

Real-Time Systems
Lecture 03: Duration Calculus I
 2013-04-23
 Dr. Bernd Westphal
 Albert-Ludwigs-Universität Freiburg, Germany

Contents & Goals

- Last Lecture:**
- Model of timed behaviour: state variables and their interpretation
 - First order predicate-logic for requirements and system properties

This Lecture:

- **Educational Objectives:** Capabilities for following tasks/questions:
 - Read (and at best also write) Duration Calculus formulae.
- **Content:**
 - Classes of requirements (safety, liveness, etc.)
 - Duration Calculus: Assertions, Terms, Formulae, Abbreviations, Examples

Recall: Correctness

Recall: Correctness

- Let 'Req' be a requirement.
- 'Des' be a design, and
- 'Impl' be an **implementation**.

Recall: each is a set of evolutions, i.e. a subset of $(Time \rightarrow \mathbb{R}^n, P(obs))$, described in any form.

We say

- 'Des' is a **correct design** (wrt. 'Req') if and only if $Des \sqsubseteq Req$.
- 'Impl' is a **correct implementation** (wrt. 'Des' (or 'Req')) if and only if $Impl \sqsubseteq Des$ (or $Impl \sqsubseteq Req$)

If 'Req' and 'Des' are described by formulae of first-order predicate logic, proving the design correct amounts to proving that $Des \implies Req$ is valid.

Classes of Timed Properties

Safety Properties

- A **safety property** states that **something bad** must **never** happen [Lampert].
 $\langle \exists t(t) \neg B(t) \rangle$
- Example: train inside level crossing with gates open.
- More general, assume observable $C : Time \rightarrow \{0, 1\}$ where $C(t) = 1$ represents a critical system state at time t .
 $\forall t \in Time \bullet \neg C(t)$

$\forall x \in N : x \geq 0$
 $\forall x \in N : x \geq 0$
 $\forall x \in N : x \geq 0$

- In general, a safety property is characterised as a property that can be **fastified** in bounded time.
- But safety is not everything...

Liveness Properties

- The simplest form of a **liveness property** states that **something good eventually does happen**.
- Example: gates open for road traffic
- More general, assume observable $G : \text{Time} \rightarrow \{0, 1\}$ where $G(t) = 1$ represents a good system state at time t .
- Then

$$\exists t \in \text{Time} \bullet G(t)$$
- is a liveness property
- Note: not falsified in finite time.
- With real-time, liveness is too weak...

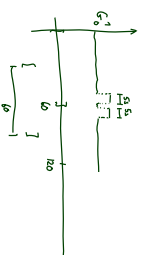
Bounded Response Properties

- A **bounded response property** states that the desired reaction on an input occurs in time interval $[b, c]$.
- Example: from request to secure level crossing to gates closed.
- More general, re-consider good thing $G : \text{Time} \rightarrow \{0, 1\}$ and request $R : \text{Time} \rightarrow \{0, 1\}$.
- Then

$$\forall t_1 \in \text{Time} \bullet (R(t_1) \implies \exists t_2 \in [t_1 + b, t_1 + b + c] \bullet G(t_2))$$
- is a bounded liveness property.
- This property can again be falsified in finite time.
- With gas burners, this is still not everything...

Duration Properties

- A **duration property** states that for observation interval $[b, c]$ the accumulated time in which the system is in a certain critical state has an upper bound $w(b, c)$.
- Example: leakage in gas burner.



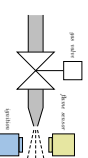
Duration Properties

- A **duration property** states that for observation interval $[b, c]$ characterised by a condition $A(b, c)$ the accumulated time in which the system is in a certain critical state has an upper bound $w(b, c)$.
- Example: leakage in gas burner. *Klassenbeispiel*
- More general, re-consider critical thing $C : \text{Time} \rightarrow \{0, 1\}$.
Then

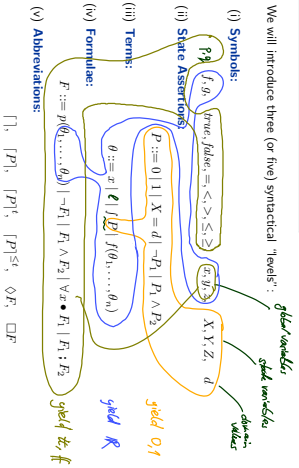
$$\forall b, c \in \text{Time} \bullet (A(b, c) \implies \int_b^c C(t) dt \leq w(b, c))$$
- is a duration property.
- This property can again be falsified in finite time.

Duration Calculus

- Duration Calculus is an **interval logic**.
- Formulae are evaluated in an (implicitly given) interval.
- Back to our gas burner:
 - $G, F, I, H : \text{Time} \rightarrow \{0, 1\}$
 - Define $L : \text{Time} \rightarrow \{0, 1\}$ as $G \wedge \neg F$.
- Strangest operators:
 - **everywhere** — Example: $[F]$ (holds in a given interval $[b, c]$ iff the gas valve is open almost everywhere.)
 - **chop** — Example: $(\neg I) \# [I] \# (\neg I) \implies L \geq 1$ (ignition phases last at least one time unit)
 - **integral** — Example: $L \geq 60 \implies \int L \leq \frac{L}{50}$ (At most 5% leakage time within intervals of at least 60 time units.)



We will introduce three (or five) syntactical 'levels':



- f, g : function symbols, each with arity $n \in \mathbb{N}_0$. Called constant if $n = 0$. Assume: constants $0, 1, \dots \in \mathbb{N}$; binary $+$, $-$, \cdot , $/$; unary symbols $!$, $\sqrt{\quad}$.
- p, q : predicate symbols, also with arity. Assume: constants *true*, *false*; binary $=, <, >, <=, >=$.
- $x, y, z \in \text{CVar}$: global variables.
- $X, Y, Z \in \text{Obs}$: state variables or observables, each of a data type D (or $\mathcal{D}(X), \mathcal{D}(Y), \mathcal{D}(Z)$ to be precise). Called **boolean observable** if data type is $\{0, 1\}$.
- d : elements taken from data types D of observables.

- Semantical domains** are
 - the truth values $B = \{\text{tt}, \text{ff}\}$,
 - the real numbers \mathbb{R} ,
 - time: $\text{Time} = \mathbb{R}_+^c$ (continuous), exception $\text{Time} = \mathbb{N}_0$ (discrete time)
 - and data types D .
- The **semantics** of an n -ary function symbol f is a (mathematical) function from \mathbb{R}^n to \mathbb{R} , denoted f , i.e.

$$f : \mathbb{R}^n \rightarrow \mathbb{R}.$$
- The semantics of an n -ary predicate symbol p is a function from \mathbb{R}^n to B , denoted p , i.e.

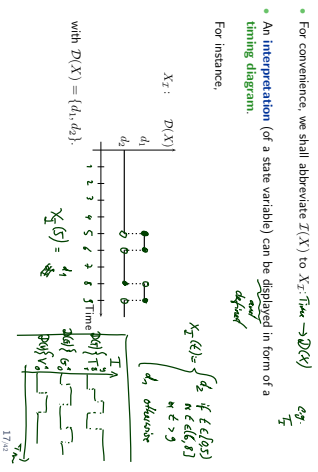
$$p : \mathbb{R}^n \rightarrow B.$$
- For constants (arity $n = 0$) we have $f \in \mathbb{R}$ and $p \in B$.

- The semantics of the function and predicate symbols assumed above is fixed throughout the lecture:
 - $\text{true} = \text{tt}, \text{false} = \text{ff}$
 - $0 \in \mathbb{R}$ is the (real) number zero, etc.
 - $+$: $\mathbb{R}^2 \rightarrow \mathbb{R}$ is the addition of real numbers, etc.
 - $=$: $\mathbb{R}^2 \rightarrow B$ is the equality relation on real numbers.
 - $<$: $\mathbb{R}^2 \rightarrow B$ is the less-than relation on real numbers, etc.
- Since the semantics is the expected one, we shall often simply use the symbols $0, +, =, <$ when we mean their semantics $0, 1, +, =, <$.

- The semantics of a **global variable** is not fixed (throughout the lecture) but given by a **valuation**, i.e. a mapping

$$V : \text{CVar} \rightarrow \mathbb{R}$$
 assigning each global variable $x \in \text{CVar}$ a real number $V(x) \in \mathbb{R}$. We use Val to denote the set of all valuations, i.e. $\text{Val} = (\text{CVar} \rightarrow \mathbb{R})$. Global variables are thought **fixed over time** in system evolutions.
- The semantics of a **state variable** is **time-dependent**. It is given by an interpretation I , i.e. a mapping

$$I : \text{Obs} \rightarrow (\text{Time} \rightarrow D)$$
 assigning each state variable $X \in \text{Obs}$ a function $I(X) : \text{Time} \rightarrow D(X)$ such that $I(X)(t) \in D(X)$ denotes the value that X has at time $t \in \text{Time}$.



Duration Calculus: Overview

We will introduce three (or five) syntactical 'levels':

- (i) **Symbols:**
 $f, g, true, false; =, <, >, \leq, \geq; x, y, z; X, Y, Z; d$
- (ii) **State Assertions:**
 $P ::= 0 \mid 1 \mid X = d \mid \neg P_1 \mid P_1 \wedge P_2$
- (iii) **Terms:**
 $\theta ::= x \mid \ell \mid P \mid f(\theta_1, \dots, \theta_n)$
- (iv) **Formulae:**
 $F ::= p(\theta_1, \dots, \theta_n) \mid \neg F_1 \mid F_1 \wedge F_2 \mid \forall x \bullet F_1 \mid F_1 ; F_2$
- (v) **Abbreviations:**
 $\lceil \cdot \rceil, \lceil P \rceil, \lceil P \rceil^c, \lceil P \rceil^{\leq}, \text{of}, \square P$

State Assertions: Syntax

The set of **state assertions** is defined by the following grammar:

- with $d \in \mathcal{D}(X)$,
 $P ::= 0 \mid 1 \mid X = d \mid \neg P_1 \mid P_1 \wedge P_2$
(ℓ , R)
- We shall use P, Q, R to denote state assertions.
 $\lceil X=d \rceil, X^c, X \leq d$
- Abbreviations:**
 - We shall write X instead of $X = 1$ if $\mathcal{D}(X) = \{1\}$.
 - Define $\forall, \Rightarrow, \Leftarrow$ as usual.

State Assertions: Semantics

Give an evaluation ν .
 The semantics of state assertion P is a function

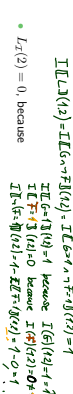
- $\llbracket P \rrbracket : \text{Time} \rightarrow \{0, 1\}$
 i.e. $\llbracket P \rrbracket(t)$ denotes the truth value of P at time $t \in \text{Time}$.
- The value is defined **inductively** on the structure of P :
 $\llbracket 0 \rrbracket(t) = 0 \in \mathcal{R}, \quad \llbracket 1 \rrbracket(t) = 1$
 $\llbracket X=d \rrbracket(t) = \begin{cases} 1, & \text{if } \nu(X)(t) = d \\ 0, & \text{otherwise} \end{cases}$
 $\llbracket \neg P_1 \rrbracket(t) = 1 - \llbracket P_1 \rrbracket(t)$
 $\llbracket P_1 \wedge P_2 \rrbracket(t) = \begin{cases} 1, & \text{if } \llbracket P_1 \rrbracket(t) = \llbracket P_2 \rrbracket(t) = 1 \\ 0, & \text{otherwise} \end{cases}$

State Assertions: Notes

- $\llbracket X \rrbracket(t) = \llbracket X \rrbracket(t) = \llbracket X \rrbracket(t) = X(t)$, if X boolean, i.e. $\mathcal{D}(X) = \{0, 1\}$
- $\llbracket P \rrbracket$ is also called **interpretation** of P .
- We shall write P_x for it.
- Here we prefer 0 and 1 as boolean values (instead of tt and ff) — for reasons that will become clear immediately.

State Assertions: Example

- Boolean observables G and F
- State assertion $L := (G \wedge \neg F)$ **shd** **variable** τ, c



References

References

[Olderog and Dierks, 2008] Olderog, E.-R. and Dierks, H. (2008). *Real-Time Systems - Formal Specification and Automatic Verification*. Cambridge University Press.