Introduction to Model Checking

(Preview of Core Course)

Emilio Tuosto
https://cs.gssi.it/emilio.tuosto/

Clemens Grabmayer
https://clegra.github.io

Department of Computer Science

GSSI GRAN SASSO SCIENCE INSTITUTE
SCHOOL OF ADVANCED STUDIES
Scuola Universitaria Superiore

December 2, 2024

Model Checking

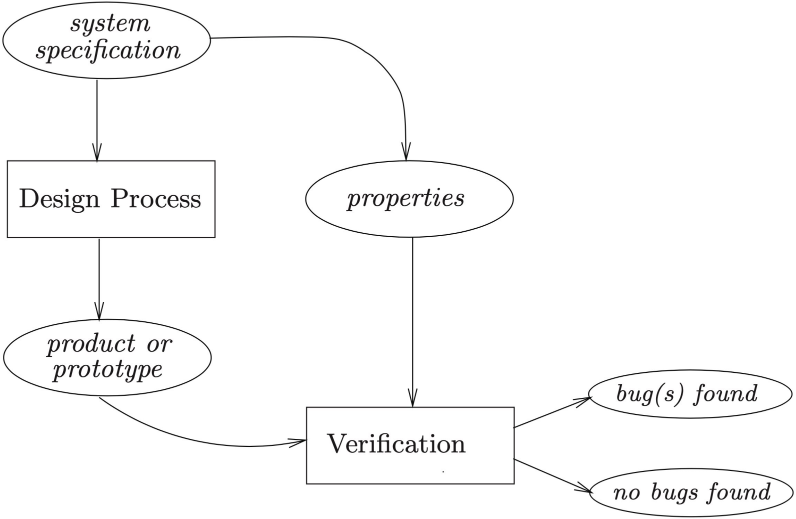
. . . is an effective automatable technique:

- *to expose potential software design errors;*
- *that, given a finite-state model of a system and a formal property, systematically checks whether this property holds for that model.*

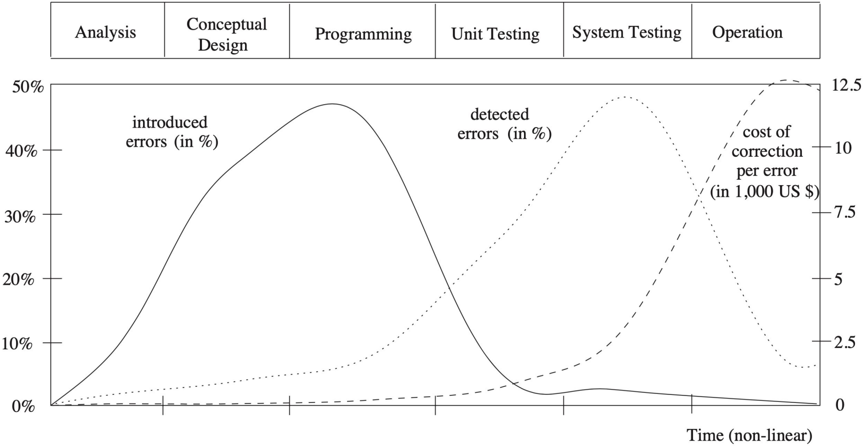
Strengths:

- widely applicable
  (embedded systems, software engineering, hardware design)
- supports partial verification (of modules)
- provides diagnostic information for debugging
- has sound mathematical underpinning (logic and process theory)

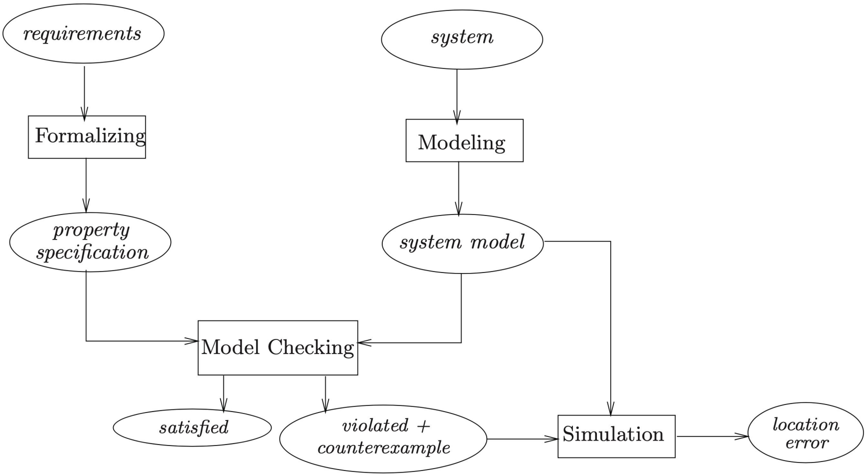
Hard-/Software Verification (traditionally)



Error introduction, detection, and repair costs



Model checking



Example: concurrency and non-determinism

Programs Inc, Dec, and Reset cooperate, and use a shared variable x:

```
proc Inc
  while true
    do
      if x < 200
        then x := x + 1
      fi
    od
```

```
proc Dec
  while true
    do
      if x > 0
        then x := x - 1
      fi
    od
```

```
proc Reset
  while true
    do
      if x = 200
        then x := 0
      fi
    od
```

Example: concurrency and non-determinism

Programs Inc, Dec, and Reset cooperate, and use a shared variable x:

```
proc Inc
  while true
    do
      if $x < 200$
        then $x := x + 1$
      fi
    od
```

```
proc Dec
  while true
    do
      if $x > 0$
        then $x := x - 1$
      fi
    od
```

```
proc Reset
  while true
    do
      if $x = 200$
        then $x := 0$
      fi
    od
```

Question: Is $0 \leq x \leq 200$ always guaranteed?

Modeling (by labeled transition systems)

```
proc Inc
  while true
    do
      if $x < 200$
        then $x := x + 1$
      fi
    od
```

```
proc Dec
  while true
    do
      if $x > 0$
        then $x := x - 1$
      fi
    od
```

```
proc Reset
  while true
    do
      if $x = 200$
        then $x := 0$
      fi
    od
```

Modeling (by labeled transition systems)

```
proc Inc
  while true
    do
1:    if $x < 200$
2:      then $x := x + 1$
      fi
    od
```

```
proc Dec
  while true
    do
1:    if $x > 0$
2:      then $x := x - 1$
      fi
    od
```

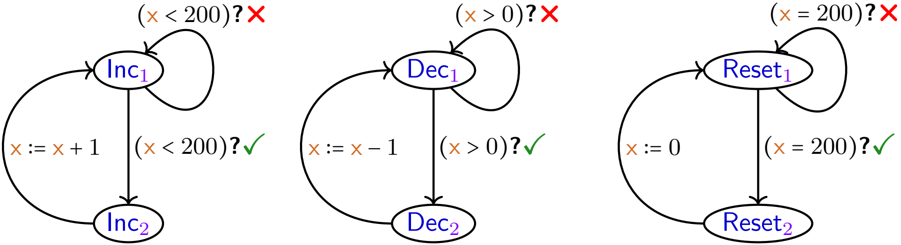
```
proc Reset
  while true
    do
1:    if $x = 200$
2:      then $x := 0$
      fi
    od
```

Modeling (by labeled transition systems)

```
   proc Inc
     while true
       do
1:       if $x < 200$
2:         then $x := x + 1$
         fi
       od
```

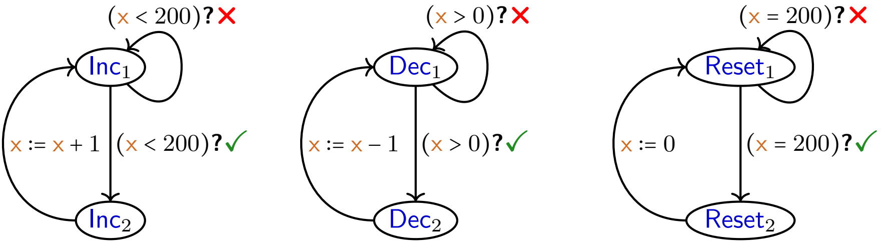
```
   proc Dec
     while true
       do
1:       if $x > 0$
2:         then $x := x - 1$
         fi
       od
```

```
   proc Reset
     while true
       do
1:       if $x = 200$
2:         then $x := 0$
         fi
       od
```



Labeled transition systems (LTSs)

Formalizing properties (in temporal logic)



$\mathsf{Inc}_1 \parallel \mathsf{Dec}_1 \parallel \mathsf{Reset}_1 \overset{?}{\models} \quad \Box(0 \leq x \wedge x \leq 200)$ (Linear-TL formula)

Counterexample (offending execution trace)

$$\boxed{\left\langle x = 199\,;\ \mathsf{Inc}_1 \parallel \mathsf{Dec}_1 \parallel \mathsf{Reset}_1 \right\rangle}$$

Counterexample (offending execution trace)

$$\boxed{\left\langle x = 199\,;\ \mathsf{Inc}_1 \parallel \mathsf{Dec}_1 \parallel \mathsf{Reset}_1 \right\rangle}$$

Counterexample (offending execution trace)

$$\begin{tikzcd}
\boxed{\left\langle x = 199\,;\ \mathsf{Inc}_1 \parallel \mathsf{Dec}_1 \parallel \mathsf{Reset}_1 \right\rangle} \arrow[d, "(\mathsf{x} < 200)\textbf{?}\checkmark"] \\
\boxed{\left\langle x = 199\,;\ \mathsf{Inc}_2 \parallel \mathsf{Dec}_1 \parallel \mathsf{Reset}_1 \right\rangle}
\end{tikzcd}$$

Counterexample (offending execution trace)

$$\begin{tikzcd} \boxed{\left\langle x = 199\,;\ \mathsf{Inc}_1 \parallel \mathsf{Dec}_1 \parallel \mathsf{Reset}_1 \right\rangle} \arrow[d, "(\mathsf{x} < 200)\textbf{?}\checkmark"] \\ \boxed{\left\langle x = 199\,;\ \mathsf{Inc}_2 \parallel \mathsf{Dec}_1 \parallel \mathsf{Reset}_1 \right\rangle} \end{tikzcd}$$

Counterexample (offending execution trace)

$$\begin{tikzcd}
\boxed{\left\langle x = 199\ ;\ \mathsf{Inc}_1 \parallel \mathsf{Dec}_1 \parallel \mathsf{Reset}_1 \right\rangle} \arrow[d, "(\mathsf{x} < 200)\textbf{?}\checkmark"] \\
\boxed{\left\langle x = 199\ ;\ \mathsf{Inc}_2 \parallel \mathsf{Dec}_1 \parallel \mathsf{Reset}_1 \right\rangle} \arrow[d, "\mathsf{x} := \mathsf{x} + 1"] \\
\boxed{\left\langle x = 200\ ;\ \mathsf{Inc}_1 \parallel \mathsf{Dec}_1 \parallel \mathsf{Reset}_1 \right\rangle}
\end{tikzcd}$$

Counterexample (offending execution trace)

$$\begin{tikzcd}
\boxed{\left\langle x = 199\,;\ \mathsf{Inc}_1 \parallel \mathsf{Dec}_1 \parallel \mathsf{Reset}_1 \right\rangle} \arrow[d, "(\mathsf{x} < 200)\textbf{?}\checkmark"] \\
\boxed{\left\langle x = 199\,;\ \mathsf{Inc}_2 \parallel \mathsf{Dec}_1 \parallel \mathsf{Reset}_1 \right\rangle} \arrow[d, "\mathsf{x} := \mathsf{x} + 1"] \\
\boxed{\left\langle x = 200\,;\ \mathsf{Inc}_1 \parallel \mathsf{Dec}_1 \parallel \mathsf{Reset}_1 \right\rangle}
\end{tikzcd}$$

Counterexample (offending execution trace)

$$\begin{tikzcd}
\boxed{\left\langle x = 199\,;\ \mathsf{Inc}_1 \parallel \mathsf{Dec}_1 \parallel \mathsf{Reset}_1 \right\rangle} \arrow[d, "(\mathsf{x} < 200)\textbf{?}\checkmark"] \\
\boxed{\left\langle x = 199\,;\ \mathsf{Inc}_2 \parallel \mathsf{Dec}_1 \parallel \mathsf{Reset}_1 \right\rangle} \arrow[d, "\mathsf{x} := \mathsf{x} + 1"] \\
\boxed{\left\langle x = 200\,;\ \mathsf{Inc}_1 \parallel \mathsf{Dec}_1 \parallel \mathsf{Reset}_1 \right\rangle} \arrow[d, "(\mathsf{x} > 0)\textbf{?}\checkmark"] \\
\boxed{\left\langle x = 200\,;\ \mathsf{Inc}_1 \parallel \mathsf{Dec}_2 \parallel \mathsf{Reset}_1 \right\rangle}
\end{tikzcd}$$

Counterexample (offending execution trace)

$$\begin{tikzcd}
\boxed{\left\langle x = 199\,;\ \mathsf{Inc}_1 \parallel \mathsf{Dec}_1 \parallel \mathsf{Reset}_1 \right\rangle} \arrow[d, "(\mathsf{x} < 200)\mathbf{?}\checkmark"] \\
\boxed{\left\langle x = 199\,;\ \mathsf{Inc}_2 \parallel \mathsf{Dec}_1 \parallel \mathsf{Reset}_1 \right\rangle} \arrow[d, "\mathsf{x} := \mathsf{x} + 1"] \\
\boxed{\left\langle x = 200\,;\ \mathsf{Inc}_1 \parallel \mathsf{Dec}_1 \parallel \mathsf{Reset}_1 \right\rangle} \arrow[d, "(\mathsf{x} > 0)\mathbf{?}\checkmark"] \\
\boxed{\left\langle x = 200\,;\ \mathsf{Inc}_1 \parallel \mathsf{Dec}_2 \parallel \mathsf{Reset}_1 \right\rangle}
\end{tikzcd}$$

Counterexample (offending execution trace)

$$\begin{tikzcd}
\boxed{\left\langle x = 199\,;\ \mathsf{Inc}_1 \parallel \mathsf{Dec}_1 \parallel \mathsf{Reset}_1 \right\rangle} \arrow[d, "(\mathsf{x} < 200)\mathbf{?}\checkmark"] \\
\boxed{\left\langle x = 199\,;\ \mathsf{Inc}_2 \parallel \mathsf{Dec}_1 \parallel \mathsf{Reset}_1 \right\rangle} \arrow[d, "\mathsf{x} := \mathsf{x} + 1"] \\
\boxed{\left\langle x = 200\,;\ \mathsf{Inc}_1 \parallel \mathsf{Dec}_1 \parallel \mathsf{Reset}_1 \right\rangle} \arrow[d, "(\mathsf{x} > 0)\mathbf{?}\checkmark"] \\
\boxed{\left\langle x = 200\,;\ \mathsf{Inc}_1 \parallel \mathsf{Dec}_2 \parallel \mathsf{Reset}_1 \right\rangle} \arrow[d, "(\mathsf{x} = 200)\mathbf{?}\checkmark"] \\
\boxed{\left\langle x = 200\,;\ \mathsf{Inc}_1 \parallel \mathsf{Dec}_2 \parallel \mathsf{Reset}_2 \right\rangle}
\end{tikzcd}$$

Counterexample (offending execution trace)

$$\boxed{\left\langle x = 199 \, ; \, \mathsf{Inc}_1 \parallel \mathsf{Dec}_1 \parallel \mathsf{Reset}_1 \right\rangle}$$

$$\Big\downarrow (\mathsf{x} < 200)\textbf{?}\checkmark$$

$$\boxed{\left\langle x = 199 \, ; \, \mathsf{Inc}_2 \parallel \mathsf{Dec}_1 \parallel \mathsf{Reset}_1 \right\rangle}$$

$$\Big\downarrow \mathsf{x} := \mathsf{x} + 1$$

$$\boxed{\left\langle x = 200 \, ; \, \mathsf{Inc}_1 \parallel \mathsf{Dec}_1 \parallel \mathsf{Reset}_1 \right\rangle}$$

$$\Big\downarrow (\mathsf{x} > 0)\textbf{?}\checkmark$$

$$\boxed{\left\langle x = 200 \, ; \, \mathsf{Inc}_1 \parallel \mathsf{Dec}_2 \parallel \mathsf{Reset}_1 \right\rangle}$$

$$\Big\downarrow (\mathsf{x} = 200)\textbf{?}\checkmark$$

$$\boxed{\left\langle x = 200 \, ; \, \mathsf{Inc}_1 \parallel \mathsf{Dec}_2 \parallel \mathsf{Reset}_2 \right\rangle}$$

Counterexample (offending execution trace)

$$\begin{tikzcd}
\boxed{\left\langle x = 199 \,;\, \mathsf{Inc}_1 \parallel \mathsf{Dec}_1 \parallel \mathsf{Reset}_1 \right\rangle} \arrow[d, "(\mathsf{x} < 200)\textbf{?}\checkmark"] \\
\boxed{\left\langle x = 199 \,;\, \mathsf{Inc}_2 \parallel \mathsf{Dec}_1 \parallel \mathsf{Reset}_1 \right\rangle} \arrow[d, "\mathsf{x} := \mathsf{x} + 1"] \\
\boxed{\left\langle x = 200 \,;\, \mathsf{Inc}_1 \parallel \mathsf{Dec}_1 \parallel \mathsf{Reset}_1 \right\rangle} \arrow[d, "(\mathsf{x} > 0)\textbf{?}\checkmark"] \\
\boxed{\left\langle x = 200 \,;\, \mathsf{Inc}_1 \parallel \mathsf{Dec}_2 \parallel \mathsf{Reset}_1 \right\rangle} \arrow[d, "(\mathsf{x} = 200)\textbf{?}\checkmark"] \\
\boxed{\left\langle x = 200 \,;\, \mathsf{Inc}_1 \parallel \mathsf{Dec}_2 \parallel \mathsf{Reset}_2 \right\rangle} \arrow[d, "\mathsf{x} := 0"] \\
\boxed{\left\langle x = 0 \,;\, \mathsf{Inc}_1 \parallel \mathsf{Dec}_2 \parallel \mathsf{Reset}_1 \right\rangle}
\end{tikzcd}$$

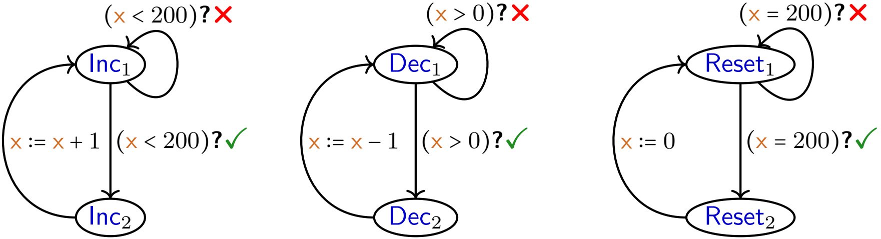
Counterexample (offending execution trace)

$$\begin{tikzcd}
\boxed{\left\langle x = 199\,;\ \mathsf{Inc}_1 \parallel \mathsf{Dec}_1 \parallel \mathsf{Reset}_1 \right\rangle} \arrow[d, "(\mathsf{x} < 200)\textbf{?}\checkmark"] \\
\boxed{\left\langle x = 199\,;\ \mathsf{Inc}_2 \parallel \mathsf{Dec}_1 \parallel \mathsf{Reset}_1 \right\rangle} \arrow[d, "\mathsf{x} := \mathsf{x} + 1"] \\
\boxed{\left\langle x = 200\,;\ \mathsf{Inc}_1 \parallel \mathsf{Dec}_1 \parallel \mathsf{Reset}_1 \right\rangle} \arrow[d, "(\mathsf{x} > 0)\textbf{?}\checkmark"] \\
\boxed{\left\langle x = 200\,;\ \mathsf{Inc}_1 \parallel \mathsf{Dec}_2 \parallel \mathsf{Reset}_1 \right\rangle} \arrow[d, "(\mathsf{x} = 200)\textbf{?}\checkmark"] \\
\boxed{\left\langle x = 200\,;\ \mathsf{Inc}_1 \parallel \mathsf{Dec}_2 \parallel \mathsf{Reset}_2 \right\rangle} \arrow[d, "\mathsf{x} := 0"] \\
\boxed{\left\langle x = 0\,;\ \mathsf{Inc}_1 \parallel \mathsf{Dec}_2 \parallel \mathsf{Reset}_1 \right\rangle}
\end{tikzcd}$$

Counterexample (offending execution trace)

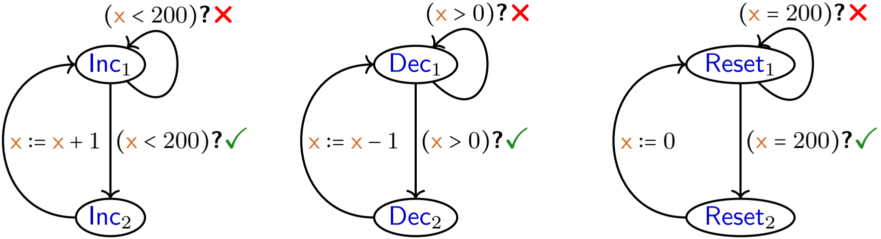
$$\begin{tikzcd}
\boxed{\left\langle x = 199\,;\ \mathsf{Inc}_1 \parallel \mathsf{Dec}_1 \parallel \mathsf{Reset}_1 \right\rangle} \arrow[d, "(\mathsf{x} < 200)\mathbf{?}\checkmark"] \\
\boxed{\left\langle x = 199\,;\ \mathsf{Inc}_2 \parallel \mathsf{Dec}_1 \parallel \mathsf{Reset}_1 \right\rangle} \arrow[d, "\mathsf{x} := \mathsf{x} + 1"] \\
\boxed{\left\langle x = 200\,;\ \mathsf{Inc}_1 \parallel \mathsf{Dec}_1 \parallel \mathsf{Reset}_1 \right\rangle} \arrow[d, "(\mathsf{x} > 0)\mathbf{?}\checkmark"] \\
\boxed{\left\langle x = 200\,;\ \mathsf{Inc}_1 \parallel \mathsf{Dec}_2 \parallel \mathsf{Reset}_1 \right\rangle} \arrow[d, "(\mathsf{x} = 200)\mathbf{?}\checkmark"] \\
\boxed{\left\langle x = 200\,;\ \mathsf{Inc}_1 \parallel \mathsf{Dec}_2 \parallel \mathsf{Reset}_2 \right\rangle} \arrow[d, "\mathsf{x} := 0"] \\
\boxed{\left\langle x = 0\,;\ \mathsf{Inc}_1 \parallel \mathsf{Dec}_2 \parallel \mathsf{Reset}_1 \right\rangle} \arrow[d, "\mathsf{x} := \mathsf{x} - 1"] \\
\boxed{\left\langle x = -1\,;\ \mathsf{Inc}_1 \parallel \mathsf{Dec}_1 \parallel \mathsf{Reset}_1 \right\rangle}
\end{tikzcd}$$

Formalizing properties (in temporal logic)



$\mathsf{Inc}_1 \parallel \mathsf{Dec}_1 \parallel \mathsf{Reset}_1 \not\models \Box(0 \leq x \wedge x \leq 200)$ (Linear-TL formula)

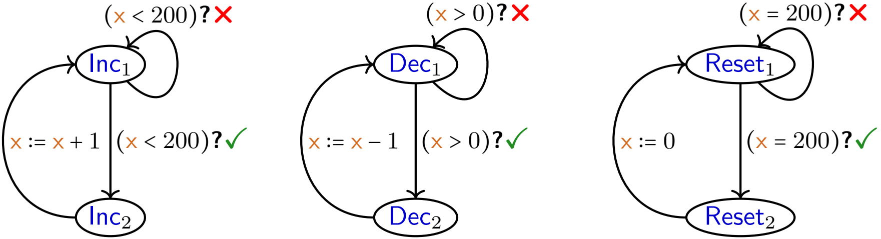
Formalizing properties (in temporal logic)



$\mathsf{Inc}_1 \parallel \mathsf{Dec}_1 \parallel \mathsf{Reset}_1 \not\models \Box(0 \leq x \wedge x \leq 200)$ (Linear-TL formula)

$\mathsf{Inc}_1 \parallel \mathsf{Dec}_1 \parallel \mathsf{Reset}_1 \quad \Diamond(x < 0)$ (LTL formula)

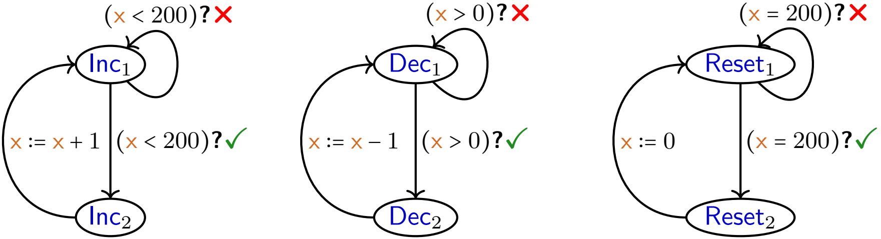
Formalizing properties (in temporal logic)



$\mathsf{Inc}_1 \parallel \mathsf{Dec}_1 \parallel \mathsf{Reset}_1 \;\not\models\; \Box(0 \le x \;\wedge\; x \le 200)$ (Linear-TL formula)

$\mathsf{Inc}_1 \parallel \mathsf{Dec}_1 \parallel \mathsf{Reset}_1 \;\models\; \Diamond(x < 0)$ (LTL formula)

Formalizing properties (in temporal logic)

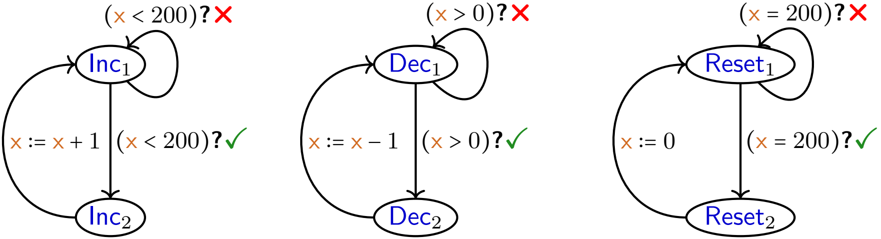


Inc$_1$ || Dec$_1$ || Reset$_1$ $\not\models$ $\Box(0 \leq x \ \wedge \ x \leq 200)$ (Linear-TL formula)

Inc$_1$ || Dec$_1$ || Reset$_1$ $\models$ $\Diamond(x < 0)$ (LTL formula)

Inc$_1$ || Dec$_1$ || Reset$_1$ $\forall\Box(0 \leq x \ \wedge \ x \leq 200)$ (Computation-Tree-L formula)

Formalizing properties (in temporal logic)

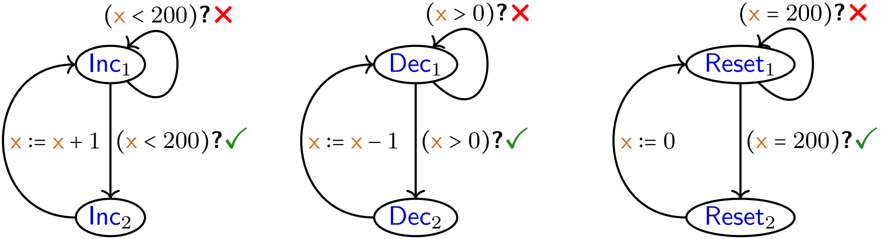


$\mathsf{Inc}_1 \parallel \mathsf{Dec}_1 \parallel \mathsf{Reset}_1 \;\not\models\; \Box(0 \le x \wedge x \le 200)$ (Linear-TL formula)

$\mathsf{Inc}_1 \parallel \mathsf{Dec}_1 \parallel \mathsf{Reset}_1 \;\models\; \Diamond(x < 0)$ (LTL formula)

$\mathsf{Inc}_1 \parallel \mathsf{Dec}_1 \parallel \mathsf{Reset}_1 \;\not\models\; \forall\Box(0 \le x \wedge x \le 200)$ (Computation-Tree-L formula)

Formalizing properties (in temporal logic)



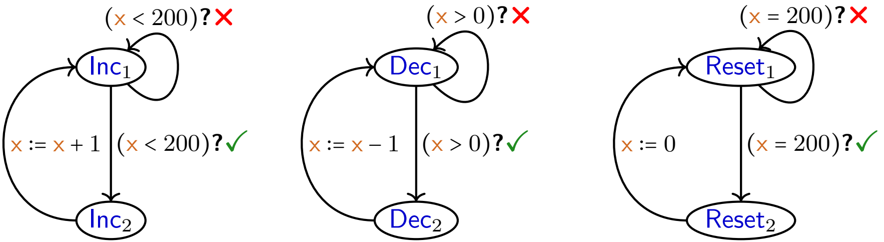
$\mathsf{Inc}_1 \parallel \mathsf{Dec}_1 \parallel \mathsf{Reset}_1 \;\not\models\; \Box(0 \leq x \wedge x \leq 200)$ (Linear-TL formula)

$\mathsf{Inc}_1 \parallel \mathsf{Dec}_1 \parallel \mathsf{Reset}_1 \;\models\; \Diamond(x < 0)$ (LTL formula)

$\mathsf{Inc}_1 \parallel \mathsf{Dec}_1 \parallel \mathsf{Reset}_1 \;\not\models\; \forall\Box(0 \leq x \wedge x \leq 200)$ (Computation-Tree-L formula)

$\mathsf{Inc}_1 \parallel \mathsf{Dec}_1 \parallel \mathsf{Reset}_1 \quad \exists\Box(0 \leq x \wedge x \leq 200)$ (CTL formula)

Formalizing properties (in temporal logic)



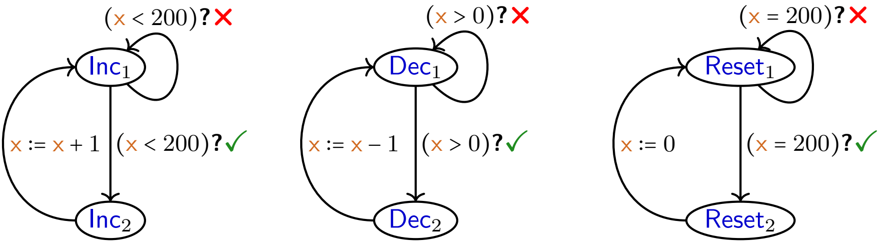
$\mathsf{Inc}_1 \parallel \mathsf{Dec}_1 \parallel \mathsf{Reset}_1 \;\not\models\; \Box(0 \le x \wedge x \le 200)$ (Linear-TL formula)

$\mathsf{Inc}_1 \parallel \mathsf{Dec}_1 \parallel \mathsf{Reset}_1 \;\models\; \Diamond(x < 0)$ (LTL formula)

$\mathsf{Inc}_1 \parallel \mathsf{Dec}_1 \parallel \mathsf{Reset}_1 \;\not\models\; \forall\Box(0 \le x \wedge x \le 200)$ (Computation-Tree-L formula)

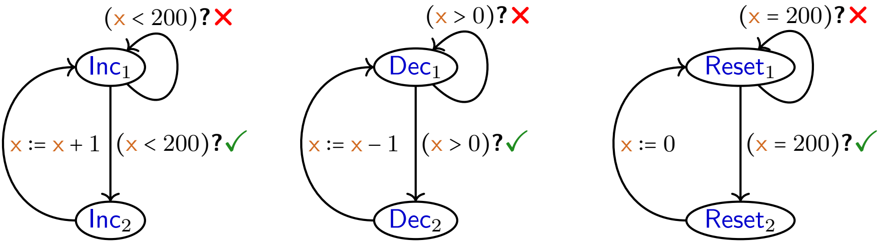
$\mathsf{Inc}_1 \parallel \mathsf{Dec}_1 \parallel \mathsf{Reset}_1 \;\models\; \exists\Box(0 \le x \wedge x \le 200)$ (CTL formula)

Formalizing properties (in temporal logic)



$\mathsf{Inc}_1 \parallel \mathsf{Dec}_1 \parallel \mathsf{Reset}_1$	$\not\models$	$\Box(0 \le x \wedge x \le 200)$	(Linear-TL formula)
$\mathsf{Inc}_1 \parallel \mathsf{Dec}_1 \parallel \mathsf{Reset}_1$	$\models$	$\Diamond(x < 0)$	(LTL formula)
$\mathsf{Inc}_1 \parallel \mathsf{Dec}_1 \parallel \mathsf{Reset}_1$	$\not\models$	$\forall\Box(0 \le x \wedge x \le 200)$	(Computation-Tree-L formula)
$\mathsf{Inc}_1 \parallel \mathsf{Dec}_1 \parallel \mathsf{Reset}_1$	$\models$	$\exists\Box(0 \le x \wedge x \le 200)$	(CTL formula)
$\mathsf{Inc}_1 \parallel \mathsf{Dec}_1 \parallel \mathsf{Reset}_1$		$\forall\Box\exists\Diamond(x < 0)$	(CTL formula)

Formalizing properties (in temporal logic)



$\mathsf{Inc}_1 \parallel \mathsf{Dec}_1 \parallel \mathsf{Reset}_1 \not\models \Box(0 \leq x \wedge x \leq 200)$ (Linear-TL formula)

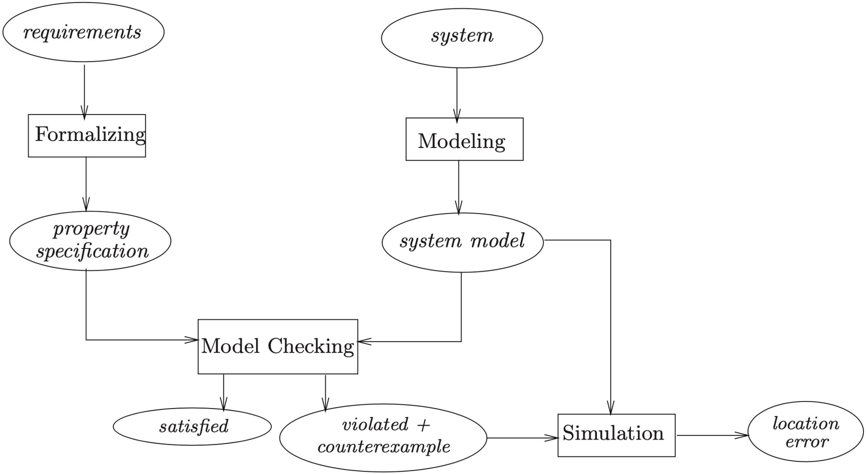
$\mathsf{Inc}_1 \parallel \mathsf{Dec}_1 \parallel \mathsf{Reset}_1 \models \Diamond(x < 0)$ (LTL formula)

$\mathsf{Inc}_1 \parallel \mathsf{Dec}_1 \parallel \mathsf{Reset}_1 \not\models \forall\Box(0 \leq x \wedge x \leq 200)$ (Computation-Tree-L formula)

$\mathsf{Inc}_1 \parallel \mathsf{Dec}_1 \parallel \mathsf{Reset}_1 \models \exists\Box(0 \leq x \wedge x \leq 200)$ (CTL formula)

$\mathsf{Inc}_1 \parallel \mathsf{Dec}_1 \parallel \mathsf{Reset}_1 \models \forall\Box\exists\Diamond(x < 0)$ (CTL formula)

Model checking



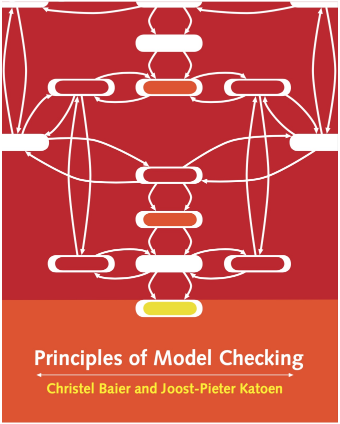
Any [such] verification is only as good as the model of the system.

Course topics

- modeling systems by labeled transition systems (LTSs)
- linear time behaviour properties (based on execution traces)
- concepts of fairness
- Linear Temporal Logic (LTL)
  - model checking
    - express properties by Büchi automata
    - model check LTSs and properties via product automata
- Computation Tree Logic (CTL) and variants (CTL^+, CTL^*)
- Partial model checking
  - for partially unknown systems (state properties/states/transitions)

- analysing system behavior with mCRL2

Book


Principles of Model Checking
Christel Baier and Joost-Pieter Katoen

- pdf available:
  https://is.ifmo.ru/books/_principles_of_model_checking.pdf

Course organization

Lectures (Emilio 2/Clemens 5)

- presentations on blackboard
- notes after the lecture (notes 2024/25 available)
- February (first/second week)

Course organization

Lectures (Emilio 2/Clemens 5)

- presentations on blackboard
- notes after the lecture (notes 2024/25 available)
- February (first/second week)

Exam

- options:
  - small verification project (of an algorithm, e.g. in mCRL2)
  - presentation about a paper
  - written exam?

Course organization

Lectures (Emilio 2/Clemens 5)

- presentations on blackboard
- notes after the lecture (notes 2024/25 available)
- February (first/second week)

Exam

- options:
  - small verification project (of an algorithm, e.g. in mCRL2)
  - presentation about a paper
  - written exam?

Thank you – we are looking forward to the course!