac{\ldots}{\varphi \vdash [h''{=}..{\geq}5][\mathtt{if}(h{=}0)\,..\mathtt{if}(4,h{\leq}5)\,..]\varphi}}{\varphi \vdash [h''{=}..{\leq}5 \cup h''{=}..{\geq}5][\mathtt{if}(h{=}0)\,..\mathtt{if}(4,h{\leq}5)\,..]\varphi}}{\varphi \vdash [(h''{=}..{\leq}5 \cup h''{=}..{\geq}5);\mathtt{if}(h{=}0)\,..\mathtt{if}(4,h{\leq}5)\,..]\varphi}$$

The right premise will be considered later. The left premise needs the solution of the differential equation

$$h := ..(t) \overset{\text{def}}{\equiv} (h := h - \frac{g}{2}t^2 - vt;\ v := v - gt) \tag{2}$$

The left premise continues as follows:

$$\forall\mathrm{r}\;\dfrac{\rightarrow\mathrm{r}\;\dfrac{\rightarrow\mathrm{r}\;\dfrac{\forall\mathrm{l}\;\dfrac{\varphi, \mathrm{t}{\geq}0, 0{\leq}\mathrm{t}{\leq}\mathrm{t} \rightarrow [h := ..(s)](h \geq 0 \wedge h \leq 5) \vdash [h := ..(\mathrm{t})][\mathtt{if}(h{=}0)\,..\mathtt{if}(4,h{\leq}5)\,..]\varphi}{\varphi, \mathrm{t}{\geq}0, \forall 0{\leq}s{\leq}\mathrm{t}\,[h := ..(s)](h \geq 0 \wedge h \leq 5) \vdash [h := ..(\mathrm{t})][\mathtt{if}(h{=}0)\,..\mathtt{if}(4,h{\leq}5)\,..]\varphi}}{\varphi, \mathrm{t}{\geq}0 \vdash \forall 0{\leq}s{\leq}\mathrm{t}\,[h := ..(s)](h \geq 0 \wedge h \leq 5) \rightarrow [h := ..(\mathrm{t})][\mathtt{if}(h{=}0)\,..\mathtt{if}(4,h{\leq}5)\,..]\varphi}}{\varphi \vdash \mathrm{t}{\geq}0 \rightarrow \big(\forall 0{\leq}s{\leq}\mathrm{t}\,[h := ..(s)](h \geq 0 \wedge h \leq 5) \rightarrow [h := ..(\mathrm{t})][\mathtt{if}(h{=}0)\,..\mathtt{if}(4,h{\leq}5)\,..]\varphi\big)}}{\varphi \vdash \forall t{\geq}0\,\big(\forall 0{\leq}s{\leq}t\,[h := ..(s)](h \geq 0 \wedge h \leq 5) \rightarrow [h := ..(t)][\mathtt{if}(h{=}0)\,..\mathtt{if}(4,h{\leq}5)\,..]\varphi\big)}}{\varphi \vdash [h''{=}..{\leq}5][\mathtt{if}(h{=}0)\,..\mathtt{if}(4,h{\leq}5)\,..]\varphi}\,[']\mathrm{r}$$

The top-most step instantiates the universal quantifier $\forall s$ in the antecedent by a smart choice. That formula in the antecedent expresses that the evolution domain $h \geq 0 \wedge h \leq 5$ holds at all times s between 0 and the duration t of the continuous evolution. That may very well be true, but what our thinking actually only depends on is that the evolution domain still holds at the end time, t of the continuous evolution. The fact that the evolution domain was also true before is not so crucial for our argument here, so we simply instantiate the universally quantifier variable s in the antecedent by the time endpoint t using rule ∀l.

Note 1 (Extreme instantiation). *The proof rule ∀l for universal quantifiers in the antecedent as well as the rule ∃r for existential quantifiers in the succedent allow instantiation of the quantified variable x with any term θ.*

$$(\forall l)\ \frac{\Gamma, \phi(\theta), \forall x\, \phi(x) \vdash \Delta}{\Gamma, \forall x\, \phi(x) \vdash \Delta}\ ^{a}$$

The way this rule is used in KeYmaera is with a direct use of weakening rule Wl to hide the quantified formula:

$$(\forall l)\ \frac{\Gamma, \phi(\theta) \vdash \Delta}{\Gamma, \forall x\, \phi(x) \vdash \Delta}\ ^{b}$$

This instantiation is very helpful if only a single instance θ is important for the argument. Often, an extremal value for x is all it takes for the proof.

This happens often for quantifiers coming from the handling of evolution domains in proof rule [′]r. The proof steps that often help then is instantiation of intermediate time s by the end time t:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{*}{\Gamma, \mathrm{t}{\geq}0 \vdash 0{\leq}\mathrm{t}{\leq}\mathrm{t}, [x := y(\mathrm{t})]\phi} \quad \dfrac{\dots}{\Gamma, \mathrm{t}{\geq}0, [x := y(\mathrm{t})]H \vdash [x := y(\mathrm{t})]\phi}}{\Gamma, \mathrm{t}{\geq}0, 0{\leq}\mathrm{t}{\leq}\mathrm{t} \rightarrow [x := y(\mathrm{t})]H \vdash [x := y(\mathrm{t})]\phi}\,{\rightarrow}l}{\Gamma, \mathrm{t}{\geq}0, \forall 0{\leq}s{\leq}\mathrm{t}\, [x := y(s)]H \vdash [x := y(\mathrm{t})]\phi}\,\forall l}{\Gamma, \mathrm{t}{\geq}0 \vdash (\forall 0{\leq}s{\leq}\mathrm{t}\, [x := y(s)]H) \rightarrow [x := y(\mathrm{t})]\phi}\,{\rightarrow}r}{\Gamma \vdash \mathrm{t}{\geq}0 \rightarrow \big((\forall 0{\leq}s{\leq}\mathrm{t}\, [x := y(s)]H) \rightarrow [x := y(\mathrm{t})]\phi\big)}\,{\rightarrow}r}{\Gamma \vdash \forall t{\geq}0\, \big((\forall 0{\leq}s{\leq}t\, [x := y(s)]H) \rightarrow [x := y(t)]\phi\big)}\,\forall r$$

Similar instantiations can simplify arithmetic in other cases as well.

[a] θ is an arbitrary term, often a new (existential) logical variable X.
[b] θ is an arbitrary term, often a new (existential) logical variable X.

Continuing the above proof as explained in Note 1 recalls that $h := ..(\mathrm{t})$ abbreviates the solution (2) and leads to:

$$\dfrac{\dfrac{\dfrac{\varphi, \mathrm{t}{\geq}0, h - \frac{g}{2}\mathrm{t}^2 - v\mathrm{t} \geq 0, h - \frac{g}{2}\mathrm{t}^2 - v\mathrm{t} \leq 5 \vdash [h := ..(\mathrm{t})][\mathtt{if}(h{=}0)\, ..\mathtt{if}(4, h{\leq}5)\, ..]\varphi}{\varphi, \mathrm{t}{\geq}0, h - \frac{g}{2}\mathrm{t}^2 - v\mathrm{t} \geq 0 \wedge h - \frac{g}{2}\mathrm{t}^2 - v\mathrm{t} \leq 5 \vdash [h := ..(\mathrm{t})][\mathtt{if}(h{=}0)\, ..\mathtt{if}(4, h{\leq}5)\, ..]\varphi}\,\wedge l}{\varphi, \mathrm{t}{\geq}0, [h := ..(s)](h \geq 0 \wedge h \leq 5) \vdash [h := ..(\mathrm{t})][\mathtt{if}(h{=}0)\, ..\mathtt{if}(4, h{\leq}5)\, ..]\varphi}\,[:=]l}{\varphi, \mathrm{t}{\geq}0, 0{\leq}\mathrm{t}{\leq}\mathrm{t} \rightarrow [h := ..(s)](h \geq 0 \wedge h \leq 5) \vdash [h := ..(\mathrm{t})][\mathtt{if}(h{=}0)\, ..\mathtt{if}(4, h{\leq}5)\, ..]\varphi}$$

This formula has gotten a bit lengthy, so abbreviate[1] $h - \frac{g}{2}\mathrm{t}^2 - v\mathrm{t}$ by $\hat{h}$ and abbreviate $v - gt$ by $\hat{v}$. Hence,

$$h := ..(\mathrm{t}) \equiv (h := \hat{h}; v := \hat{v})$$

But there also is a problem that we have not noticed before. Which proof rule do we apply next? Sequent proof rules insist on being applied only to formulas on the top level of the sequent, i.e. directly as a formula of the antecedent or directly to a formula

[1] Abbreviating long terms or long formulas by short names can help simplify KeYmaera proofs as well.

in the succedent. Except for splitting conjunctions in φ by $\wedge$l, the only other formula to apply a proof rule to is the single formula in the succedent, which has a $[\cdot]$ modality with an assignment as the top-level operator. Thus, the only proof rule that applies is [:=]r. Rule [:=]r substitutes the right-hand side θ of an assignment for the variable x assigned to.

$$([:=])\ \frac{\phi_x^\theta}{[x:=\theta]\phi}$$

For simple arithmetic and propositional formulas, it is obvious what such a substitution does. It just replaces x by θ everywhere in the scope of the substitution. That is exactly what we have done with $h := \hat{h}$ when using rule [:=]l in the antecedent in the above proof.

Yet, the above formula

$$[h := ..(\mathrm{t})][\mathtt{if}(h{=}0)\ ..\mathtt{if}(4, h{\leq}5)\ ..]\varphi$$

in the succedent has a postcondition $[\mathtt{if}(h{=}0)\ ..\mathtt{if}(4, h{\leq}5)\ ..]\varphi$ with a modality. It is not necessarily entirely obvious how to substitute $\hat{h}$ for h in such a modality which involves a HP. In this particular case, we could actually perform such a substitution without much difficulty.

Even though such *substitutions* can be defined [Pla10, Chapter 2.5.1] with a little bit of care, we usually stay away from using them.[2]

[2] KeYmaera would even need to be persuaded to use these substitutions on HPs at all by setting the advanced option *update modalities*.

Note 2 (Excursion: Updates). *For that reason, KeYmaera simply postpones the substitution resulting from an assignment according to rule [:=]r,[:=]l,⟨:=⟩r,⟨:=⟩l if the postcondition is not a first-order formula but involves modalities with HPs. What this corresponds to is, essentially to leave the assignment as is and apply proof rules to the postcondition, but only in this particular case of assignments! Because that would be a bit confusing without further notice, KeYmaera changes the notation slightly and turns an assignment into what it calls an* update.

$$(R4)\ \frac{\{x:=\theta\}\phi}{[x:=\theta]\phi} \qquad (R5)\ \frac{\phi_x^\theta}{\{x:=\theta\}\phi}$$

The meaning of the formula $\{x:=\theta\}\phi$ in the premise of R4 is exactly the same as the formula $[x:=\theta]\phi$ in the conclusion of R4. The notation $\{x:=\theta\}\phi$ is only meant as a reminder for the user that KeYmaera decided to put the handling of the assignment by substitution on hold until the postcondition ϕ looks more civilized (meaning: first-order). KeYmaera collects all the state changes in such an update (or a list of updates). KeYmaera will then, essentially, just carry the $\{x:=\theta\}$ around with it and apply the sequent proof rules directly to postcondition ϕ until the substitution can be applied (R5) which will make the update disappear again. Thus, KeYmaera splits the assignment rule [:=] into two parts: R4 followed by R5.

More information on updates can be found in [Pla08, Pla10, Chapter 2.2,2.3,2.5].

Recall that we use the abbreviated notation $\hat{h}$ and $\hat{v}$ and, hence $h := ..(\mathrm{t})$ is just $h := \hat{h}; v := \hat{v}$.

After using rule R4 to changing the assignment notation into an update notation (remember that this only changes notation because both are equivalent) the above sequent reads

$$\varphi, \mathrm{t}{\geq}0, \hat{h} \geq 0, \hat{h} \leq 5 \vdash \{h := \hat{h}; v := \hat{v}\}[\texttt{if}(h{=}0)\ ..\texttt{if}(4, h{\leq}5)\ ..]\varphi \tag{3}$$

Before proceeding with any proof, we need to figure out what to do with the `if-then-else` statements. Before doing any proofs, previous lectures, replaced `if-then-else` statements by other hybrid program statements, which is always possible. In this lecture, we decide differently and develop a direct proof rule for `if-then-else`.

$$(\langle\text{if}\rangle)\ \frac{(H \to \langle\alpha\rangle\phi) \wedge (\neg H \to \langle\beta\rangle\phi)}{\langle \texttt{if}(H)\,\alpha\,\texttt{else}\,\beta\rangle\phi} \qquad ([\text{if}])\ \frac{(H \to [\alpha]\phi) \wedge (\neg H \to [\beta]\phi)}{[\texttt{if}(H)\,\alpha\,\texttt{else}\,\beta]\phi}$$

When following up on a use of the [if] rule in the succedent of a sequent (call the corresponding sequent rule [if]r) with propositional rules ∧r,→r, the sequent splits into two cases as expected:[3]

[3] These propositional steps following the [if]r rule are so useful that KeYmaera does them for you right away. In fact, KeYmaera even jumps from the formula at the bottom directly to the two premises.

$$\dfrac{\dfrac{\Gamma, H \vdash [\alpha]\phi}{\Gamma \vdash H \to [\alpha]\phi}\,{\to}\text{r} \qquad \dfrac{\Gamma, \neg H \vdash [\beta]\phi}{\Gamma \vdash \neg H \to [\beta]\phi}\,{\to}\text{r}}{\dfrac{\Gamma \vdash (H \to [\alpha]\phi) \wedge (\neg H \to [\beta]\phi)}{\Gamma \vdash [\texttt{if}(H)\,\alpha\,\texttt{else}\,\beta]\phi, \Delta}\,[\text{if}]\text{r}}\,\wedge\text{r}$$

Indeed, the conjecture at the bottom says that we want to show that all behavior of a system whose behavior branches by an `if-then-else` is safe (satisfies ϕ). We do not know which state we are in, except that we get to assume it satisfies Γ (and the negation of Δ by the sequent semantics). So there are usually many possible states. Hence, there is generally no way of knowing whether if-condition H evaluates to $true$ or $false$. Hence, we need to consider both options. If H evaluates to $true$, then α runs, so all α behavior needs to be shown to be safe in that case (left premise). If H evaluates to $false$, then β runs instead, so all β behavior needs to be shown to be safe (right premise).

Applying the [if]r rule two times to the sequent (3) yields 3 premises corresponding to the 3 possible outcomes of the `if-then-else` statements (Exercise 1):

$$\begin{aligned}
&\varphi, \mathfrak{t}{\geq}0, \hat{h} \geq 0, \hat{h} \leq 5, \hat{h} = 0 \vdash \{h := \hat{h}; v := \hat{v}\}[v := -cv]\varphi \\
&\varphi, \mathfrak{t}{\geq}0, \hat{h} \geq 0, \hat{h} \leq 5, \hat{h} \neq 0, 4 \leq \hat{h} \leq 5 \wedge \hat{v} \geq 0 \vdash \{h := \hat{h}; v := \hat{v}\}[v := -fv]\varphi \qquad (4) \\
&\varphi, \mathfrak{t}{\geq}0, \hat{h} \geq 0, \hat{h} \leq 5, \hat{h} \neq 0, \neg(4 \leq \hat{h} \leq 5 \wedge \hat{v} \geq 0) \vdash \{h := \hat{h}; v := \hat{v}\}\varphi
\end{aligned}$$

Let's address the three branches separately. The first branch of (4) turns into the following using either [:=]r or R4 via R5:

$$\varphi, \mathfrak{t}{\geq}0, \hat{h} \geq 0, \hat{h} \leq 5, \hat{h} = 0 \vdash \{h := \hat{h}; v := -c\hat{v}\}\varphi$$

which gives the following by applying the update using R5 (can also be obtained directly by [:=]r):

$$\varphi, \mathfrak{t}{\geq}0, \hat{h} \geq 0, \hat{h} \leq 5, \hat{h} = 0 \vdash 0 \leq \hat{h} \leq 5 \wedge (\hat{h} = 5 \to -c\hat{v} \leq 0) \wedge 1 \geq c \geq 0 \wedge g > 0 \wedge f \geq 0$$

That proves by arithmetic, because $\hat{h} = 0$ and implies $0 \leq \hat{h} \leq 5$ and $\hat{h} \neq 5$ and the other parts prove similarly.[4]

The second branch of (4) turns by either [:=] or via R4 and R5 into:

$$\varphi, \mathfrak{t}{\geq}0, \hat{h} \geq 0, \hat{h} \leq 5, \hat{h} \neq 0, 4 \leq \hat{h} \leq 5 \wedge \hat{v} \geq 0 \vdash \{h := \hat{h}; v := -f\hat{v}\}\varphi$$

which R5 turns into

$$\varphi, \mathfrak{t}{\geq}0, \hat{h} \geq 0, \hat{h} \leq 5, \hat{h} \neq 0, 4 \leq \hat{h} \leq 5 \wedge \hat{v} \geq 0 \vdash 0 \leq \hat{h} \leq 5 \wedge (\hat{h} = 5 \to -f\hat{v} \leq 0) \wedge 1 \geq c \geq 0 \wedge g > 0 \wedge f \geq 0$$

which proves by arithmetic using that $f \geq 0$ and $\hat{v} \geq 0$ as well as the fact that $4 \leq \hat{h} \leq 5$ trivially implies $0 \leq \hat{h} \leq 5$, which is obvious thanks to the abbreviations.

The third branch of (4) turns with [:=]r or R5 into:

$$\varphi, \mathfrak{t}{\geq}0, \hat{h} \geq 0, \hat{h} \leq 5, \hat{h} \neq 0, \neg(4 \leq \hat{h} \leq 5 \wedge \hat{v} \geq 0) \vdash 0 \leq \hat{h} \leq 5 \wedge (\hat{h} = 5 \to \hat{v} \leq 0) \wedge 1 \geq c \geq 0 \wedge g > 0 \wedge f \geq 0$$

[4] Note how abbreviations simplify this proof step compared to what would have happened when expanding $\hat{h}$.

which a combination of propositional rules and/or arithmetic proves (Exercise!)

All this reasoning was for just the branch of the proof that came from the dynamics $h''{=}..{\leq}5$. There is a second branch with the dynamics $h''{=}..{\geq}5$. In that one, the proof is quite similar, except that it makes crucial use of the conjunct $h = 5 \rightarrow v \leq 0$ of the invariant φ. Without that condition available as an assumption from the invariant φ, the upper physics $h''{=}..{\geq}5$ would obviously violate the safety condition $0 \leq h \leq 5$ if the velocity at $h = 5$ were positive $v > 0$.

Stepping back, it is crucial to observe this general phenomenon. We have to be able to assume the turning-point part $h = 5 \rightarrow v \leq 0$ of invariant φ for the proof of the upper dynamics $h''{=}..{\geq}5$. But we also need to prove that this turning-point invariant $h = 5 \rightarrow v \leq 0$ holds along with the rest of the invariant φ after all runs of the lower physics $h''{=}..{\leq}5$. That is, this part of the invariant φ transports knowledge about the behavior of the controller in the lower physics $h''{=}..{\leq}5$ to be used in the proof parts about the upper physics $h''{=}..{\geq}5$.

Note 3 (Invariants transport knowledge)**.** *Invariants can be used to gather knowledge about the individual bits and pieces of a system and make them accessible to the other parts.*

3 Proving Systems with Delays in Control

$$2h = 2H - v^2 \land 0 \leq h \land h \leq 5 \land v \leq 0 \land g = 1 > 0 \land 1 = c \geq 0 \land 1 = f > 0 \rightarrow$$
$$\big[\big(\texttt{if}(h = 0)\, v := -cv; \texttt{if}((h > 5\frac{1}{2} - v \lor 2h > 2 \cdot 5 - v^2 \land v < 1) \land v \geq 0)\, v := -fv; \quad (5)$$
$$t := 0; h' = v, v' = -g, t' = 1 \,\&\, h \geq 0 \land t \leq 1\big)^*\big](0 \leq h \leq 5)$$

Lecture 8 on Events & Delays identified the following invariant for this system:

$$2h = 2H - v^2 \land h \geq 0 \land h \leq 5 \tag{6}$$

although there was no proof yet. Recall that (global) invariants need to be augmented with the usual assumptions about the unchanged variables, like $g = 1 \land 1 = c \land 1 = f$. So let's define the formula we conjecture to be an invariant as:

$$\varphi \overset{\text{def}}{\equiv} 2h = 2H - v^2 \land h \geq 0 \land h \leq 5 \land g = 1 \land 1 = c \land 1 = f$$

With this invariant, (5) is provable in KeYmaera.

4 Cutting Real Arithmetic

The *cut* rule from Lecture 6 on Truth & Proof is not just a curiosity, but can be very helpful in practice. It can speed up real arithmetic a lot when using a cut to replace a difficult arithmetic formula by a simpler one that is sufficient for the proof.

For example, suppose $\psi(x)$ is a very complicated formula of first-order real arithmetic. Then proving the following formula

$$(x - y)^2 \leq 0 \land \psi(x) \rightarrow \psi(y)$$

by just real arithmetic will turn out to be surprisingly difficult and can take ages. Yet, thinking about it, $(x - y)^2 \leq 0$ implies that $y = x$, which should make the rest of the proof easy since, $\psi(x)$ should easily imply $\psi(y)$ if $y = x$. How do we exhibit a proof based on these thoughts?

The critical idea to make such a proof work is to use *cut* for a creative cut with the suitable arithmetic. So we choose $y = x$ as the cut formula ϕ in *cut* and proceed as follows:

$$\dfrac{\dfrac{\dfrac{\dfrac{(x-y)^2 \leq 0 \vdash y = x}{(x-y)^2 \leq 0 \vdash y = x, \psi(y)}\,\text{Wr}}{(x-y)^2 \leq 0, \psi(x) \vdash y = x, \psi(y)}\,\text{Wl} \qquad \dfrac{\dfrac{*}{\psi(x), y = x \vdash \psi(x)}\,ax}{\psi(x), y = x \vdash \psi(y)}\,\text{=r}}{(x-y)^2 \leq 0, \psi(x), y = x \vdash \psi(y)}\,\text{Wl}}{(x-y)^2 \leq 0, \psi(x) \vdash \psi(y)}\,cut}{(x-y)^2 \leq 0 \land \psi(x) \vdash \psi(y)}\,\land\text{l}}{\vdash (x-y)^2 \leq 0 \land \psi(x) \rightarrow \psi(y)}\,\rightarrow\text{r}$$

Indeed, the left premise proves easily using real arithmetic. The right premise proves comparably easily as well. This proof uses proof rule =r that we discuss next.

5 Applying Equations by Substitution

The above cut proof uses the following proof rule for applying an equation to a formula ϕ by substituting the left-hand side x of an equation by its right-hand side θ. This substitution is sound, because x is assumed to be equal to θ in the antecedent. The same rule works applies to formulas ϕ that are in the antecedent (=l) as well as in the succedent (=r). Obviously, the assumed equality $x = \theta$ has to be in the antecedent for the rule to be sound.

$$(=\text{r})\ \frac{\Gamma, x=\theta \vdash \phi_x^\theta, \Delta}{\Gamma, x=\theta \vdash \phi, \Delta} \qquad (=\text{l})\ \frac{\Gamma, x=\theta, \phi_x^\theta \vdash \Delta}{\Gamma, x=\theta, \phi \vdash \Delta}$$

It would be okay to use the equation in the other direction for replacing all occurrences of θ by x, because the equation $\theta = x$ is equivalent to $x = \theta$.

Exercises

Exercise 1. Explicitly complete the proof steps that lead from (3) to the 3 branches identified in the lecture notes by writing a proper sequent derivation. Recall how updates are delayed substitutions and that they "hang around" until they can be applied.

Exercise 2. The sequent proof shown in these lecture notes is for the case coming from the lower dynamics $h''{=}..{\leq}5$. This alone does not prove (1). Write a sequent proof for the missing branches coming from the upper dynamics $h''{=}..{\geq}5$.

Exercise 3. Develop a sequent proof for the time-triggered ping pong ball (5). Is it easier or more difficult than the proof for (1)?

Exercise 4. Relate the event-driven system proof for (1) discussed in lecture to the proof that KeYmaera produces. What do they have in common? Where do they differ?

References

[Pla08] André Platzer. Differential dynamic logic for hybrid systems. *J. Autom. Reas.*, 41(2):143–189, 2008. doi:10.1007/s10817-008-9103-8.

[Pla10] André Platzer. *Logical Analysis of Hybrid Systems: Proving Theorems for Complex Dynamics*. Springer, Heidelberg, 2010. doi:10.1007/978-3-642-14509-4.

[PQR09] André Platzer, Jan-David Quesel, and Philipp Rümmer. Real world verification. In Renate A. Schmidt, editor, *CADE*, volume 5663 of *LNCS*, pages 485–501. Springer, 2009. doi:10.1007/978-3-642-02959-2_35.