15-424: Foundations of Cyber-Physical Systems

Lecture Notes on Differential & Temporal Proofs

André Platzer

Carnegie Mellon University

Lecture 17

1 Introduction

This lecture continues the study of temporal aspects of cyber-physical systems that Lecture 5 on Differential & Temporal Logics started. The trace semantics of hybrid programs as well as the semantics of differential temporal dynamic logic (dTL) [Pla10], a temporal extension of differential dynamic logic d$\mathcal{L}$ [Pla08, Pla12], have been discussed in said lecture.

This lecture is based on [Pla10, Chapter 4], which extends [Pla07].

2 Temporal Proof Rules

When extending a logic, it is not enough to extend just the syntax (Lecture 5) and semantics (Lecture 5). The proof rules also need to be extended to handle the new concepts, that is the temporal modalities of dTL.

This section shows a sequent calculus for verifying temporal specifications of hybrid systems in differential temporal dynamic logic dTL. With the basic idea being to perform a symbolic decomposition, the calculus transforms hybrid programs successively into simpler logical formulas describing their effects. Statements about the temporal behaviour of a hybrid program are successively reduced to corresponding nontemporal statements about the intermediate states. This lecture shows a proof calculus for differential temporal dynamic logic dTL that inherits the proof rules of d$\mathcal{L}$ from previous lectures and adds new proof rules for temporal modalities.

Inherited Nontemporal Rules The dTL calculus is presented in Fig. 1 and inherits the (nontemporal) d$\mathcal{L}$ proof rules, i.e., the propositional, first-order, dynamic, and global rules from d$\mathcal{L}$. That is, it includes the propositional and quantifier rules from Lecture 6. The dynamic rules ($\langle;\rangle$–$[']$) and global rules ($[]gen$,$\langle\rangle gen$,ind,con) for handling nontemporal dynamic modalities are also inherited directly from Lecture 6. The only possible exception is that $[\cup]$,$\langle\cup\rangle$ can be generalised to apply to formulas of the form $[\alpha\cup\beta]\pi$ where π is an arbitrary trace formula, and not just a state formula as in d$\mathcal{L}$. Thus, π may begin with $\Box$ or $\Diamond$, which is why the rules are repeated in this generalised form as $[\cup]\Box$ and $\langle\cup\rangle\Diamond$ in Fig. 1.

Note 1.

$$([\cup]\Box)\quad \frac{[\alpha]\pi \land [\beta]\pi}{[\alpha\cup\beta]\pi}\;\text{[1]} \qquad\qquad (\langle\cup\rangle\Diamond)\quad \frac{\langle\alpha\rangle\pi \lor \langle\beta\rangle\pi}{\langle\alpha\cup\beta\rangle\pi}\;\text{[1]}$$

$$([;]\Box)\quad \frac{[\alpha]\Box\phi \land [\alpha][\beta]\Box\phi}{[\alpha;\beta]\Box\phi} \qquad\qquad (\langle;\rangle\Diamond)\quad \frac{\langle\alpha\rangle\Diamond\phi \lor \langle\alpha\rangle\langle\beta\rangle\Diamond\phi}{\langle\alpha;\beta\rangle\Diamond\phi}$$

$$([?]\Box)\quad \frac{\phi}{[?\chi]\Box\phi} \qquad\qquad (\langle?\rangle\Diamond)\quad \frac{\phi}{\langle?\chi\rangle\Diamond\phi}$$

$$([:=]\Box)\quad \frac{\phi \land [x:=\theta]\phi}{[x:=\theta]\Box\phi} \qquad\qquad (\langle:=\rangle\Diamond)\quad \frac{\phi \lor \langle x:=\theta\rangle\phi}{\langle x:=\theta\rangle\Diamond\phi}$$

$$([']\Box)\quad \frac{[x'=\theta]\phi}{[x'=\theta]\Box\phi} \qquad\qquad (\langle'\rangle\Diamond)\quad \frac{\langle x'=\theta\rangle\phi}{\langle x'=\theta\rangle\Diamond\phi}$$

$$([^{*n}]\Box)\quad \frac{[\alpha;\alpha^*]\Box\phi}{[\alpha^*]\Box\phi} \qquad\qquad (\langle^{*n}\rangle\Diamond)\quad \frac{\langle\alpha;\alpha^*\rangle\Diamond\phi}{\langle\alpha^*\rangle\Diamond\phi}$$

$$([^*]\Box)\quad \frac{[\alpha^*][\alpha]\Box\phi}{[\alpha^*]\Box\phi} \qquad\qquad (\langle^*\rangle\Diamond)\quad \frac{\langle\alpha^*\rangle\langle\alpha\rangle\Diamond\phi}{\langle\alpha^*\rangle\Diamond\phi}$$

[1] π is a trace formula and—unlike the state formulas ϕ and ψ—may thus begin with a temporal modality $\Box$ or $\Diamond$.

Figure 1: Axiomatization of differential temporal dynamic logic dTL

Temporal Rules The new temporal rules in Fig. 1 for the dTL calculus successively transform temporal specifications of hybrid programs into nontemporal d$\mathcal{L}$ formulas. The idea underlying this transformation is to decompose hybrid programs and recursively augment intermediate state transitions with appropriate specifications. Also see Fig. 2 for an illustration of the correspondence of a representative set of proof rules for temporal modalities to the trace semantics of hybrid programs (Def. **??**).

Rule $[;]\Box$ decomposes invariants of $\alpha;\beta$ (i.e., $[\alpha;\beta]\Box\phi$ holds) into an invariant of α (i.e., $[\alpha]\Box\phi$) and an invariant of β that holds when β is started in *any* final state of α (i.e., $[\alpha]([\beta]\Box\phi)$). Its difference with the d$\mathcal{L}$ rule $[;]$ thus is that the dTL rule $[;]\Box$ also checks safety invariant ϕ at the symbolic states in between the execution of α and β, and recursively so because of the temporal modality $\Box$. Again, see Fig. 2 for an illustration

$$\frac{\phi \land [x := \theta]\phi}{[x := \theta]\Box\phi}$$

$$\frac{[x' = \theta]\phi}{[x' = \theta]\Box\phi}$$

$$\frac{[\alpha]\Box\phi \land [\alpha][\beta]\Box\phi}{[\alpha; \beta]\Box\phi}$$

$$\frac{[\alpha]\Box\phi \land [\beta]\Box\phi}{[\alpha \cup \beta]\Box\phi}$$

$$\frac{[\alpha^*][\alpha]\Box\phi}{[\alpha^*]\Box\phi}$$

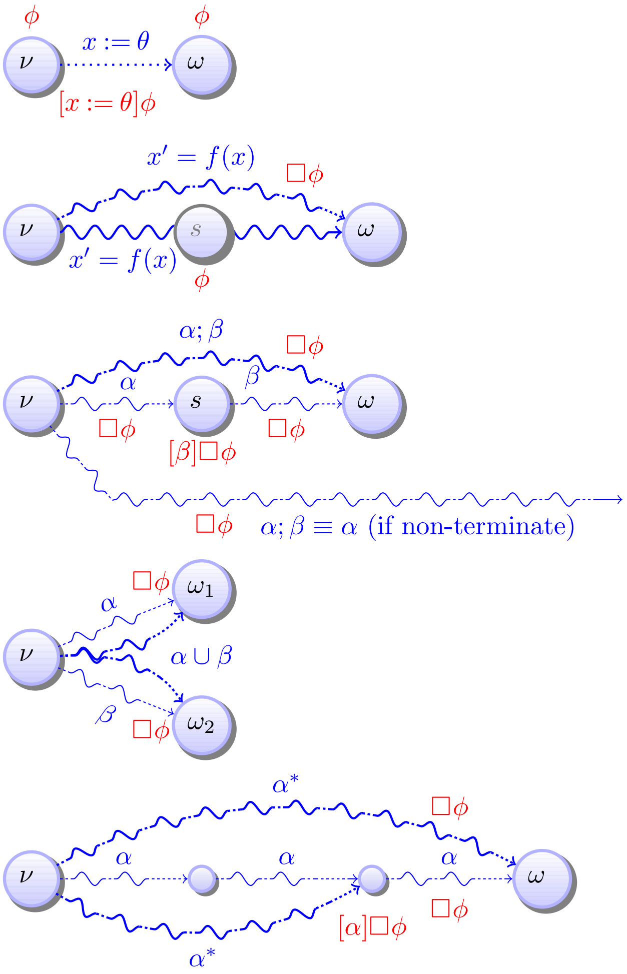


Figure 2: Correspondence of temporal proof rules and trace semantics

of this proof principle.

Rule $[:=]\Box$ expresses that invariants of assignments need to hold before and after the discrete change (similarly for $[?]\Box$, except that tests do not lead to a state change, so ϕ holding before the test is all there is to it). Rule $[']\Box$ can directly reduce invariants of continuous evolutions to nontemporal formulas as restrictions of solutions of differential equations are themselves solutions of different duration and thus already included in the evolutions of $x' = \theta$. In particular, observe that the handling of differential equations within hybrid systems is fully encapsulated within the fragment of dynamic rules from d$\mathcal{L}$.

The (optional) iteration rule $[*^n]\Box$ can partially unwind loops. It relies on rule $[;]\Box$ and is simpler than d$\mathcal{L}$ rule $[*^n]$, because the other rules will inductively produce a premise that ϕ holds in the current state, because of the temporal modality $\Box\phi$. The dual rules $\langle\cup\rangle\Diamond$,$\langle;\rangle\Diamond$,$\langle?\rangle\Diamond$,$\langle:=\rangle\Diamond$,$\langle'\rangle\Diamond$,$\langle*^n\rangle\Diamond$ work similarly.

In d$\mathcal{L}$ (Lecture 7 on Control Loops & Invariants), the primary means for handling loops are the invariant induction (*ind*) and variant convergence (*con*) rules. The logic dTL takes a different, completely modular approach for verifying temporal properties of loops based on the d$\mathcal{L}$ capabilities for verifying nontemporal properties of loops. Rules $[*]\Box$ and $\langle*\rangle\Diamond$ actually *define* temporal properties of loops inductively. Rule $[*]\Box$ expresses that ϕ holds at all times during repetitions of α (i.e., $[\alpha^*]\Box\phi$) iff, *after* repeating α any number of times, ϕ holds at all times *during* one execution of α (i.e., $[\alpha^*]([\alpha]\Box\phi)$). See Fig. 2 for an illustration. Dually, $\langle*\rangle\Diamond$ expresses that α holds at some time during repetitions of α (i.e., $\langle\alpha^*\rangle\Diamond\phi$) iff, after some number of repetitions of α, formula ϕ holds at some point during one execution of α (i.e., $\langle\alpha^*\rangle(\langle\alpha\rangle\Diamond\phi)$). In this context, the nontemporal modality $\langle\alpha^*\rangle$ can be thought of as skipping over to the iteration of α during which ϕ actually occurs, as expressed by the nested dTL formula $\langle\alpha\rangle\Diamond\phi$. The inductive definition rules $[*]\Box$ and $\langle*\rangle\Diamond$ completely reduce temporal properties of loops to dTL properties of standard nontemporal d$\mathcal{L}$-modalities such that standard induction (*ind*) or convergence rules (*con*) can be used for the outer nontemporal modality of the loop. Hence, after applying the inductive loop definition rules $[*]\Box$ and $\langle*\rangle\Diamond$, the standard d$\mathcal{L}$ loop invariant and variant rules can be used for verifying temporal properties of loops without change, except that the postcondition contains temporal modalities.

Rules for handling $[\alpha]\Diamond\phi$ and $\langle\alpha\rangle\Box\phi$ are discussed in [Pla10].

3 Temporal Bouncing Ball

Recall the bouncing ball that has served us so well in previous lectures.

$$(v^2 \leq 2g(H-h) \wedge h \geq 0 \wedge g > 0 \wedge H \geq 0 \wedge 1 > c \geq 0) \rightarrow [\mathit{ball}](0 \leq h \leq H). \qquad (1)$$

Use the abbreviations

$$\begin{aligned}
\mathit{ball} &\equiv h' = v, v' = -g \,\&\, h \geq 0; (?h > 0 \cup (?h = 0; v := -cv)) \\
\psi &\equiv g > 0 \land H \geq 0 \land 1 > c \geq 0, \\
\varphi &\equiv v^2 \leq 2g(H-h) \land h \geq 0 \\
\langle h := ..(t) \rangle F &\equiv \langle h := h + vt - \frac{g}{2}t^2; v := v - tg \rangle F.
\end{aligned}$$

When simplifying the *ball* dynamics to remove evolution domain constraints:

$$h' = v, v' = -g; (?h > 0 \cup (?h = 0; v := -cv))$$

the proof for the simplified bouncing ball property without evolution domain constraint is shown in Fig. 3. The d$\mathcal{L}$ proof for the original bouncing ball property (1) with an evolution domain constraint is shown in Fig. 4.

4 Verification Example

Recall the bouncing ball. The proofs from previous lectures or Fig. 4 can be generalized easily to a proof of the temporal property

$$\begin{aligned}
&v^2 \leq 2g(H-h) \land h \geq 0 \land g > 0 \land H \geq 0 \land 1 > c \geq 0 \\
&\qquad \to [(h'' = -g \,\&\, h \geq 0; (?h > 0 \cup (?h = 0; v := -cv)))^*]\Box(0 \leq h \leq H). \quad (2)
\end{aligned}$$

The only aspect of the proof that changes is that the temporal proof rules in Fig. 1 are used instead of the dynamic proof rules for d$\mathcal{L}$, and that the resulting extra proof goals for the invariance property at intermediate steps have to be proven.

In contrast, the proof in Fig. 3 for the simplified dynamics without evolution domain restriction $h \geq 0$ cannot be generalized to a proof of the temporal property

$$\begin{aligned}
&v^2 \leq 2g(H-h) \land h \geq 0 \land g > 0 \land H \geq 0 \land 1 > c \geq 0 \\
&\qquad \to [(h'' = -g; (?h > 0 \cup (?h = 0; v := -cv)))^*]\Box(0 \leq h \leq H). \quad (3)
\end{aligned}$$

This difference in provability is for good reasons. The property in (2) is valid, but the property in (3) is not! While there was no noticeable semantical difference between the nontemporal d$\mathcal{L}$ counterparts of the properties (2) versus (3), there is a decisive difference between the corresponding temporal properties (3) and (2). Because there is no evolution domain restriction in (3), its hybrid program does not prevent continuous evolution to a negative height under the floor ($h < 0$), for which $0 \leq h \leq H$ does not hold.

The reason for this discrepancy of the temporal version compared to the nontemporal versions thus is that the nontemporal modalities do not "see" the temporary violation of $0 \leq h \leq H$. Such a temporary violation of $0 \leq h$ during the continuous evolution does not produce a successful run of the hybrid program, because it is blocked by

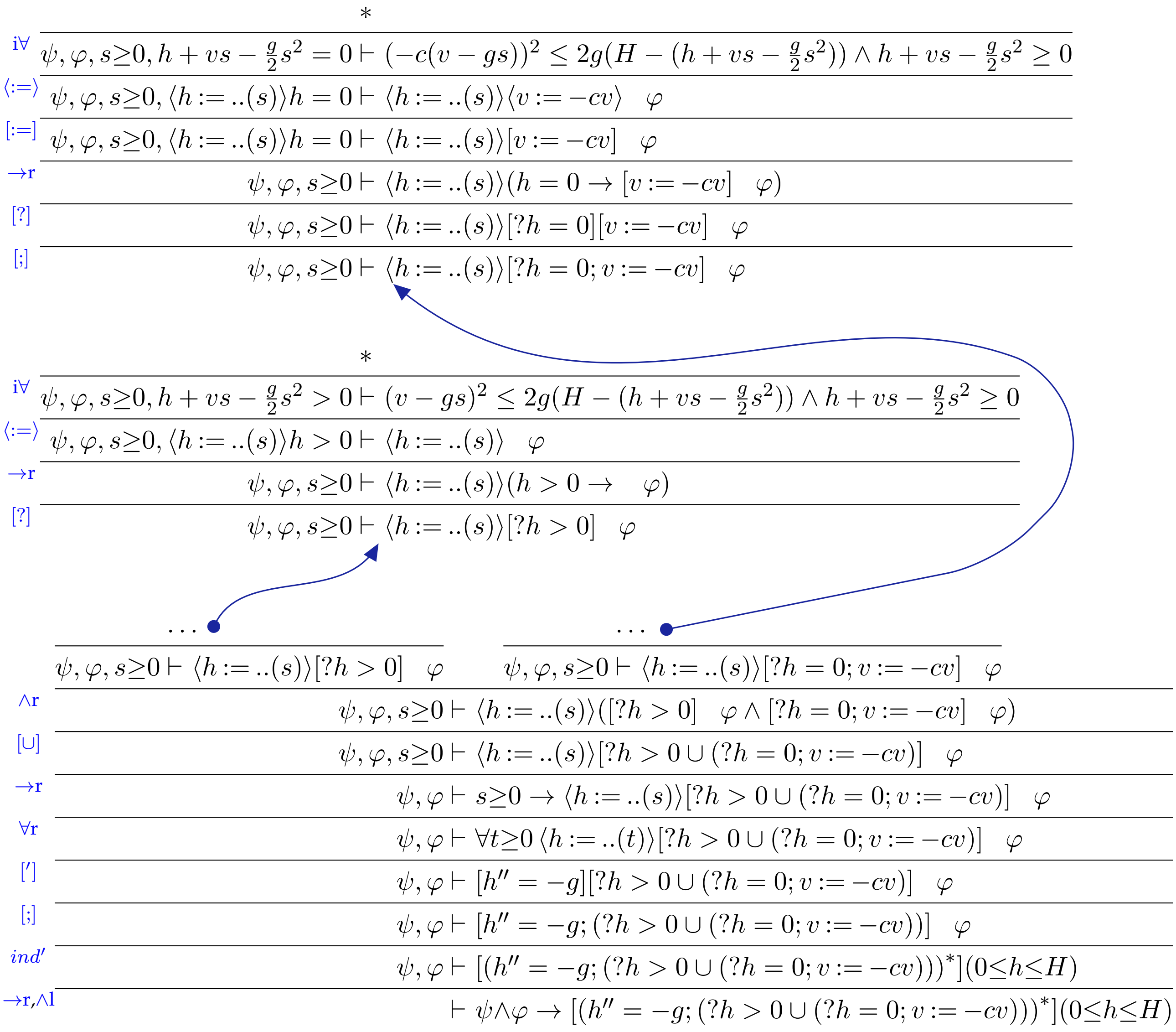
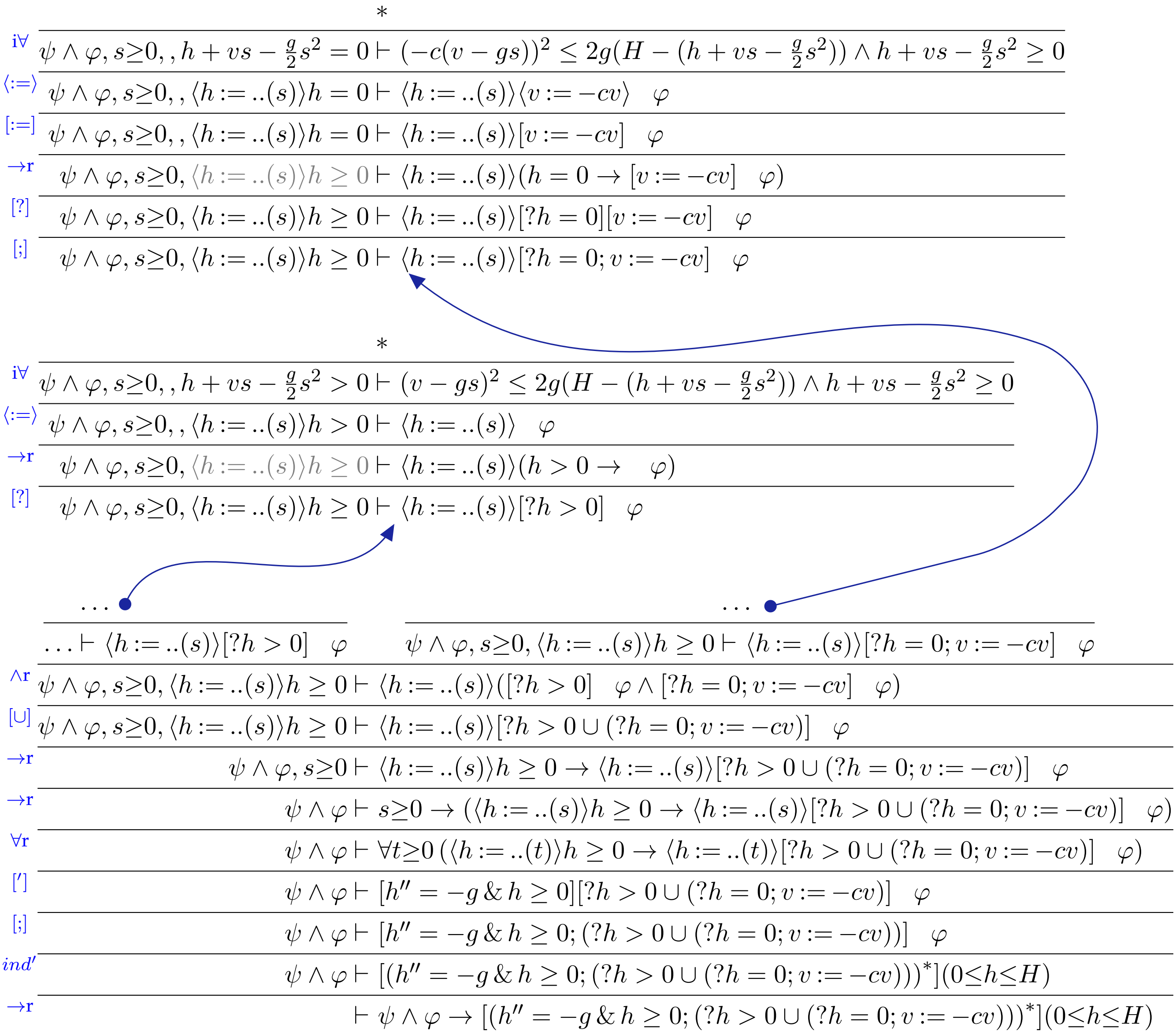

*
i∀ $\psi, \varphi, s\geq0, h+vs-\frac{g}{2}s^2=0 \vdash (-c(v-gs))^2 \leq 2g(H-(h+vs-\frac{g}{2}s^2)) \land h+vs-\frac{g}{2}s^2 \geq 0$
⟨:=⟩ $\psi, \varphi, s\geq0, \langle h:=..(s)\rangle h=0 \vdash \langle h:=..(s)\rangle\langle v:=-cv\rangle \quad \varphi$
[:=] $\psi, \varphi, s\geq0, \langle h:=..(s)\rangle h=0 \vdash \langle h:=..(s)\rangle[v:=-cv] \quad \varphi$
→r $\psi, \varphi, s\geq0 \vdash \langle h:=..(s)\rangle(h=0 \to [v:=-cv] \quad \varphi)$
[?] $\psi, \varphi, s\geq0 \vdash \langle h:=..(s)\rangle[?h=0][v:=-cv] \quad \varphi$
[;] $\psi, \varphi, s\geq0 \vdash \langle h:=..(s)\rangle[?h=0; v:=-cv] \quad \varphi$
*
i∀ $\psi, \varphi, s\geq0, h+vs-\frac{g}{2}s^2>0 \vdash (v-gs)^2 \leq 2g(H-(h+vs-\frac{g}{2}s^2)) \land h+vs-\frac{g}{2}s^2 \geq 0$
⟨:=⟩ $\psi, \varphi, s\geq0, \langle h:=..(s)\rangle h>0 \vdash \langle h:=..(s)\rangle \quad \varphi$
→r $\psi, \varphi, s\geq0 \vdash \langle h:=..(s)\rangle(h>0 \to \quad \varphi)$
[?] $\psi, \varphi, s\geq0 \vdash \langle h:=..(s)\rangle[?h>0] \quad \varphi$
. . .
. . .
$\psi, \varphi, s\geq0 \vdash \langle h:=..(s)\rangle[?h>0] \quad \varphi$
$\psi, \varphi, s\geq0 \vdash \langle h:=..(s)\rangle[?h=0; v:=-cv] \quad \varphi$
∧r $\psi, \varphi, s\geq0 \vdash \langle h:=..(s)\rangle([?h>0] \quad \varphi \land [?h=0; v:=-cv] \quad \varphi)$
[∪] $\psi, \varphi, s\geq0 \vdash \langle h:=..(s)\rangle[?h>0 \cup (?h=0; v:=-cv)] \quad \varphi$
→r $\psi, \varphi \vdash s\geq0 \to \langle h:=..(s)\rangle[?h>0 \cup (?h=0; v:=-cv)] \quad \varphi$
∀r $\psi, \varphi \vdash \forall t\geq0\, \langle h:=..(t)\rangle[?h>0 \cup (?h=0; v:=-cv)] \quad \varphi$
['] $\psi, \varphi \vdash [h''=-g][?h>0 \cup (?h=0; v:=-cv)] \quad \varphi$
[;] $\psi, \varphi \vdash [h''=-g; (?h>0 \cup (?h=0; v:=-cv))] \quad \varphi$
ind' $\psi, \varphi \vdash [(h''=-g; (?h>0 \cup (?h=0; v:=-cv)))^*](0\leq h\leq H)$
→r,∧l $\vdash \psi\land\varphi \to [(h''=-g; (?h>0 \cup (?h=0; v:=-cv)))^*](0\leq h\leq H)$

Figure 3: Bouncing ball proof (no evolution domain)



$$*$$

$$\text{i}\forall \quad \psi \land \varphi, s{\geq}0, , h + vs - \frac{g}{2}s^2 = 0 \vdash (-c(v-gs))^2 \leq 2g(H - (h + vs - \frac{g}{2}s^2)) \land h + vs - \frac{g}{2}s^2 \geq 0$$

$$\langle{:=}\rangle \quad \psi \land \varphi, s{\geq}0, , \langle h := ..(s)\rangle h = 0 \vdash \langle h := ..(s)\rangle \langle v := -cv\rangle \quad \varphi$$

$$[{:=}] \quad \psi \land \varphi, s{\geq}0, , \langle h := ..(s)\rangle h = 0 \vdash \langle h := ..(s)\rangle [v := -cv] \quad \varphi$$

$$\to\text{r} \quad \psi \land \varphi, s{\geq}0, \langle h := ..(s)\rangle h \geq 0 \vdash \langle h := ..(s)\rangle (h = 0 \to [v := -cv] \quad \varphi)$$

$$[?] \quad \psi \land \varphi, s{\geq}0, \langle h := ..(s)\rangle h \geq 0 \vdash \langle h := ..(s)\rangle [?h = 0][v := -cv] \quad \varphi$$

$$[;] \quad \psi \land \varphi, s{\geq}0, \langle h := ..(s)\rangle h \geq 0 \vdash \langle h := ..(s)\rangle [?h = 0; v := -cv] \quad \varphi$$

$$*$$

$$\text{i}\forall \quad \psi \land \varphi, s{\geq}0, , h + vs - \frac{g}{2}s^2 > 0 \vdash (v-gs)^2 \leq 2g(H - (h + vs - \frac{g}{2}s^2)) \land h + vs - \frac{g}{2}s^2 \geq 0$$

$$\langle{:=}\rangle \quad \psi \land \varphi, s{\geq}0, , \langle h := ..(s)\rangle h > 0 \vdash \langle h := ..(s)\rangle \quad \varphi$$

$$\to\text{r} \quad \psi \land \varphi, s{\geq}0, \langle h := ..(s)\rangle h \geq 0 \vdash \langle h := ..(s)\rangle (h > 0 \to \quad \varphi)$$

$$[?] \quad \psi \land \varphi, s{\geq}0, \langle h := ..(s)\rangle h \geq 0 \vdash \langle h := ..(s)\rangle [?h > 0] \quad \varphi$$

$$\ldots \qquad\qquad \ldots$$

$$\ldots \vdash \langle h := ..(s)\rangle [?h > 0] \quad \varphi \qquad \psi \land \varphi, s{\geq}0, \langle h := ..(s)\rangle h \geq 0 \vdash \langle h := ..(s)\rangle [?h = 0; v := -cv] \quad \varphi$$

$$\land\text{r} \quad \psi \land \varphi, s{\geq}0, \langle h := ..(s)\rangle h \geq 0 \vdash \langle h := ..(s)\rangle ([?h > 0] \quad \varphi \land [?h = 0; v := -cv] \quad \varphi)$$

$$[\cup] \quad \psi \land \varphi, s{\geq}0, \langle h := ..(s)\rangle h \geq 0 \vdash \langle h := ..(s)\rangle [?h > 0 \cup (?h = 0; v := -cv)] \quad \varphi$$

$$\to\text{r} \quad \psi \land \varphi, s{\geq}0 \vdash \langle h := ..(s)\rangle h \geq 0 \to \langle h := ..(s)\rangle [?h > 0 \cup (?h = 0; v := -cv)] \quad \varphi$$

$$\to\text{r} \quad \psi \land \varphi \vdash s{\geq}0 \to (\langle h := ..(s)\rangle h \geq 0 \to \langle h := ..(s)\rangle [?h > 0 \cup (?h = 0; v := -cv)] \quad \varphi)$$

$$\forall\text{r} \quad \psi \land \varphi \vdash \forall t{\geq}0\, (\langle h := ..(t)\rangle h \geq 0 \to \langle h := ..(t)\rangle [?h > 0 \cup (?h = 0; v := -cv)] \quad \varphi)$$

$$['] \quad \psi \land \varphi \vdash [h'' = -g \,\&\, h \geq 0][?h > 0 \cup (?h = 0; v := -cv)] \quad \varphi$$

$$[;] \quad \psi \land \varphi \vdash [h'' = -g \,\&\, h \geq 0; (?h > 0 \cup (?h = 0; v := -cv))] \quad \varphi$$

$$\mathit{ind}' \quad \psi \land \varphi \vdash [(h'' = -g \,\&\, h \geq 0; (?h > 0 \cup (?h = 0; v := -cv)))^*](0{\leq}h{\leq}H)$$

$$\to\text{r} \quad \vdash \psi \land \varphi \to [(h'' = -g \,\&\, h \geq 0; (?h > 0 \cup (?h = 0; v := -cv)))^*](0{\leq}h{\leq}H)$$

Figure 4: Bouncing ball proof (with evolution domain)

the subsequent tests $?h = 0$ and $?h > 0$. A state with negative height fails both tests. While this behaviour does not give a successful program transition of $(\nu, \omega) \in \rho(ball)$ by Lecture 3 so that the proof in Fig. 3 is correct, the behaviour still gives a valid trace $\sigma \in \tau(ball)$ by Def. **??**. This trace σ is a partial trace, because it ends in a failure state Λ, but it is still one of the traces that $[ball]\Box(0 \leq h \leq H)$ quantifies over (quite unlike $[ball](0 \leq h \leq H)$, which only considers final states of successful traces).

5 Summary

This lecture showed a systematic way of specifying and verifying temporal properties of hybrid systems. The focus was on safety properties that hold always throughout the evolution of the system and are specified as $[\alpha]\Box\phi$ with a mix of a temporal and a dynamic modality instead of just a dynamic modality as in $[\alpha]\phi$. The difference is that $[\alpha]\Box\phi$ includes that safety condition ϕ holds at all intermediate states during all traces of α, whereas $[\alpha]\phi$ only specifies that ϕ holds at the end of each trace of α. This difference matters in systems that have more intermediate states than final states. The difference is insignificant for systems that can "stop anytime", because those will already include all intermediate states of longer system runs as the final state of a corresponding shorter system run. This has been the case in almost all systems studied in this course and is frequently the case in practice.

The systematic way of ensuring safety always throughout the execution of hybrid systems is the use of the dynamic and temporal modality $[\alpha]\Box\phi$, which works whether or not the system has the special structure that allows it to stop anytime. In a nutshell, the temporal proof rules for $[\alpha]\Box\phi$ properties lead to additional branches that correspond to the safety conditions at the respective intermediate state. It can be shown that temporal dTL properties reduce to nontemporal d$\mathcal{L}$ properties completely [Pla10, Chapter 4], justifying the intimate relation of temporal and nontemporal properties That completeness result made crucial use of the clever form of the [*]□ proof rule.

Other temporal modalities are more complicated but can either be handled directly (in the case of $\langle\alpha\rangle\Diamond\phi$) or by transformation [Pla10].

Exercises

Exercise 1. Can you give a formula of the following form that is valid?

$$[\alpha]\Box\phi \land \neg[\alpha]\phi$$

Exercise 2. In which case does the temporal $[\alpha]\Box\phi$ differ from the nontemporal $[\alpha]\phi$.

Exercise 3. Can you give a temporal box version of the differential invariant proof rule?

References

[Pla07] André Platzer. A temporal dynamic logic for verifying hybrid system invariants. In Sergei N. Artëmov and Anil Nerode, editors, *LFCS*, volume 4514 of *LNCS*, pages 457–471. Springer, 2007. doi:10.1007/978-3-540-72734-7_32.

[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.

[Pla12] André Platzer. Logics of dynamical systems. In *LICS*, pages 13–24. IEEE, 2012. doi:10.1109/LICS.2012.13.