Real-Time Systems

Lecture 8: DC Properties II

2014-06-05

Dr. Bernd Westphal

Albert-Ludwigs-Universität Freiburg, Germany

Contents & Goals

Last Lecture:

- DC Implementables

This Lecture:

- **Educational Objectives:** Capabilities for following tasks/questions.
  - Facts: (un)decidability properties of DC in discrete/continuous time.
  - What's the idea of the considered (un)decidability proofs?

- **Content:**
  - DC Implementables Cont'd
  - RDC in discrete time
  - Satisfiability and realisability from 0 is decidable for RDC in discrete time
  - Undecidable problems of DC in continuous time

DC Implementables Cont'd

Recall: DC Implementables

- DC Implementables
  are special patterns of DC Standard Forms (due to A.P. Ravn).
- Within one pattern,
  - $\pi, \pi_1, \ldots, \pi_n$, $n \geq 0$, denote **phases** of **the same** state variable X_i,
  - φ denotes a state assertion not depending on X_i.
- θ denotes a **rigid** term.
- **Initialisation**:

$$\lceil\rceil \vee \lceil \pi \rceil \, ; \, true$$

- **Sequencing**:

$$\lceil \pi \rceil \longrightarrow \lceil \pi \vee \pi_1 \vee \cdots \vee \pi_n \rceil$$

- **Progress**:

$$\lceil \pi \rceil \xrightarrow{\theta} \lceil \neg \pi \rceil$$

- **Synchronisation**:

$$\lceil \pi \wedge \varphi \rceil \xrightarrow{\theta} \lceil \neg \pi \rceil$$

Recall: DC Implementables Cont'd

- **Bounded Stability**:

$$\lceil \neg\pi \rceil \,;\, \lceil \pi \wedge \varphi \rceil \xrightarrow{\leq\theta} \lceil \pi \vee \pi_1 \vee \cdots \vee \pi_n \rceil$$

- **Unbounded Stability**:

$$\lceil \neg\pi \rceil \,;\, \lceil \pi \wedge \varphi \rceil \longrightarrow \lceil \pi \vee \pi_1 \vee \cdots \vee \pi_n \rceil$$

- **Bounded initial stability**:

$$\lceil \pi \wedge \varphi \rceil \xrightarrow{\leq\theta}_0 \lceil \pi \vee \pi_1 \vee \cdots \vee \pi_n \rceil$$

- **Unbounded initial stability**:

$$\lceil \pi \wedge \varphi \rceil \longrightarrow_0 \lceil \pi \vee \pi_1 \vee \cdots \vee \pi_n \rceil$$

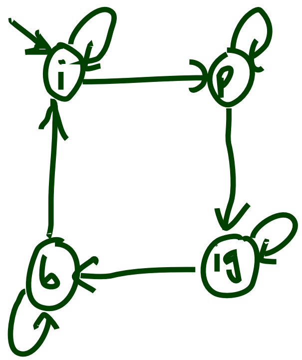
Recall: Control Automata

Model of Gas Burner controller as a system of four control automata:

- H : Boolean,
  representing **heat request**, (input)
- F : Boolean,
  representing **flame**, (input)
- C with $\mathcal{D}(C) = \{\text{idle}, \text{purge}, \text{ignite}, \text{burn}\}$,
  representing the **controller**, (local)
- G : Boolean,
  representing **gas valve**. (output)

Gas Burner Controller Specification

$\lceil\rceil \vee \lceil \mathsf{idle} \rceil \,;\, true, \quad \lceil\rceil \vee \lceil \neg H \rceil \,;\, true, \quad \lceil\rceil \vee \lceil \neg F \rceil \,;\, true, \quad \lceil\rceil \vee \lceil \neg G \rceil \,;\, true$ (Init-1 - 4)



$\lceil \mathsf{idle} \rceil \longrightarrow \lceil \mathsf{idle} \vee \mathsf{purge} \rceil$ (Seq-1)

$\lceil \mathsf{purge} \rceil \longrightarrow \lceil \mathsf{purge} \vee \mathsf{ignite} \rceil$ (Seq-2)

$\lceil \mathsf{ignite} \rceil \longrightarrow \lceil \mathsf{ignite} \vee \mathsf{burn} \rceil$ (Seq-3)

$\lceil \mathsf{burn} \rceil \longrightarrow \lceil \mathsf{burn} \vee \mathsf{idle} \rceil$ (Seq-4)

$\lceil \mathsf{purge} \rceil \xrightarrow{30+\varepsilon} \lceil \neg \mathsf{purge} \rceil$ (Prog-1)

$\lceil \mathsf{ignite} \rceil \xrightarrow{0.5+\varepsilon} \lceil \neg \mathsf{ignite} \rceil$ (Prog-2)

$\lceil \mathsf{idle} \wedge H \rceil \xrightarrow{\varepsilon} \lceil \neg \mathsf{idle} \rceil$! (Syn-1)

$\lceil \mathsf{burn} \wedge (\neg H \vee \neg F) \rceil \xrightarrow{\varepsilon} \lceil \neg \mathsf{burn} \rceil$ (Syn-2)

$\lceil G \wedge (\mathsf{idle} \vee \mathsf{purge}) \rceil \xrightarrow{\varepsilon} \lceil \neg G \rceil$ (Syn-3)

$\lceil \neg G \wedge (\mathsf{ignite} \vee \mathsf{burn}) \rceil \xrightarrow{\varepsilon} \lceil G \rceil$ (Syn-4)

$\lceil \neg \mathsf{idle} \rceil \,;\, \lceil \mathsf{idle} \wedge \neg H \rceil \longrightarrow \lceil \mathsf{idle} \rceil$! (Stab-1)

$\lceil \mathsf{idle} \wedge \neg H \rceil \longrightarrow_0 \lceil \mathsf{idle} \rceil$ (Stab-1-init)

$\lceil \neg \mathsf{purge} \rceil \,;\, \lceil \mathsf{purge} \rceil \xrightarrow{\leq 30} \lceil \mathsf{purge} \rceil$ (Stab-2)

$\lceil \neg \mathsf{ignite} \rceil \,;\, \lceil \mathsf{ignite} \rceil \xrightarrow{\leq 0.5} \lceil \mathsf{ignite} \rceil$ (Stab-3)

$\lceil \neg \mathsf{burn} \rceil \,;\, \lceil \mathsf{burn} \wedge H \wedge F \rceil \longrightarrow \lceil \mathsf{burn} \rceil$ (Stab-4)

$\lceil F \rceil \,;\, \lceil \neg F \wedge \neg \mathsf{ignite} \rceil \longrightarrow \lceil \neg F \rceil$ (Stab-5)

$\lceil \neg F \wedge \neg \mathsf{ignite} \rceil \longrightarrow_0 \lceil \neg F \rceil$ (Stab-5-init)

$\lceil G \rceil \,;\, \lceil \neg G \wedge (\mathsf{idle} \vee \mathsf{purge}) \rceil \longrightarrow \lceil \neg G \rceil$ (Stab-6)

$\lceil \neg G \wedge (\mathsf{idle} \vee \mathsf{purge}) \rceil \longrightarrow_0 \lceil \neg G \rceil$ (Stab-6-init)

$\lceil \neg G \rceil \,;\, \lceil G \wedge (\mathsf{ignite} \vee \mathsf{burn}) \rceil \longrightarrow \lceil G \rceil$ (Stab-7)

Gas Burner Controller Correctness Proof

$$\mathsf{GB\text{-}Ctrl} := \mathsf{Init\text{-}1} \wedge \cdots \wedge \mathsf{Stab\text{-}7} \wedge \varepsilon > 0$$

Recall:

$$\mathsf{Req} :\iff \Box(\ell \geq 60 \implies 20 \cdot \textstyle\int L \leq \ell)$$

and (cf. [Olderog and Dierks, 2008])

$$\models \mathsf{Req\text{-}1} \implies \mathsf{Req}$$

for the **simplified**

$$\mathsf{Req\text{-}1} := \Box(\ell \leq 30 \implies \textstyle\int L \leq 1).$$

Here we show

$$\models \mathsf{GB\text{-}Ctrl} \wedge A(\varepsilon) \implies \mathsf{Req\text{-}1}.$$

Lemma 3.15

$$\models \text{GB-Ctrl} \implies \Box \left(\begin{array}{rl} & (\lceil \mathsf{idle} \rceil \implies \int G \leq \varepsilon) \\ \wedge & (\lceil \mathsf{purge} \rceil \implies \int G \leq \varepsilon) \\ \wedge & (\lceil \mathsf{ignite} \rceil \implies \ell \leq 0.5 + \varepsilon) \\ \wedge & (\lceil \mathsf{burn} \rceil \implies \int \neg F \leq 2\varepsilon) \end{array} \right) \; (*)$$

Proof: Let $\mathcal{I}$ be an interpretation, $\mathcal{V}$ a valuation, and $[c, d]$ an interval with $\mathcal{I}, \mathcal{V}, [c, d] \models$ GB-Ctrl. $\overbrace{\text{Let } [b, e] \subseteq [c, d]}^{\text{cf. } \Box}$.

- Case 1: $\mathcal{I}, \mathcal{V}, [b, e] \models \lceil \mathsf{idle} \rceil$

$$\lceil G \wedge (\mathsf{idle} \vee \mathsf{purge}) \rceil \xrightarrow{\varepsilon} \lceil \neg G \rceil \qquad \text{(Syn-3)}$$

conclude

$$\lceil G \rceil \,;\, \lceil \neg G \wedge (\mathsf{idle} \vee \mathsf{purge}) \rceil \longrightarrow \lceil \neg G \rceil \qquad \text{(Stab-6)}$$

$$\mathcal{I}, \mathcal{V}, [b, e] \models \Box(\lceil G \rceil \implies \ell \leq \varepsilon) \wedge \underbrace{\neg \Diamond (\lceil G \rceil \,;\, \lceil \neg G \rceil \,;\, \lceil G \rceil)}_{\text{gas valve doesn't open up again in idle phase}}$$

$(*)$

- Case 2: $\mathcal{I}, \mathcal{V}, [b, e] \models \lceil \mathsf{purge} \rceil$ Analogously to case 1.

Lemma 3.15 Cont'd

$$
\begin{aligned}
(\lceil \mathsf{idle} \rceil &\implies \textstyle\int G \leq \varepsilon) \\
(\lceil \mathsf{purge} \rceil &\implies \textstyle\int G \leq \varepsilon) \\
(\lceil \mathsf{ignite} \rceil &\implies \ell \leq 0.5 + \varepsilon) \\
(\lceil \mathsf{burn} \rceil &\implies \textstyle\int \neg F \leq 2\varepsilon)
\end{aligned}
$$

- Case 3: $\mathcal{I}, \mathcal{V}, [b, e] \models \lceil \mathsf{ignite} \rceil$

$$\lceil \mathsf{ignite} \rceil \xrightarrow{0.5+\varepsilon} \lceil \neg \mathsf{ignite} \rceil \qquad \text{(Prog-2)}$$

$$\mathcal{I}, \mathcal{V}, [b, e] \models \ell \leq 0.5 + \varepsilon$$

$\lceil\,\rceil$

$\lceil \neg F \rceil$

$\lceil F \rceil$

$\lceil F \rceil ; \lceil \neg F \rceil$

$\lceil \neg F \rceil ; \lceil F \rceil$

$\lceil \neg F \rceil ; \lceil F \rceil ; \lceil \neg F \rceil$

- Case 4: $\mathcal{I}, \mathcal{V}, [b, e] \models \lceil \mathsf{burn} \rceil$

$$\lceil \mathsf{burn} \wedge (\neg H \vee \neg F) \rceil \xrightarrow{\varepsilon} \lceil \neg \mathsf{burn} \rceil \qquad \text{(Syn-2)}$$

$$\lceil F \rceil \,;\, \lceil \neg F \wedge \neg \mathsf{ignite} \rceil \longrightarrow \lceil \neg F \rceil \qquad \text{(Stab-5)}$$

$$\mathcal{I}, \mathcal{V}, [b, e] \models \Box(\lceil \neg F \rceil \implies \ell \leq \varepsilon) \wedge \neg \Diamond(\lceil F \rceil \,;\, \lceil \neg F \rceil \,;\, \lceil F \rceil)$$

$(*)$

Lemma 3.16

$$\models \exists \varepsilon \bullet \text{GB-Ctrl} \implies \underbrace{\Box(\ell \leq 30 \implies \textstyle\int L \leq 1)}_{\text{Req-1}}$$

Proof Sketch

Choose $\mathcal{I}, \mathcal{V}, [b,e]$ s.t. $\mathcal{I}, \mathcal{V}, [b,e] \models \text{GB-Ctrl} \wedge \ell \leq 30$.

Distinguish 5 cases:

$$
\begin{aligned}
\mathcal{I}, \mathcal{V}, [b,e] \models\ & \lceil\,\rceil & (0)\\
& \vee (\lceil idle \rceil ; true \wedge \ell \leq 30) & (1)\\
& \vee (\lceil purge \rceil ; true \wedge \ell \leq 30) & (2)\\
& \vee (\lceil ignite \rceil ; true \wedge \ell \leq 30) & (3)\\
& \vee (\lceil burn \rceil ; true \wedge \ell \leq 30) & (4)
\end{aligned}
$$

Lemma 3.16 Cont'd

- Case 0: $\mathcal{I}, \mathcal{V}, [b, e] \models \lceil\rceil$ ✓

- Case 1: $\mathcal{I}, \mathcal{V}, [b, e] \models \lceil \mathsf{idle} \rceil \,;\, \mathit{true} \wedge \ell \leq 30$

$$\lceil \mathsf{idle} \rceil \longrightarrow \lceil \mathsf{idle} \vee \mathsf{purge} \rceil \qquad \text{(Seq-1)}$$

$$\lceil \neg \mathsf{purge} \rceil \,;\, \lceil \mathsf{purge} \rceil \xrightarrow{\leq 30} \lceil \mathsf{purge} \rceil \qquad \text{(Stab-2)}$$

$\leadsto \mathcal{I}, \mathcal{V}, [b,e] \models \lceil idle \rceil \vee \lceil idle \rceil ; \lceil purge \rceil$

3.15 $\leadsto \mathcal{I}, \mathcal{V}, [b,e] \models \int L \leq \varepsilon \vee \int L \leq \varepsilon ; \int L \leq \varepsilon$

$\leadsto \mathcal{I}, \mathcal{V}, [b,e] \models \int L \leq 2\varepsilon$

Thus $\boxed{\varepsilon \leq 0.5}$ is sufficient for Req-1 in this case.

Lemma 3.16 Cont'd

- Case 2: $\mathcal{I}, \mathcal{V}, [b,e] \models \lceil \mathsf{burn} \rceil \,;\, true \wedge \ell \leq 30$

$$\lceil \mathsf{burn} \rceil \longrightarrow \lceil \mathsf{burn} \vee \mathsf{idle} \rceil \qquad \text{(Seq-4)}$$

$\Rightarrow \mathcal{I}, \mathcal{V}, [b,e] \models (\lceil burn \rceil \vee \lceil burn \rceil ; \underbrace{\lceil idle \rceil ; true}_{(1)}) \wedge \ell \leq 30$

3.15, (1) $\Rightarrow \mathcal{I}, \mathcal{V}, [b,e] \models (\int L \leq 2\varepsilon \vee \int L \leq 2\varepsilon ; \int L \leq 2\varepsilon) \wedge \ell \leq 30$

$\Rightarrow \mathcal{I}, \mathcal{V}, [b,e] \models \int L \leq 4\varepsilon$

Thus $\boxed{\varepsilon \leq 0.25}$ sufficient for Req-1 in this case.

Lemma 3.16 Cont'd

- Case 3: $\mathcal{I}, \mathcal{V}, [b, e] \models \lceil \mathsf{ignite} \rceil \, ; \, true \wedge \ell \leq 30$

$$\lceil \mathsf{ignite} \rceil \longrightarrow \lceil \mathsf{ignite} \vee \mathsf{burn} \rceil \qquad \text{(Seq-3)}$$

$$\mathcal{I}, \mathcal{V}, [b,e] \models (\lceil ignite \rceil \vee (\lceil ignite \rceil ; \underbrace{\lceil burn \rceil ; true}_{(2)})) \wedge \ell \leq 30$$

3.15 (2)
$$\mathcal{I}, \mathcal{V}, [b,e] \models (\int L \leq 0.5 + \varepsilon \vee \int L \leq 0.5 + \varepsilon \, ; \int L \leq 4\varepsilon) \wedge \ell \leq 30$$

$$\mathcal{I}, \mathcal{V}, [b,e] \models \int L \leq 0.5 + 5\varepsilon$$

So $\boxed{\varepsilon \leq 0.1}$ sufficient in this case.

Lemma 3.16 Cont'd

- Case 4: $\mathcal{I}, \mathcal{V}, [b, e] \models \lceil \text{purge} \rceil \, ; \, true \wedge \ell \leq 30$

$$\lceil \text{purge} \rceil \longrightarrow \lceil \text{purge} \vee \text{ignite} \rceil \qquad \text{(Seq-2)}$$

3.15
(3)

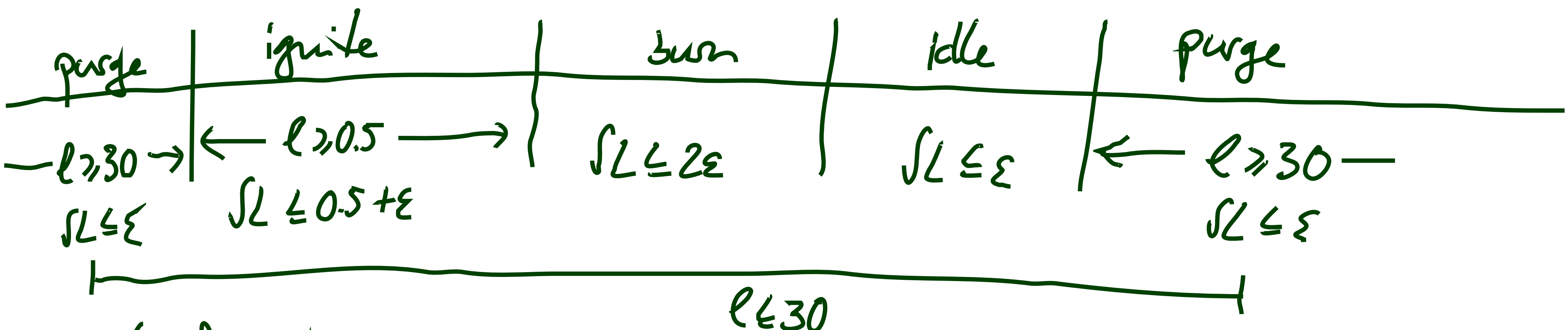
$\mathcal{I}, \mathcal{V}, [b,e] \models \int L \leq 0.5 + 6\varepsilon$

Thus $\boxed{\varepsilon \leq \frac{1}{12}}$ is sufficient for Req-1 in this case.

Correctness Result

Theorem 3.17.

$$\models \left(\text{GB-Ctrl} \wedge \varepsilon \leq \frac{1}{12} \right) \implies \text{Req}$$



$\hookrightarrow \int L \leq 0.5 + 6\varepsilon$

$\hookrightarrow A(\varepsilon) := \varepsilon \leq \frac{1}{12}$

Discussion

- We used only

  ‘Seq-1’, ‘Seq-2’, ‘Seq-3’, ‘Seq-4’,
  ‘Prog-2’, ‘Syn-2’, ‘Syn-3’,
  ‘Stab-2’, ‘Stab-5’, ‘Stab-6’.

  What about

  $$\text{Prog-1} = \lceil \text{purge} \rceil \xrightarrow{30+\varepsilon} \lceil \neg\text{purge} \rceil$$

  for instance?

Naja, there is the requirement (not noted down)
that the system does something finally,
e.g. get the heating going on request.

RDC in Discrete Time Cont'd

Restricted DC (RDC)

$$F ::= \lceil P \rceil \mid \neg F_1 \mid F_1 \vee F_2 \mid F_1 \,;\, F_2$$

where P is a state assertion, but with **boolean** observables **only**.

Note:

- No global variables, thus don't need $\mathcal{V}$.
- chop is there
- no $\int$, no ℓ (in general)
- no predicates, no function symbols (in general)
- $\Diamond F$ ...?
- $\lceil \rceil$ ...?

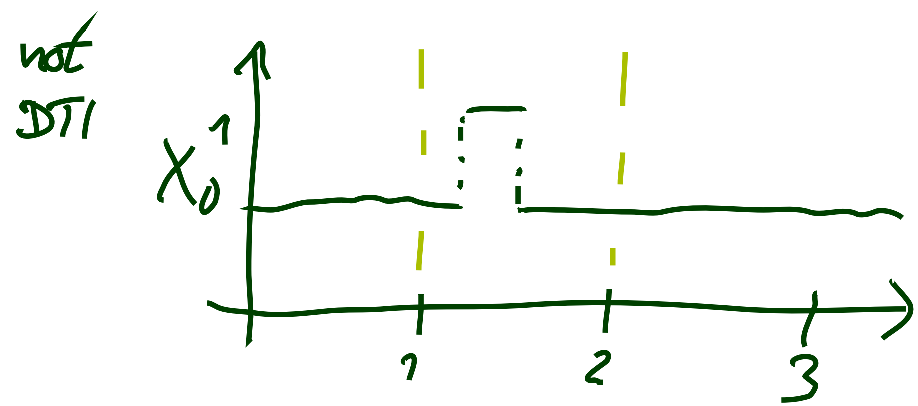
Discrete Time Interpretations

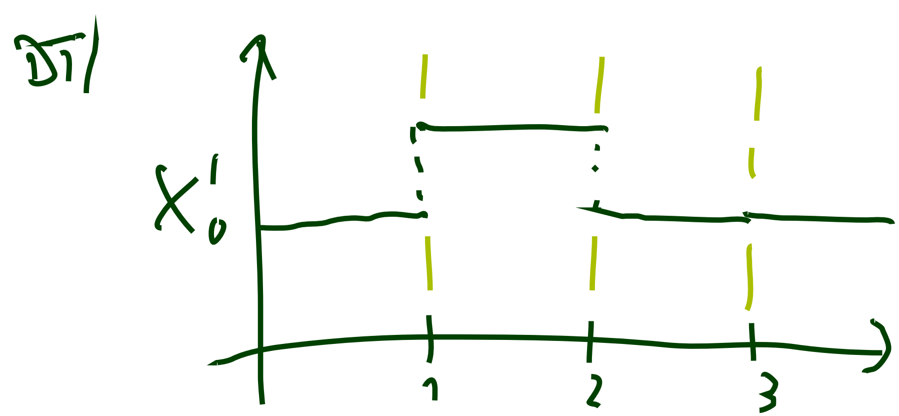
- An interpretation $\mathcal{I}$ is called **discrete time interpretation** if and only if, for each state variable X,

$$X_{\mathcal{I}} : \mathsf{Time} \to \mathcal{D}(X)$$

with

- $\mathsf{Time} = \mathbb{R}_0^+$,
- all discontinuities are in $\mathbb{N}_0$.





Discrete Time Interpretations

- An interpretation $\mathcal{I}$ is called **discrete time interpretation** if and only if, for each state variable X,

$$X_{\mathcal{I}} : \mathsf{Time} \to \mathcal{D}(X)$$

  with

  - $\mathsf{Time} = \mathbb{R}_0^+$,
  - all discontinuities are in $\mathbb{N}_0$.

- An interval $[b, e] \subset \mathsf{Intv}$ is called **discrete** if and only if $b, e \in \mathbb{N}_0$.

Discrete Time Interpretations

- An interpretation $\mathcal{I}$ is called **discrete time interpretation** if and only if, for each state variable X,

$$X_\mathcal{I} : \mathsf{Time} \to \mathcal{D}(X)$$

with

  - $\mathsf{Time} = \mathbb{R}_0^+$,
  - all discontinuities are in $\mathbb{N}_0$.

- We say $\mathcal{I}, [b,e] \models \lceil P \rceil$ if $\int_b^e P_\mathcal{I}(t)\,dt = (e-b) \wedge (e-b) > 0$

- An interval $[b,e] \subset \mathsf{Intv}$ is called **discrete** if and only if $b, e \in \mathbb{N}_0$.

- We say (for a discrete time interpretation $\mathcal{I}$ and a discrete interval $[b,e]$)

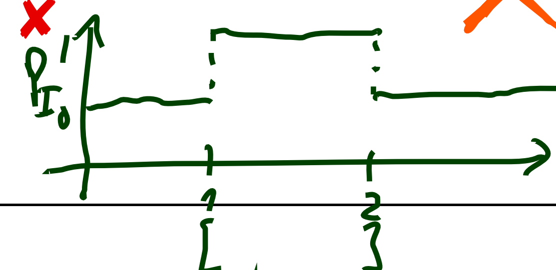
$$\mathcal{I}, [b,e] \models F_1 \,;\, F_2$$

if and only if there exists $m \in [b,e] \cap \mathbb{N}_0$ such that

$$\mathcal{I}, [b,m] \models F_1 \quad \text{and} \quad \mathcal{I}, [m,e] \models F_2$$

Differences between Continuous and Discrete Time

- Let P be a state assertion.

	Continuous Time	Discrete Time
$\models^? (\lceil P \rceil \,;\, \lceil P \rceil) \implies \lceil P \rceil$	✔ ✓	✔ ✓
$\models^? \lceil P \rceil \implies (\lceil P \rceil \,;\, \lceil P \rceil)$	✔ ✓	✘ ✗ 

$\lceil P \rceil$

only chop-point candidates are $m=1$ and $m=2$

but then $m-b=0$ or $e-m=0$

- In particular: $\ell = 1 :\iff (\lceil 1 \rceil \land \neg(\lceil 1 \rceil \,;\, \lceil 1 \rceil))$ (in discrete time).

Expressiveness of RDC

- $\ell = 1 \iff \lceil 1 \rceil \wedge \neg(\lceil 1 \rceil \,;\, \lceil 1 \rceil)$
- $\ell = 0 \iff \neg\lceil 1 \rceil$
- $true \iff \ell = 0 \vee \neg(\ell = 0)$
- $\int P = 0 \iff \lceil \neg P \rceil \vee \ell = 0$
- $\int P = 1 \iff (\int P = 0) \,;\, (\lceil P \rceil \wedge \ell = 1) \,;\, (\int P = 0)$
- $\int P = k + 1 \iff (\int P = k) \,;\, (\int P = 1)$
- $\int P \geq k \iff (\int P = k) \,;\, true$
- $\int P > k \iff \int P \geq k + 1$
- $\int P \leq k \iff \neg(\int P > k)$
- $\int P < k \iff \int P \leq k - 1$

where $k \in \mathbb{N}^{+}$.

so still

$\Diamond F := true \,;\, F \,;\, true$

in RDC

Decidability of Satisfiability/Realisability from 0

Theorem 3.6.
The satisfiability problem for RDC with discrete time is decidable.

Theorem 3.9.
The realisability problem for RDC with discrete time is decidable.

RDC formula $\mathcal{F}$.

$$
\begin{tikzcd}
\mathcal{F} \arrow[d, squiggly, "\text{construct}", "1"'] & \exists \arrow[d, Leftrightarrow, "5\ \text{prove}"] & \mathcal{I}\ \text{DTI} \\
\Sigma^* \supseteq \mathcal{L}(\mathcal{F}) & \ni & w \in \Sigma^* \arrow[u, squiggly, "\text{construct}\ 4"'] \\
\text{regular language} & 3 & \text{word} \\
 & & 2
\end{tikzcd}
$$

- $\mathcal{L}(\mathcal{F}) = \emptyset \Longrightarrow \mathcal{F}$ not SAT
- $\mathcal{L}(\mathcal{F}) = \emptyset$ is decidable

References

[Chaochen and Hansen, 2004] Chaochen, Z. and Hansen, M. R. (2004). *Duration Calculus: A Formal Approach to Real-Time Systems*. Monographs in Theoretical Computer Science. Springer-Verlag. An EATCS Series.

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