Real-Time Systems

Lecture 10: DC Properties IIb

2014-06-26

Dr. Bernd Westphal

Albert-Ludwigs-Universität Freiburg, Germany

Contents & Goals

Last Lecture:

- Satisfiability and realisability from 0 is decidable for RDC in discrete time
- Undecidable problems of DC in continuous time

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:**
  - Undecidable problems of DC in continuous time cont'd

(Variants of) RDC in Continuous Time

Sketch: Proof of Theorem 3.10

Reduce divergence of **two-counter machines** to realisability from 0:

- Given a two-counter machine $\mathcal{M}$ with final state q_{fin},
- construct a DC formula $F(\mathcal{M}) := \mathit{encoding}(\mathcal{M})$
- such that

$\mathcal{M}$ **diverges** **if and only if** the DC formula

$$F(\mathcal{M}) \wedge \neg\Diamond\lceil q_{\mathit{fin}} \rceil$$

is **realisable from 0**.

- If realisability from 0 was (semi-)decidable,
  divergence of two-counter machines would be (which it isn't).

Reducing Divergence to DC realisability: Idea

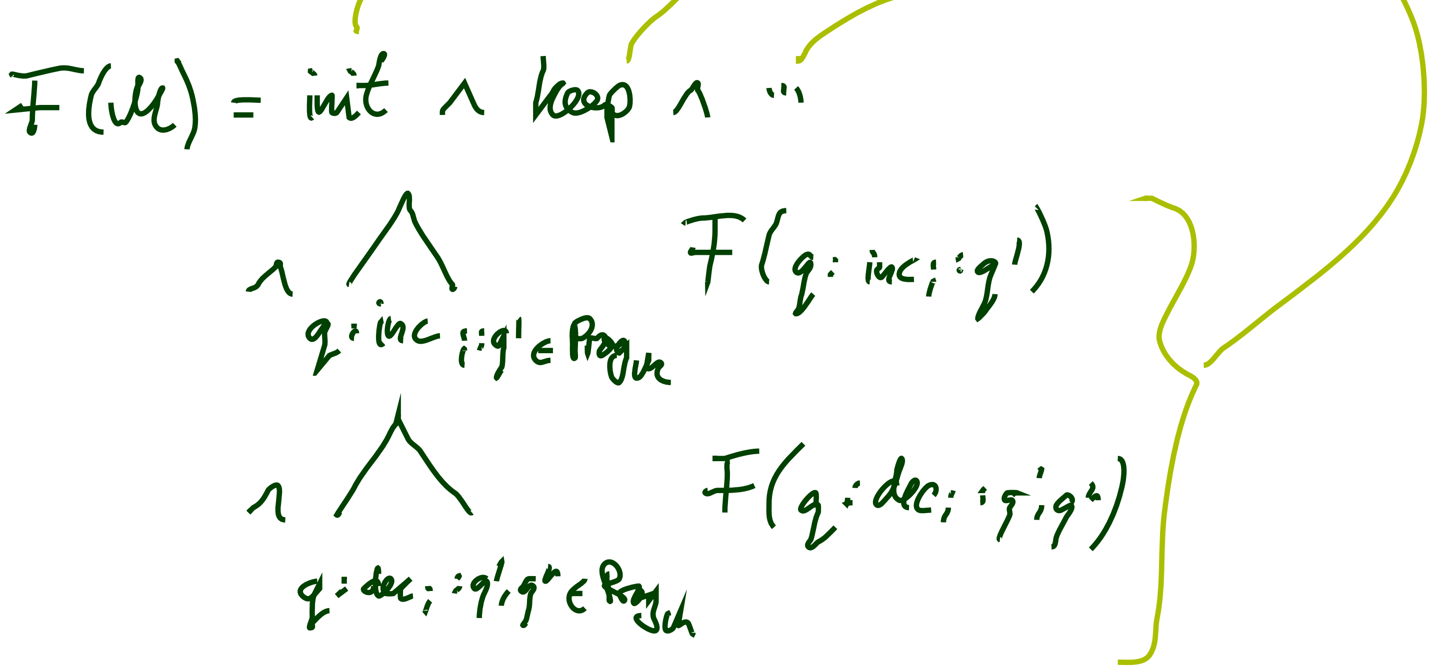
- A single configuration K of $\mathcal{M}$ can be encoded in an interval of length 4; being an encoding interval can be **characterised** by a DC formula.
- An interpretation on 'Time' encodes **the** computation of $\mathcal{M}$ if
  - each interval $[4n, 4(n+1)]$, $n \in \mathbb{N}_0$, **encodes** a configuration K_n,
  - each two subsequent intervals $[4n, 4(n+1)]$ and $[4(n+1), 4(n+2)]$, $n \in \mathbb{N}_0$, encode configurations $K_n \vdash K_{n+1}$ **in transition relation**.
- Being encoding of the run can be **characterised** by DC formula $F(\mathcal{M})$.
- Then $\mathcal{M}$ **diverges** if and only if $F(\mathcal{M}) \wedge \neg\Diamond\lceil q_{\mathit{fin}} \rceil$ is realisable from 0.

Construction of $F(\mathcal{M})$

In the following, we give DC formulae describing

- the initial configuration,
- the general form of configurations,
- the transitions between configurations,
- the handling of the final state.

$F(\mathcal{M})$ is the conjunction of all these formulae.

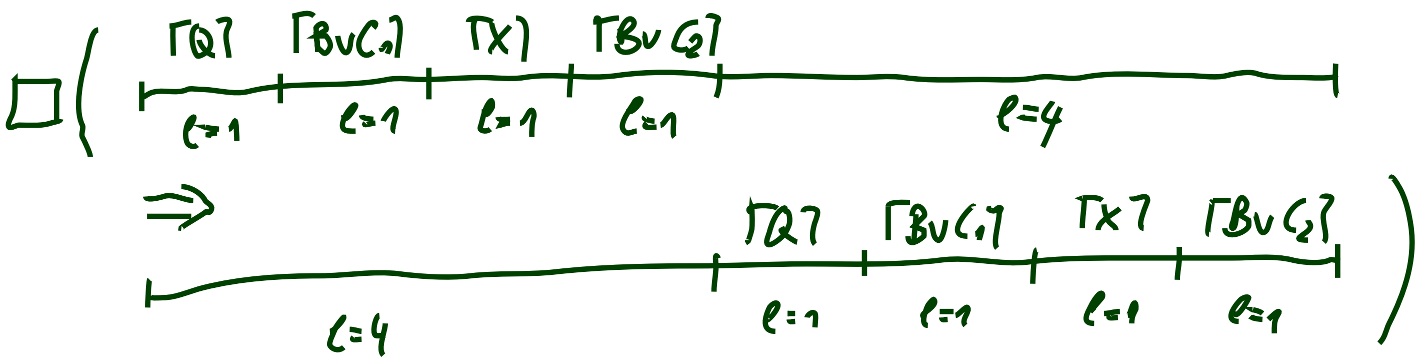


Initial and General Configurations

$$init :\iff (\ell \geq 4 \implies \lceil q_0 \rceil^1 \,;\, \lceil B \rceil^1 \,;\, \lceil X \rceil^1 \,;\, \lceil B \rceil^1 \,;\, true)$$

$$\begin{aligned} keep :\iff \Box(&\lceil Q \rceil^1 \,;\, \lceil B \vee C_1 \rceil^1 \,;\, \lceil X \rceil^1 \,;\, \lceil B \vee C_2 \rceil^1 \,;\, \ell = 4 \\ &\implies \ell = 4 \,;\, \lceil Q \rceil^1 \,;\, \lceil B \vee C_1 \rceil^1 \,;\, \lceil X \rceil^1 \,;\, \lceil B \vee C_2 \rceil^1) \end{aligned}$$

where $Q := \neg(X \vee C_1 \vee C_2 \vee B)$.



Auxiliary Formula Pattern copy

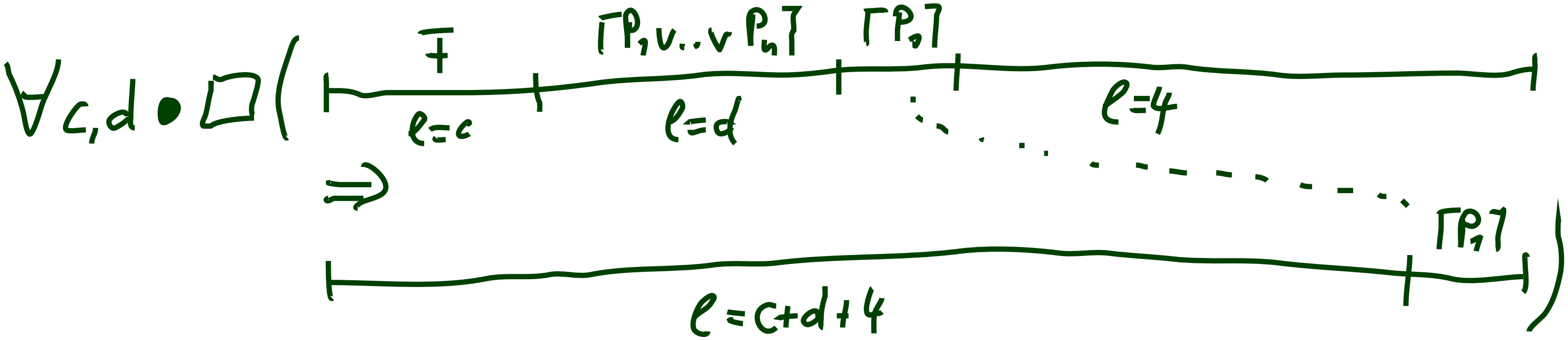
formula   state assertions

$$copy(F, \{P_1, \dots, P_n\}) :\iff$$

$$\forall\, c, d \bullet \Box((F \wedge \ell = c) \,;\, (\lceil P_1 \vee \dots \vee P_n \rceil \wedge \ell = d) \,;\, \lceil P_1 \rceil \,;\, \ell = 4$$
$$\implies \ell = c + d + 4 \,;\, \lceil P_1 \rceil$$

$$\dots$$

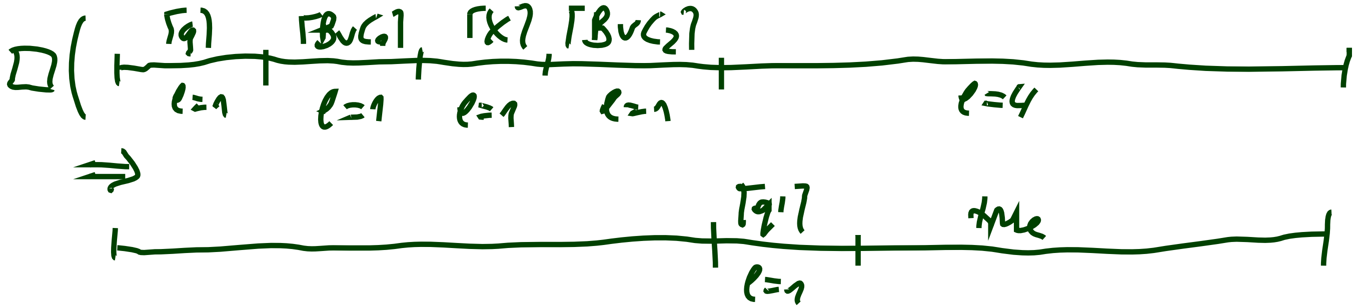
$$\forall\, c, d \bullet \Box((F \wedge \ell = c) \,;\, (\lceil P_1 \vee \dots \vee P_n \rceil \wedge \ell = d) \,;\, \lceil P_n \rceil \,;\, \ell = 4$$
$$\implies \ell = c + d + 4 \,;\, \lceil P_n \rceil$$



$q : inc_1 : q'$ *(Increment)*

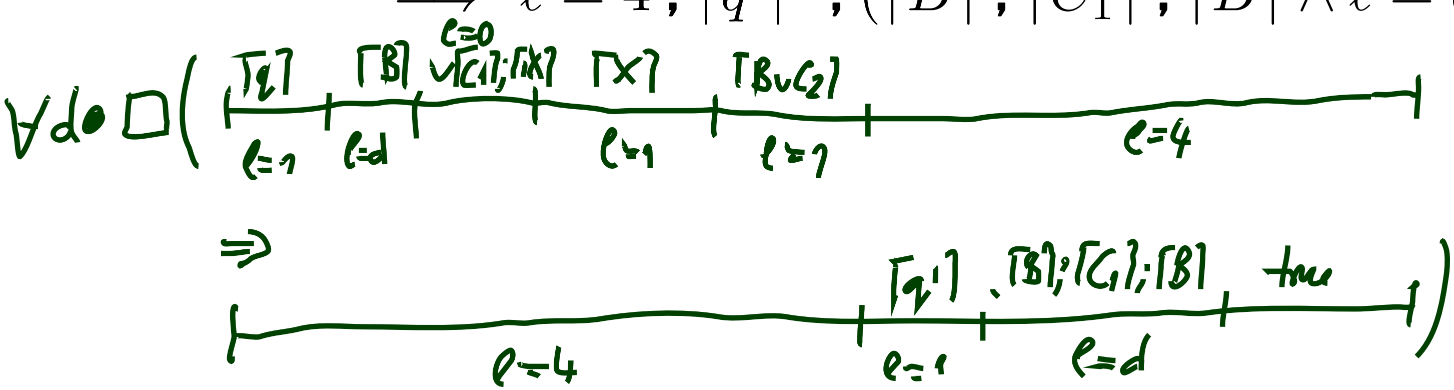
(i) Change state

$$\Box(\lceil q \rceil^1 ; \lceil B \vee C_1 \rceil^1 ; \lceil X \rceil^1 ; \lceil B \vee C_2 \rceil^1 ; \ell = 4 \implies \ell = 4 ; \lceil q' \rceil^1 ; \mathit{true})$$



(ii) Increment counter

$$\forall\, d \bullet \Box(\lceil q \rceil^1 ; \lceil B \rceil^d ; (\ell = 0 \vee \lceil C_1 \rceil ; \lceil \neg X \rceil) ; \lceil X \rceil^1 ; \lceil B \vee C_2 \rceil^1 ; \ell = 4$$
$$\implies \ell = 4 ; \lceil q' \rceil^1 ; (\lceil B \rceil ; \lceil C_1 \rceil ; \lceil B \rceil \wedge \ell = d) ; \mathit{true}$$



$q : inc_1 : q'$ *(Increment)*

(i) Keep rest of first counter

F $\{P_1, P_2\}$

$$copy(\lceil q \rceil^1 \,;\, \lceil B \vee C_1 \rceil \,;\, \lceil C_1 \rceil, \{B, C_1\})$$

(ii) Leave second counter unchanged

$$copy(\lceil q \rceil^1 \,;\, \lceil B \vee C_1 \rceil \,;\, \lceil X \rceil^1, \{B, C_2\})$$

$q : dec_1 : q', q''$ (Decrement)

(i) If zero

$$\Box(\lceil q \rceil^1 ; \lceil B \rceil^1 ; \lceil X \rceil^1 ; \lceil B \vee C_2 \rceil^1 ; \ell = 4 \implies \ell = 4 ; \lceil q' \rceil^1 ; \lceil B \rceil^1 ; true)$$

(ii) Decrement counter

$$\forall\, d \bullet \Box(\lceil q \rceil^1 ; (\lceil B \rceil ; \lceil C_1 \rceil \wedge \ell = d) ; \lceil B \rceil ; \lceil B \vee C_1 \rceil ; \lceil X \rceil^1 ; \lceil B \vee C_2 \rceil^1 ; \ell =$$
$$\implies \ell = 4 ; \lceil q'' \rceil^1 ; \lceil B \rceil^d ; true)$$

(iii) Keep rest of first counter

$$copy(\lceil q \rceil^1 ; \lceil B \rceil ; \lceil C_1 \rceil ; \lceil B_1 \rceil, \{B, C_1\})$$

Final State

$$copy(\lceil q_{\mathit{fin}} \rceil^1 \,;\, \lceil B \vee C_1 \rceil^1 \,;\, \lceil X \rceil \,;\, \lceil B \vee C_2 \rceil^1, \{q_{\mathit{fin}}, B, X, C_1, C_2\})$$

Satisfiability

- Following [Chaochen and Hansen, 2004] we can observe that

  $\mathcal{M}$ **halts if and only if** the DC formula $F(\mathcal{M}) \wedge \Diamond\lceil q_{\mathit{fin}} \rceil$ is **satisfiable**.

  This yields

  > **Theorem 3.11.** The satisfiability problem for DC with continuous time is undecidable.

  (It is semi-decidable.)

- Furthermore, by taking the contraposition, we see

  $\mathcal{M}$ **diverges** **if and only if** $\mathcal{M}$ does not **halt**
  if and only if $F(\mathcal{M}) \wedge \neg\Diamond\lceil q_{\mathit{fin}} \rceil$ is **not** satisfiable.

- Thus whether a DC formula is **not satisfiable** is not decidable, not even semi-decidable.

Validity

- By Remark 2.13, F is valid iff $\neg F$ is not satisfiable, so

> **Corollary 3.12.** The validity problem for DC with continuous time is undecidable, not even semi-decidable.

Discussion

- Note: the DC fragment defined by the following grammar is **sufficient** for the reduction

$$F ::= \lceil P \rceil \mid \neg F_1 \mid F_1 \vee F_2 \mid F_1 \,;\, F_2 \mid \ell = 1 \mid \ell = x \mid \forall\, x \bullet F_1,$$

  P a state assertion, x a global variable.

- Formulae used in the reduction are abbreviations:

$$\begin{aligned} \ell = 4 &\iff \ell = 1 \,;\, \ell = 1 \,;\, \ell = 1 \,;\, \ell = 1 \\ \ell \geq 4 &\iff \ell = 4 \,;\, \mathit{true} \\ \ell = x + y + 4 &\iff \ell = x \,;\, \ell = y \,;\, \ell = 4 \end{aligned}$$

- Length 1 is not necessary — we can use $\ell = z$ instead, with fresh z.

- This is RDC augmented by "$\ell = x$" and "$\forall\, x$", which we denote by **RDC** $+ \ell = x, \forall\, x$.

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.