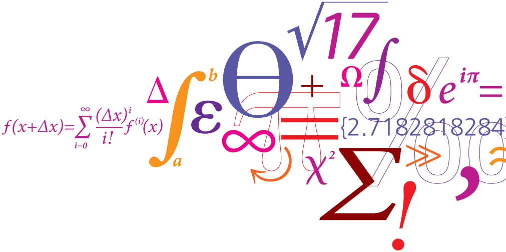
02917 Advanced Topics in Embedded Systems

Brief Introduction to Duration Calculus

Michael R. Hansen



DTU Informatics
Department of Informatics and Mathematical Modelling

Plan for today:

- A motivating example
  wireless sensor networks
- Brief introduction to Duration Calculus
- Overview of fundamental (un)decidability results
- A basic decidability results
  – with non-elementary complexity
- Towards efficient model checking for Duration Calculus based on approximations
- A decision procedure for Presburger Arithmetic

At 1 pm: IMM summer party.

Plan for today:

- A motivating example
  wireless sensor networks
- Brief introduction to Duration Calculus
- Overview of fundamental (un)decidability results
- A basic decidability results
  – with non-elementary complexity
- Towards efficient model checking for Duration Calculus based on approximations
- A decision procedure for Presburger Arithmetic

At 1 pm: IMM summer party.

Plan for today:

- A motivating example
  wireless sensor networks
- Brief introduction to Duration Calculus
- Overview of fundamental (un)decidability results
- A basic decidability results
  – with non-elementary complexity
- Towards efficient model checking for Duration Calculus based on approximations
- A decision procedure for Presburger Arithmetic

At 1 pm: IMM summer party.

Plan for today:

- A motivating example
  wireless sensor networks
- Brief introduction to Duration Calculus
- Overview of fundamental (un)decidability results
- A basic decidability results
  – with non-elementary complexity
- Towards efficient model checking for Duration Calculus based on approximations
- A decision procedure for Presburger Arithmetic

At 1 pm: IMM summer party.

Plan for today:

- A motivating example
  wireless sensor networks
- Brief introduction to Duration Calculus
- Overview of fundamental (un)decidability results
- A basic decidability results
  – with non-elementary complexity
- Towards efficient model checking for Duration Calculus based on approximations
- A decision procedure for Presburger Arithmetic

At 1 pm: IMM summer party.

Plan for today:

- A motivating example
  wireless sensor networks
- Brief introduction to Duration Calculus
- Overview of fundamental (un)decidability results
- A basic decidability results
  – with non-elementary complexity
- Towards efficient model checking for Duration Calculus based on approximations
- A decision procedure for Presburger Arithmetic

At 1 pm: IMM summer party.

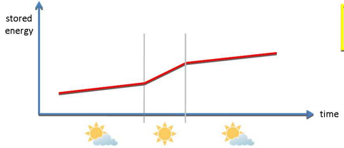
Plan for today:

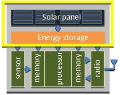
- A motivating example
  wireless sensor networks
- Brief introduction to Duration Calculus
- Overview of fundamental (un)decidability results
- A basic decidability results
  – with non-elementary complexity
- Towards efficient model checking for Duration Calculus based on approximations
- A decision procedure for Presburger Arithmetic

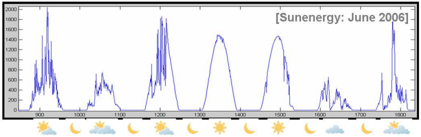
At 1 pm: IMM summer party.

Nodes with solar panels

A node of a wireless sensor network has a solar panel:

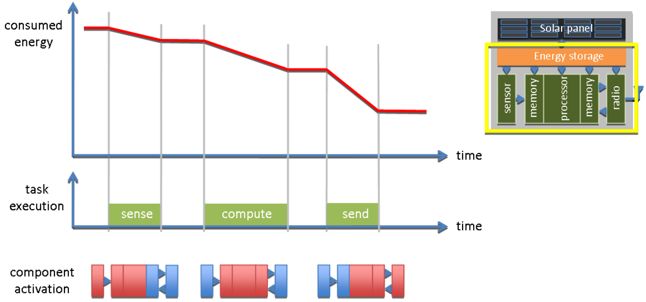






Energy consumption depends on usage

A node has a platform consisting of several components:



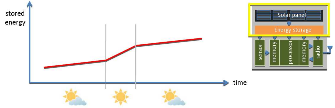
WSN-Model using parallel automata

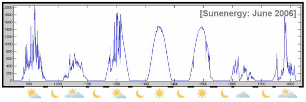
A wireless sensor network can be modelled by parallel automata:

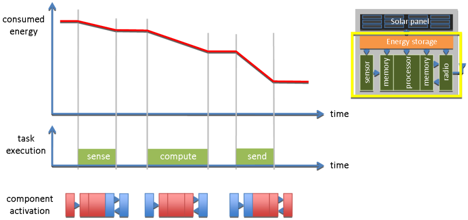
$$
\begin{aligned}
\mathrm{WSN} &= \|_{i=1}^{n}(\mathrm{Node}_i \parallel \mathrm{Environment}_i) \\
\mathrm{Node}_i &= \mathrm{SolarPanel}_i \parallel \mathrm{Application}_i \\
\mathrm{Environment}_i &= \mathrm{Sun}_i \\
\mathrm{Application}_i &= \|_{j=1}^{m_i}\mathrm{Program}_j \parallel \mathrm{Platform}_i \\
\mathrm{Platform}_i &= \mathrm{Processor}_i \parallel \mathrm{Sensor}_i \parallel \mathrm{Memory}_i \parallel \mathrm{Radio}_i \\
&\vdots
\end{aligned}
$$

WSN-Requirements expressed in Duration Calculus

Requirements can be modelled by Duration Calculus







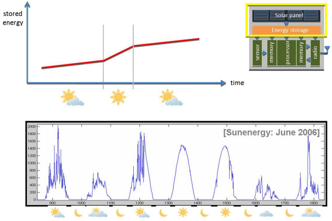
There should be sufficient energy during the lifetime:

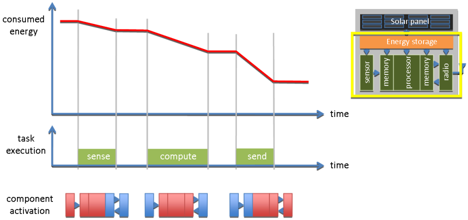
$$\Box_p \left(\ell \leq K \Rightarrow E_0 + \underbrace{\Sigma_i c_i \int \mathrm{sun}_i}_{\text{stored energy}} - \underbrace{\Sigma_j k_j \int \mathrm{program}_j}_{\text{consumed energy}} > 0 \right)$$

- Succinct formulation
- Tool support

WSN-Requirements expressed in Duration Calculus

Requirements can be modelled by Duration Calculus





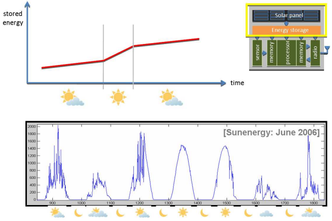
There should be sufficient energy during the lifetime:

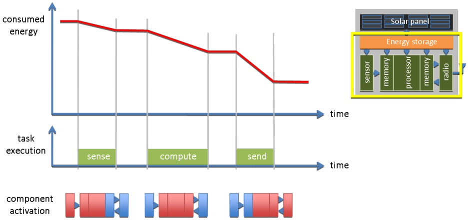
$$\Box_p \; (\; \ell \leq K \; \Rightarrow E_0 + \underbrace{\Sigma_i c_i \int \mathrm{sun}_i}_{\text{stored energy}} - \underbrace{\Sigma_j k_j \int \mathrm{program}_j}_{\text{consumed energy}} > 0 \;)$$

- Succinct formulation
- Tool support

WSN-Requirements expressed in Duration Calculus

Requirements can be modelled by Duration Calculus





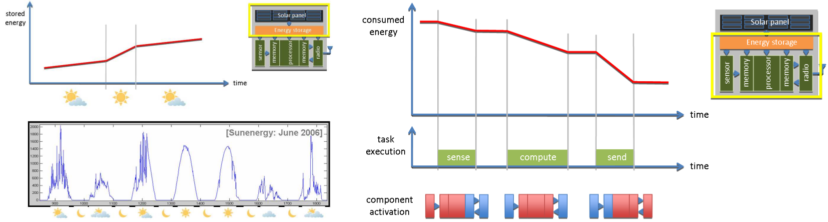
There should be sufficient energy during the lifetime:

$$\Box_p \left(\ell \leq K \Rightarrow E_0 + \underbrace{\Sigma_i c_i \int \mathrm{sun}_i}_{\text{stored energy}} - \underbrace{\Sigma_j k_j \int \mathrm{program}_j}_{\text{consumed energy}} > 0 \right)$$

- Succinct formulation 🙂
- Tool support

WSN-Requirements expressed in Duration Calculus

Requirements can be modelled by Duration Calculus



There should be sufficient energy during the lifetime:

$$\Box_p \; (\; \ell \leq K \Rightarrow E_0 + \underbrace{\Sigma_i c_i \int \mathrm{sun}_i}_{\text{stored energy}} - \underbrace{\Sigma_j k_j \int \mathrm{program}_j}_{\text{consumed energy}} > 0 \;)$$

- Succinct formulation
- Tool support

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

Current focus: Tool support with applications

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

Current focus: Tool support with applications

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

Current focus: Tool support with applications

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

Current focus: Tool support with applications

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

Current focus: Tool support with applications

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

Current focus: Tool support with applications

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

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

A ProCoS Case Study: Gas Burner System

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

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

A ProCoS Case Study: Gas Burner System

State variables modelling Gas and Flame:

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

State expression modelling that gas is Leaking

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

Requirement

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

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

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

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

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

- At least 30s between leaks:

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

Proof obligation: Conjunction of design decisions implies the requirements.

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:

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

Proof obligation: Conjunction of design decisions implies the requirements.

Gas Burner example: Design decisions

- Leaks are detectable and stoppable within 1s:

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

  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:

$$\begin{array}{l} \forall c, d, r, s : b \le c < r < s < d \le e . \\ \qquad (\mathrm{L}[c, r] \wedge \neg \mathrm{L}[r, s] \wedge \mathrm{L}[s, d]) \;\Rightarrow\; (s - r) \ge 30\,\mathrm{s} \end{array}$$

Proof obligation: Conjunction of design decisions implies the requirements.

Interval Logic - Halpern Moszkowski Manna 83

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

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

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

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

Chop:

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

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

Interval Logic - Halpern Moszkowski Manna 83

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

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

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

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

Chop:

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

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

Interval Logic - Halpern Moszkowski Manna 83

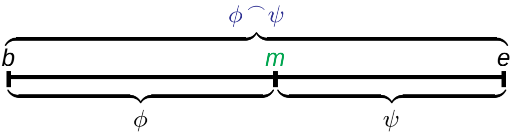
Terms: $\theta \ ::= \ x \mid v \mid \theta_1 + \theta_n \mid \ \ldots$ Temporal Variable

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

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

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

Chop:



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

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

Duration Calculus - Zhou Hoare Ravn 91

Extends Interval Temporal Logic as follows:

- 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

Duration Calculus - Zhou Hoare Ravn 91

Extends Interval Temporal Logic as follows:

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

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

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

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

– Temporal variables with a structure

Duration Calculus - Zhou Hoare Ravn 91

Extends Interval Temporal Logic as follows:

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

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

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

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

  – Temporal variables with a structure

Example: Gas Burner

Requirement

$$\ell \geq 60 \;\Rightarrow\; 20 \int \mathrm{L} \leq \ell$$

Design decisions

$$D_1 \;\widehat{=}\; \Box(\lceil \mathrm{L} \rceil \;\Rightarrow\; \ell \leq 1)$$
$$D_2 \;\widehat{=}\; \Box((\lceil \mathrm{L} \rceil \frown \lceil \neg \mathrm{L} \rceil \frown \lceil \mathrm{L} \rceil) \;\Rightarrow\; \ell \geq 30)$$

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"
$\lceil P \rceil$	$\widehat{=}\; \int P = \ell \;\wedge\; \ell > 0$	"P holds throughout a non-point interval"

succinct formulation — no interval endpoints

Example: Gas Burner

Requirement

$$\ell \geq 60 \;\Rightarrow\; 20 \int \mathrm{L} \leq \ell$$

Design decisions

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

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"
$\lceil P \rceil$	$\widehat{=} \int P = \ell \;\wedge\; \ell > 0$	"P holds throughout a non-point interval"

succinct formulation — no interval endpoints

Example: Gas Burner

Requirement

$$\ell \geq 60 \;\Rightarrow\; 20\int \mathrm{L} \leq \ell$$

Design decisions

$$\begin{aligned} D_1 \;&\widehat{=}\; \Box(\lceil \mathrm{L} \rceil \;\Rightarrow\; \ell \leq 1) \\ D_2 \;&\widehat{=}\; \Box((\lceil \mathrm{L} \rceil \frown \lceil \neg \mathrm{L} \rceil \frown \lceil \mathrm{L} \rceil) \;\Rightarrow\; \ell \geq 30) \end{aligned}$$

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"
$\lceil P \rceil$	$\widehat{=} \int P = \ell \;\wedge\; \ell > 0$	"P holds throughout a non-point interval"

succinct formulation — no interval endpoints