Declarative modelling for timing

The real-time logic: Duration Calculus

Michael R. Hansen

mrh@imm.dtu.dk

Informatics and Mathematical Modelling

Technical University of Denmark

Informal introduction to Duration Calculus

A logic for declarative modelling of real-time properties

- Background
- A simple case study: Gas Burner
- A decidability result
- pointers to current focus

Background

- Provable Correct Systems (ProCoS, ESPRIT BRA 3104)
  Bjørner Langmaack Hoare Olderog
- Project case study: Gas Burner Sørensen Ravn Rischel

Background

- Provable Correct Systems (ProCoS, ESPRIT BRA 3104)
  Bjørner Langmaack Hoare Olderog
- Project case study: Gas Burner Sørensen Ravn Rischel

  Intervals properties

  Timed Automata, Real-time Logic, Metric Temporal Logic, Explicit Clock Temporal, . . ., Alur, Dill, Jahanian, Mok, Koymans, Harel, Lichtenstein, Pnueli, . . .

Background

- Provable Correct Systems (ProCoS, ESPRIT BRA 3104)
  Bjørner Langmaack Hoare Olderog
- Project case study: Gas Burner Sørensen Ravn Rischel

  Intervals properties

  Timed Automata, Real-time Logic, Metric Temporal Logic, Explicit Clock Temporal, . . ., Alur, Dill, Jahanian, Mok, Koymans, Harel, Lichtenstein, Pnueli, . . .

  Duration of states

  Duration Calculus Zhou Hoare Ravn 91

Background

- Provable Correct Systems (ProCoS, ESPRIT BRA 3104)
  Bjørner Langmaack Hoare Olderog
- Project case study: Gas Burner Sørensen Ravn Rischel

  Intervals properties

  Timed Automata, Real-time Logic, Metric Temporal Logic, Explicit Clock Temporal, . . ., Alur, Dill, Jahanian, Mok, Koymans, Harel, Lichtenstein, Pnueli, . . .

  Duration of states

  Duration Calculus Zhou Hoare Ravn 91

  — an Interval Temporal Logic Halpern Moszkowski Manna

Background

- Provable Correct Systems (ProCoS, ESPRIT BRA 3104)
  Bjørner Langmaack Hoare Olderog
- Project case study: Gas Burner Sørensen Ravn Rischel
  Intervals properties
  Timed Automata, Real-time Logic, Metric Temporal Logic, Explicit Clock Temporal, . . ., Alur, Dill, Jahanian, Mok, Koymans, Harel, Lichtenstein, Pnueli, . . .
  Duration of states
  Duration Calculus Zhou Hoare Ravn 91
  — an Interval Temporal Logic Halpern Moszkowski Manna
- Logical Calculi, Applications, Mechanical Support
- Duration Calculus: A formal approach to real-time systems
  Zhou Chaochen and Michael R. Hansen
  Springer 2004

Gas Burner example: Requirements

State variables modelling Gas and Flame:

$$\mathrm{G}, \mathrm{F} : \mathbb{T}\text{ime} \to \{0, 1\}$$

State expression modelling that gas is Leaking

$$\mathrm{L} \mathrel{\widehat{=}} \mathrm{G} \land \neg \mathrm{F}$$

Gas Burner example: Requirements

State variables modelling Gas and Flame:

$$\mathrm{G}, \mathrm{F} : \mathbb{T}\text{ime} \rightarrow \{0, 1\}$$

State expression modelling that gas is Leaking

$$\mathrm{L} \mathrel{\widehat{=}} \mathrm{G} \wedge \neg \mathrm{F}$$

Requirement

- Gas must at most be leaking 1/20 of the elapsed time

$$(e - b) \geq 60\,\mathrm{s} \;\Rightarrow\; 20 \int_b^e \mathrm{L}(t)dt \leq (e - b)$$

Gas Burner example: Design decisions

- Leaks are detectable and stoppable within 1s:

$$\forall c, d : b \leq c < d \leq e.(\mathrm{L}[c, d] \;\Rightarrow\; (d - c) \leq 1\,\mathrm{s})$$

where

$$P[c, d] \;\widehat{=}\; \int_c^d P(t) = (d - c) > 0$$

which reads “P holds throughout $[c, d]$”

Gas Burner example: Design decisions

- Leaks are detectable and stoppable within 1s:

$$\forall c, d : b \leq c < d \leq e.(\mathrm{L}[c, d] \;\Rightarrow\; (d - c) \leq 1\,\mathrm{s})$$

where

$$P[c, d] \;\widehat{=}\; \int_c^d P(t) = (d - c) > 0$$

which reads "P holds throughout $[c, d]$"

- At least 30s between leaks:

$$\forall c, d, r, s : b \leq c < r < s < d \leq e.$$
$$(\mathrm{L}[c, r] \wedge \neg \mathrm{L}[r, s] \wedge \mathrm{L}[s, d]) \;\Rightarrow\; (s - r) \geq 30\,\mathrm{s}$$

Interval Logic

[Halpern Moszkowski Manna 83]

Terms: $\theta \; ::= \; x \mid v \mid \theta_1 + \theta_n \mid \; \ldots$ Temporal Variable

Interval Logic [Halpern Moszkowski Manna 83]

Terms: $\theta \;::=\; x \mid v \mid \theta_1 + \theta_n \mid \;\ldots$ Temporal Variable

$v : \mathbb{I}\text{ntv} \rightarrow \mathbb{R}$

Formulas: $\phi \;::=\; \theta_1 = \theta_n \mid \neg\phi \mid \phi \vee \psi \mid \phi ^\frown \psi \mid (\exists x)\phi \mid \;\ldots$ chop

$\phi : \mathbb{I}\text{ntv} \rightarrow \{\text{tt},\text{ff}\}$

Interval Logic [Halpern Moszkowski Manna 83]

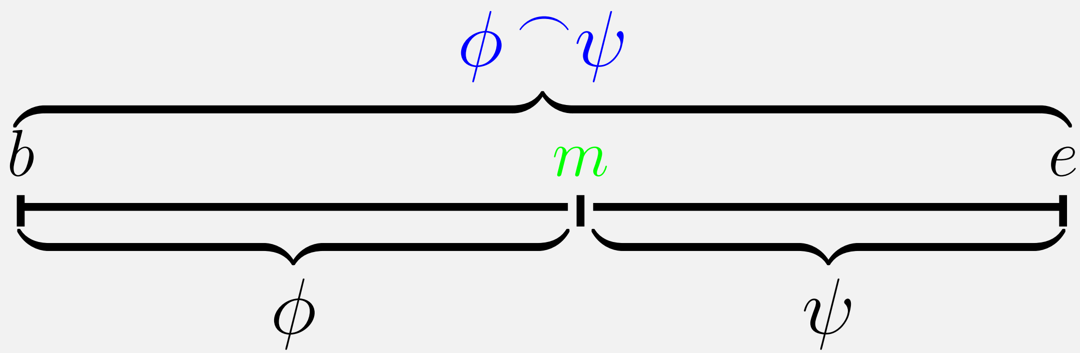
Terms: $\theta \ ::= \ x \mid v \mid \theta_1 + \theta_n \mid \ \ldots$ Temporal Variable

$v : \mathbb{I}\text{ntv} \to \mathbb{R}$

Formulas: $\phi \ ::= \ \theta_1 = \theta_n \mid \neg\phi \mid \phi \vee \psi \mid \phi \frown \psi \mid (\exists x)\phi \mid \ \ldots$ chop

$\phi : \mathbb{I}\text{ntv} \to \{\text{tt,ff}\}$

Chop:



for some $m : b \leq m \leq e$

Interval Logic [Halpern Moszkowski Manna 83]

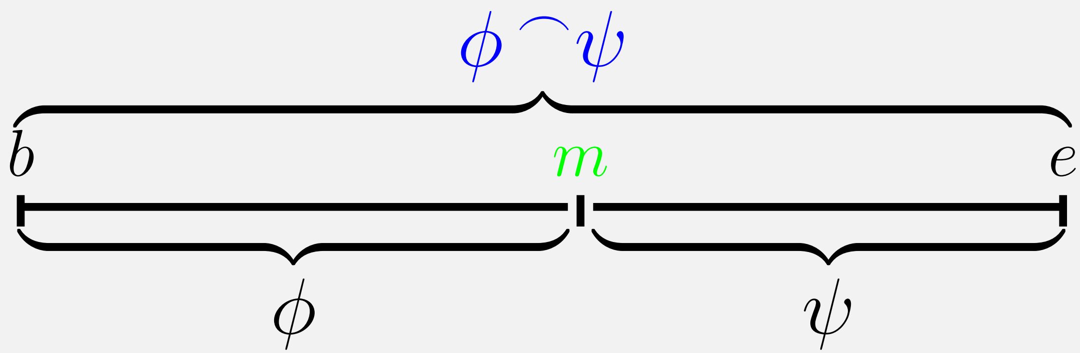
Terms: $\theta \;::=\; x \mid v \mid \theta_1 + \theta_n \mid \ldots$ Temporal Variable

v : $\mathbb{I}$ntv $\longrightarrow \mathbb{R}$

Formulas: $\phi \;::=\; \theta_1 = \theta_n \mid \neg\phi \mid \phi \vee \psi \mid \phi \frown \psi \mid (\exists x)\phi \mid \ldots$ chop

ϕ : $\mathbb{I}$ntv $\longrightarrow$ {tt,ff}

Chop:



for some $m : b \leq m \leq e$

In DC: $\mathbb{I}$ntv $= \{\ [a,b] \mid a, b \in \mathbb{R} \wedge a \leq b\}$

Duration Calculus [Zhou Hoare Ravn 91]

- State variables $P: \mathbb{T}\text{ime} \rightarrow \{0,1\}$ Finite Variability
- State expressions $S ::= 0 \mid 1 \mid P \mid \neg S \mid S_1 \vee S_2$

  $S : \mathbb{T}\text{ime} \rightarrow \{0,1\}$ pointwise defined

Duration Calculus [Zhou Hoare Ravn 91]

- State variables $P: \mathbb{T}\text{ime} \rightarrow \{0, 1\}$ Finite Variability

- State expressions $S ::= 0 \mid 1 \mid P \mid \neg S \mid S_1 \vee S_2$

  $S : \mathbb{T}\text{ime} \rightarrow \{0, 1\}$ pointwise defined

- Durations $\int S : \mathbb{I}\text{ntv} \rightarrow \mathbb{R}$ defined on $[b, e]$ by

  $$\int_b^e S(t)dt$$

  – Temporal variables with a structure

Example: Gas Burner

Requirement

$$\ell \geq 60 \;\Rightarrow\; 20\int L \leq \ell$$

Design decisions

$$\begin{array}{lcl} D_1 & \widehat{=} & \Box(\llbracket L \rrbracket \;\Rightarrow\; \ell \leq 1) \\ D_2 & \widehat{=} & \Box((\llbracket L \rrbracket \frown \llbracket \neg L \rrbracket \frown \llbracket L \rrbracket) \;\Rightarrow\; \ell \geq 30) \end{array}$$

where ℓ denotes the *length* of the interval, and

$\Diamond\phi$	$\widehat{=}$ true $\frown \phi \frown$ true	"for some sub-interval: ϕ"
$\Box\phi$	$\widehat{=} \neg\Diamond\neg\phi$	"for all sub-intervals: ϕ"
$\llbracket P \rrbracket$	$\widehat{=} \int P = \ell \;\wedge\; \ell > 0$	"P holds throughout a non-point interval"

Example: Gas Burner

Requirement

$$\ell \geq 60 \;\Rightarrow\; 20 \int L \leq \ell$$

Design decisions

$$D_1 \;\widehat{=}\; \Box(\lceil\!\lceil L \rceil\!\rceil \;\Rightarrow\; \ell \leq 1)$$

$$D_2 \;\widehat{=}\; \Box((\lceil\!\lceil L \rceil\!\rceil \frown \lceil\!\lceil \neg L \rceil\!\rceil \frown \lceil\!\lceil L \rceil\!\rceil) \;\Rightarrow\; \ell \geq 30)$$

where ℓ denotes the *length* of the interval, and

$\Diamond\phi$	$\widehat{=}$ true $\frown \phi \frown$ true	"for some sub-interval: ϕ"
$\Box\phi$	$\widehat{=} \neg\Diamond\neg\phi$	"for all sub-intervals: ϕ"
$\lceil\!\lceil P \rceil\!\rceil$	$\widehat{=} \int P = \ell \;\wedge\; \ell > 0$	"P holds throughout a non-point interval"

succinct formulation — no interval endpoints

Decidability

Decidability

What can't the computer do for me ?

Overview

[Zhou Hansen Sestoft 93]

Restricted Duration Calculus :

- $\llbracket S \rrbracket$
- $\neg\phi,\ \phi \vee \psi,\ \phi \frown \psi$

Satisfiability is reduced to emptiness of regular languages

Hence decidable for both discrete and continuous time

Overview

[Zhou Hansen Sestoft 93]

Restricted Duration Calculus :

- $\llbracket S \rrbracket$
- $\neg\phi,\ \phi \vee \psi,\ \phi \frown \psi$

Satisfiability is reduced to emptiness of regular languages

Hence decidable for both discrete and continuous time

Even small extensions give undecidable subsets

RDC_1 (Cont. time)	RDC_2	RDC_3
• $\ell = r,\ \llbracket S \rrbracket$ • $\neg\phi, \phi \vee \psi, \phi \frown \psi$	• $\int S_1 = \int S_2$ • $\neg\phi, \phi \vee \psi, \phi \frown \psi$	• $\ell = x, \llbracket S \rrbracket$ • $\neg\phi, \phi \vee \psi, \phi \frown \psi$ • $(\exists x)\phi$

Overview

[Zhou Hansen Sestoft 93]

Restricted Duration Calculus :

- $\lceil\!\lceil S \rceil\!\rceil$
- $\neg\phi,\ \phi \vee \psi,\ \phi\frown\psi$

Satisfiability is reduced to emptiness of regular languages

Hence decidable for both discrete and continuous time

Even small extensions give undecidable subsets

RDC_1 (Cont. time)	RDC_2	RDC_3
• $\ell = r,\ \lceil\!\lceil S \rceil\!\rceil$ • $\neg\phi, \phi \vee \psi, \phi\frown\psi$	• $\int S_1 = \int S_2$ • $\neg\phi, \phi \vee \psi, \phi\frown\psi$	• $\ell = x, \lceil\!\lceil S \rceil\!\rceil$ • $\neg\phi, \phi \vee \psi, \phi\frown\psi$ • $(\exists x)\phi$

How would you show such results?

Decidability of *RDC* for Discrete Time

Satisfiability is reduced to emptiness of regular languages

Decidability of *RDC* for Discrete Time

Satisfiability is reduced to emptiness of regular languages

Idea: $a \in \Sigma$ describes a piece of an interpretation, e.g. $P_1 \wedge \neg P_2 \wedge P_3$

Decidability of *RDC* for Discrete Time

Satisfiability is reduced to emptiness of regular languages

Idea: $a \in \Sigma$ describes a piece of an interpretation, e.g. $P_1 \land \neg P_2 \land P_3$

Discrete time — one letter corresponds to one time unit

$$\begin{aligned}
\mathcal{L}(\llbracket S \rrbracket) &= (DNF(S))^+ \\
\mathcal{L}(\varphi \lor \psi) &= \mathcal{L}(\varphi) \cup \mathcal{L}(\psi) \\
\mathcal{L}(\neg \varphi) &= \Sigma^* \setminus \mathcal{L}(\varphi) \\
\mathcal{L}(\varphi \frown \psi) &= \mathcal{L}(\varphi)\,\mathcal{L}(\psi)
\end{aligned}$$

Decidability of *RDC* for Discrete Time

Satisfiability is reduced to emptiness of regular languages

Idea: $a \in \Sigma$ describes a piece of an interpretation, e.g. $P_1 \wedge \neg P_2 \wedge P_3$

Discrete time — one letter corresponds to one time unit

$$
\begin{array}{lcl}
\mathcal{L}([\![S]\!]) & = & (DNF(S))^+ \\
\mathcal{L}(\varphi \vee \psi) & = & \mathcal{L}(\varphi) \cup \mathcal{L}(\psi) \\
\mathcal{L}(\neg\varphi) & = & \Sigma^* \setminus \mathcal{L}(\varphi) \\
\mathcal{L}(\varphi \frown \psi) & = & \mathcal{L}(\varphi)\,\mathcal{L}(\psi)
\end{array}
$$

- $\mathcal{L}(\phi)$ is regular
- ϕ is satisfiable iff $\mathcal{L}(\phi) \neq \emptyset$
- Satisfiability problem for *RDC* is decidable non-elementary

Example

- Is the formula $(\llbracket P \rrbracket \frown \llbracket P \rrbracket) \Rightarrow \llbracket P \rrbracket$ valid for discrete time?

Example

- Is the formula $(\llbracket P \rrbracket ^\frown \llbracket P \rrbracket) \Rightarrow \llbracket P \rrbracket$ valid for discrete time?
- $\Sigma = \{\{P\}, \{\}\}$.

Example

- Is the formula $(\llbracket P \rrbracket \frown \llbracket P \rrbracket) \Rightarrow \llbracket P \rrbracket$ valid for discrete time?
- $\Sigma = \{\{P\}, \{\}\}$.
- We have

$$
\begin{array}{ll}
 & (\llbracket P \rrbracket \frown \llbracket P \rrbracket) \Rightarrow \llbracket P \rrbracket \text{ is valid} \\
\text{iff} & \neg((\llbracket P \rrbracket \frown \llbracket P \rrbracket) \Rightarrow \llbracket P \rrbracket) \text{ is not satisfiable} \\
\text{iff} & (\llbracket P \rrbracket \frown \llbracket P \rrbracket) \wedge \neg \llbracket P \rrbracket \text{ is not satisfiable} \\
\text{iff} & \mathcal{L}_1(\llbracket P \rrbracket \frown \llbracket P \rrbracket) \cap \mathcal{L}_1(\neg \llbracket P \rrbracket) = \{\} \\
\text{iff} & \{\{P\}^i \mid i \geq 2\} \cap (\Sigma^* \setminus \{\{P\}^i \mid i \geq 1\}) = \{\}
\end{array}
$$

The last equality holds.

Example

- Is the formula $(\llbracket P \rrbracket \frown \llbracket P \rrbracket) \Rightarrow \llbracket P \rrbracket$ valid for discrete time?
- $\Sigma = \{\{P\}, \{\}\}$.
- We have

$$\begin{array}{ll} & (\llbracket P \rrbracket \frown \llbracket P \rrbracket) \Rightarrow \llbracket P \rrbracket \text{ is valid} \\ \text{iff} & \neg((\llbracket P \rrbracket \frown \llbracket P \rrbracket) \Rightarrow \llbracket P \rrbracket) \text{ is not satisfiable} \\ \text{iff} & (\llbracket P \rrbracket \frown \llbracket P \rrbracket) \wedge \neg \llbracket P \rrbracket \text{ is not satisfiable} \\ \text{iff} & \mathcal{L}_1(\llbracket P \rrbracket \frown \llbracket P \rrbracket) \cap \mathcal{L}_1(\neg \llbracket P \rrbracket) = \{\} \\ \text{iff} & \{\{P\}^i \mid i \geq 2\} \cap (\Sigma^* \setminus \{\{P\}^i \mid i \geq 1\}) = \{\} \end{array}$$

  The last equality holds.

- Therefore, the formula is valid for discrete time.

Hybrid Duration Calculus

Bolander Hansen Hansen 06-07

Improved expressivity at the same price

Hybrid DC

Hybrid DC is Restricted Duration Calculus extended by:

- Nominals a — names a specific interval

Hybrid DC

Hybrid DC is Restricted Duration Calculus extended by:

- Nominals a — names a specific interval $G(a) = [t_a, u_a]$
- Satisfaction operator $a : \phi$ — ϕ holds at a
- downarrow binder $\downarrow a.\phi$ holds if ϕ holds under the assumption that a names the current interval.
- global modality $E\phi$ holds if there is some interval where ϕ holds.

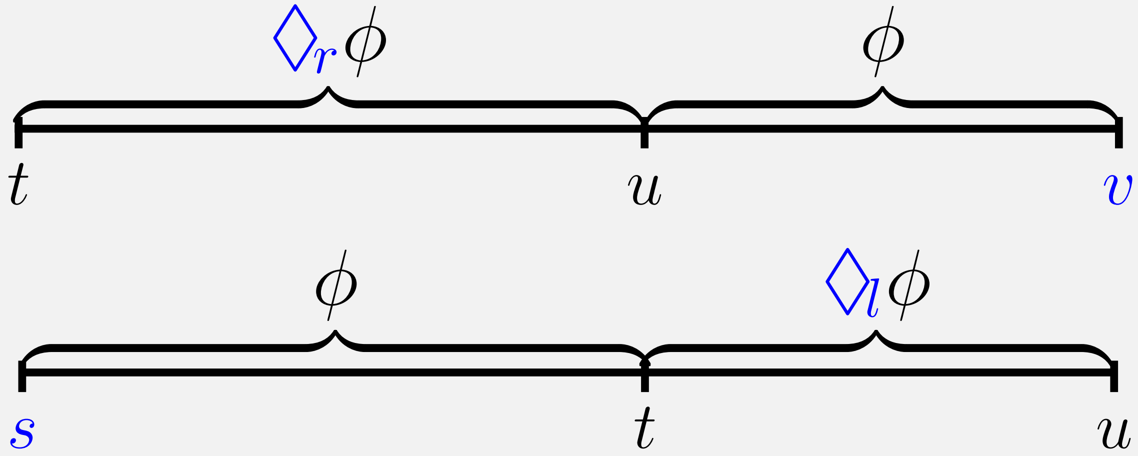
$\mathcal{I}, G, [t, u] \models a$	iff	$G(a) = [t, u]$
$\mathcal{I}, G, [t, u] \models a : \phi$	iff	$\mathcal{I}, G, G(a) \models \phi$
$\mathcal{I}, G, [t, u] \models E\phi$	iff	for some interval $[v, w]$: $\mathcal{I}, G, [v, w] \models \phi$
$\mathcal{I}, G, [t, u] \models \downarrow a.\phi$	iff	$\mathcal{I}, G[\,a := [t, u]\,], [t, u] \models \phi$

Expressibility: Neighbourhood RDC

Propositional neighbourhood logic:

ZhouHansen98,BaruaRoyZhou00

$$\mathcal{I},[t,u] \models \Diamond_l\phi \quad \text{iff} \quad \mathcal{I},[s,t] \models \phi \text{ for some } s \leq t$$
$$\mathcal{I},[t,u] \models \Diamond_r\phi \quad \text{iff} \quad \mathcal{I},[u,v] \models \phi \text{ for some } v \geq u$$



for some $v \geq u$

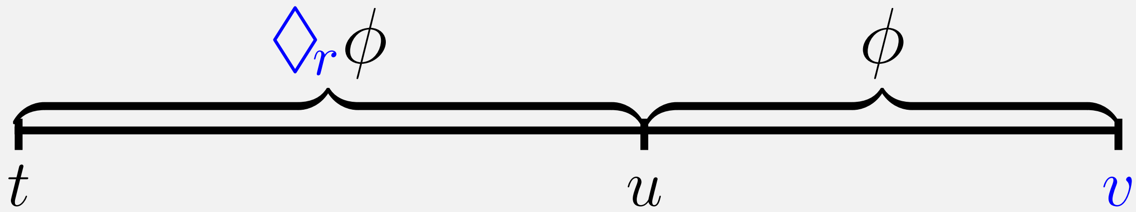
for some $s \leq t$

Expressibility: Neighbourhood RDC

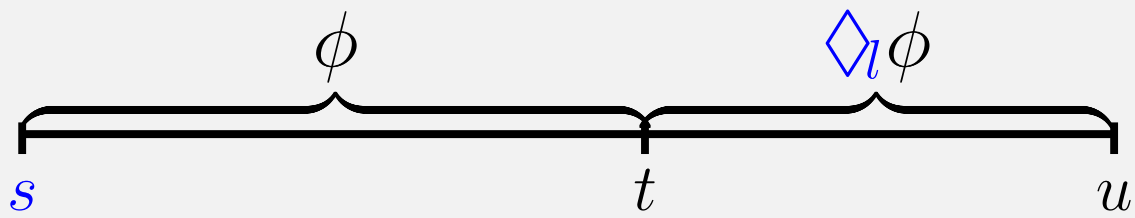
Propositional neighbourhood logic:

ZhouHansen98,BaruaRoyZhou00

$$\begin{array}{lll} \mathcal{I},[t,u] \models \Diamond_l \phi & \text{iff} & \mathcal{I},[s,t] \models \phi \text{ for some } s \leq t \\ \mathcal{I},[t,u] \models \Diamond_r \phi & \text{iff} & \mathcal{I},[u,v] \models \phi \text{ for some } v \geq u \end{array}$$



for some $v \geq u$



for some $s \leq t$

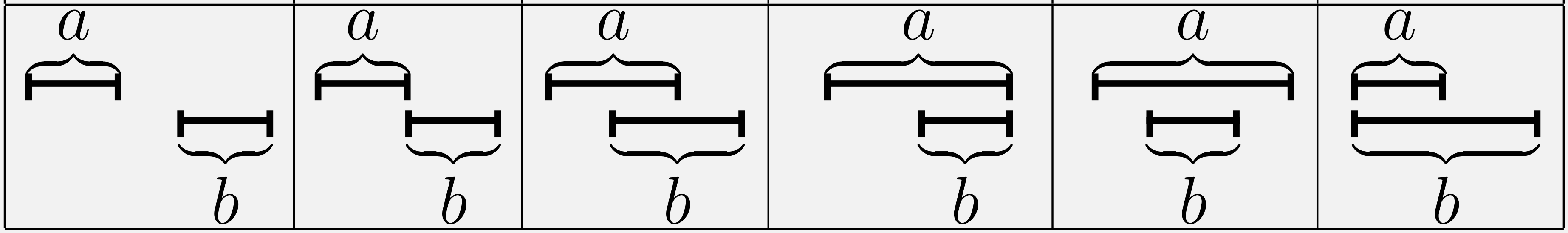
can be embedded in Hybrid DC:

$$\begin{array}{lll} \tau(\Diamond_l \phi) & = & \downarrow a.E(\phi \frown a) \\ \tau(\Diamond_r \phi) & = & \downarrow a.E(a \frown \phi) \end{array}$$

Expressibility: Allen's binary relations

All 13 (Allen) relations between two intervals are expressible. E.g.

a precedes b	a meets b	a overlaps b	a finished by b	a contains b	a starts b



a precedes b	$a : \Diamond_r(\neg\pi \wedge \Diamond_r b)$
a meets b	$a : \Diamond_r b$
a overlaps b	$E(\downarrow c. \neg\pi \wedge a : (\neg\pi \frown c) \wedge b : (c \frown \neg\pi))$
a finished by b	$a : (\neg\pi \frown b)$
a contains b	$a : (\neg\pi \frown b \frown \neg\pi)$
a starts b	$b : (a \frown \neg\pi)$

Monadic second-order theory of order $L_2^<$

We reduce satisfiability of Hybrid Duration Calculus to satisfiability of $L_2^<$. (Discrete as well as continuous time.)

Monadic second-order theory of order $L_2^<$

We reduce satisfiability of Hybrid Duration Calculus to satisfiability of $L_2^<$. (Discrete as well as continuous time.)

The formulas of $L_2^<$ are constructed from:

- First-order variables ranged over by $x, y, z, \ldots$.
- Second-order variables ranged over by $P, Q, X, \ldots$.

Monadic second-order theory of order $L_2^<$

We reduce satisfiability of Hybrid Duration Calculus to satisfiability of $L_2^<$. (Discrete as well as continuous time.)

The formulas of $L_2^<$ are constructed from:

- First-order variables ranged over by $x, y, z, \ldots$.
- Second-order variables ranged over by $P, Q, X, \ldots$.

The formulas are generated from the following grammar:

$$\phi ::= x < y \mid x \in P \mid \phi \vee \psi \mid \neg\phi \mid \exists x\phi \mid \exists P\phi \; .$$

Semantics of $L_2^<$

A *structure* $(A, B, <)$ consists of a set A partially ordered by $<$ and a set B of Boolean-valued functions from A. An element $b \in B$ can be considered a, possibly infinite, subset of A.

- An *interpretation* $\mathcal{I}$ associates a member $P_\mathcal{I}$ of B to every second-order variable P.
- A *valuation* ν is a function assigning a member $\nu(x)$ of A to every first-order variable x.

The semantic relation $\mathcal{I}, \nu \models \phi$ is then defined by:

$$
\begin{array}{lll}
\mathcal{I}, \nu \models x < y & \text{iff} & \nu(x) < \nu(y) \\
\mathcal{I}, \nu \models x \in P & \text{iff} & \nu(x) \in P_\mathcal{I} \\
\mathcal{I}, \nu \models \neg\phi & \text{iff} & \mathcal{I}, \nu \not\models \phi \\
\mathcal{I}, \nu \models \phi \vee \psi & \text{iff} & \mathcal{I}, \nu \models \phi \text{ or } \mathcal{I}, \nu \models \psi \\
\mathcal{I}, \nu \models \exists x \phi & \text{iff} & \text{for some } a \in A\text{: } \mathcal{I}, \nu[x := a] \models \phi \\
\mathcal{I}, \nu \models \exists P \phi & \text{iff} & \text{for some } b \in B\text{: } \mathcal{I}[P := b], \nu \models \phi
\end{array}
$$

Decidability results for $L_2^<$

Let $\omega = (\mathbb{N}, 2^{\mathbb{N}}, <)$.

- $L_2^<(\omega)$ is decidable — Büchi

From Hybrid DC to $L_2^<(\omega)$ — discrete time

- each state variable P corresponds to a second-order variable denoted by P. Idea: $i \in P$ iff $P(t) = 1$ in the interval $]i, i+1[$.
- each nominal a is associated with two variables x_a and y_a.

From Hybrid DC to $L_2^<(\omega)$ — discrete time

- each state variable P corresponds to a second-order variable denoted by P. Idea: $i \in P$ iff $P(t) = 1$ in the interval $]i, i+1[$.
- each nominal a is associated with two variables x_a and y_a.

$$
\begin{array}{lcl}
\mathcal{T}_{x,y}(\pi) & = & x = y \\
\mathcal{T}_{x,y}(P) & = & x < y \wedge \forall z (x \leq z < y \rightarrow z \in P) \\
\mathcal{T}_{x,y}(\neg\phi) & = & \neg\mathcal{T}_{x,y}(\phi) \\
\mathcal{T}_{x,y}(\phi \vee \psi) & = & \mathcal{T}_{x,y}(\phi) \vee \mathcal{T}_{x,y}(\psi) \\
\mathcal{T}_{x,y}(\phi \frown \psi) & = & \exists z (\mathcal{T}_{x,z}(\phi) \wedge \mathcal{T}_{z,y}(\phi) \wedge x \leq z \wedge z \leq y) \\
\mathcal{T}_{x,y}(a) & = & x = x_a \wedge y = y_a \\
\mathcal{T}_{x,y}(a : \phi) & = & \mathcal{T}_{x_a,y_a}(\phi) \\
\mathcal{T}_{x,y}(E\phi) & = & \exists x \exists y (x \leq y \wedge \mathcal{T}_{x,y}(\phi)) \\
\mathcal{T}_{x,y}(\downarrow a.\phi) & = & \exists x_a \exists y_a (x = x_a \wedge y = y_a \wedge \mathcal{T}_{x,y}(\phi))
\end{array}
$$

Correctness of translation

Discrete time:

- ϕ is satisfiable in discrete-time Hybrid DC
  iff $\mathcal{T}_{x,y}(\phi) \wedge x \leq y \wedge \bigwedge_{a \text{ in } \phi} x_a \leq y_a$ is satisfiable in $L_2^{<}(\omega)$.

The decision problem is non-elementary

Current focus

Model checking and deciding an interval logic with durations, aiming at verification of durational properties like:

- Per day, the telephone network is down for at most 15 seconds
$$\int Down \leq 15$$
- Total delay of message delivery across the network is less than 235ms $\Sigma_i \int delay(m_i) \leq 235$
- The lifetime of a system with two processors is at least k:

$$\left(\begin{array}{rl} & c_1 \int (A_1 \wedge A_2) \\ + & c_2 \int (A_1 \wedge \neg A_2) \\ + & c_3 \int (\neg A_1 \wedge A_2) \\ + & c_4 \int (\neg A_1 \wedge \neg A_2) \end{array}\right) \geq e \Rightarrow \ell \geq k$$

Involves *theory*, *applications* and *implementation*