Software Verification
Exercise class:
Real Time Systems

Carlo A. Furia
Exercises:
Does the property hold?
Does the property hold?

\[
\begin{align*}
x &:= 0 \quad x := 0 \\
x &= 1 \quad x = 1
\end{align*}
\]
Does the property hold?

Yes:
- it simply means that \( a \) holds at every position in the word (if any)
Does the property hold?

\[ \square ( \diamond = 1 \ a ) \]
Does the property hold?

$\Box ( \Diamond = 1 \ a )$

No:

- this requires that there is always a future position, 1 time unit in the future, where $a$ holds
- but this is not the case in the last position of any (non-empty) timed word
Does the property hold?

\[ \square ( \square = 1 \; a ) \]
Does the property hold?

\[ \Box \ ( \ \Box = 1 \ a ) \]

Yes:
- the formula just requires that there if there is a future position 1 time unit in the future, then a holds there
- the automaton accepts only a's every time unit, hence the property is satisfied by any word accepted by the automaton
Does the property hold?

\[ \square (a \Rightarrow \Diamond (0,1) \ c) \]
Does the property hold?

\[ (a \Rightarrow \Diamond (0,1) \ c) \]

Yes:
- clock \( x \) is reset upon reading \( a \)
- after that, it is checked upon reading \( c \)
- the constraint requires that \( x \) is in the range \((0,1)\)

\( S_1 \)

\( x := 0 \)

\( 0 < x, y < 1 \)

\( S_2 \)

\( y := 0 \)

\( S_3 \)

\( c \)

\( x, y := 0 \)
Does the property hold?

□ ( a ⇒ ◊(0,1) b )
Does the property hold?

\[ (a \Rightarrow \Diamond(0,1) b) \]

Yes:
- clock \( x \) is reset upon reading \( a \); after that, it is checked upon reading \( c \), which is always preceded by a reading of \( b \)
- if \( b \) occurs later than or exactly after 1 time unit since the reading of \( b \), the same occurs for the reading of \( c \)
- in this case the constraint on \( x \) would be violated
Does the property hold?

□ \( (a \Rightarrow (a \lor b) \cup (0,1) c) \)
Does the property hold?

□ \((a \Rightarrow (a \lor b) \cup (0,1) c)\)

Yes:
- clock x is reset upon reading a
- after that there is one reading of b followed by a reading of c, which satisfies the sequence of events required by the until formula
- as far as timing is concerned, c must occur within interval of time (0,1) since a occurred because of the clock constraint \(0 < x, y < 1\)
Does the property hold?

□ ( a ⇒ (a ∨ b) U(1,2) c)
Does the property hold?

□ \((a \Rightarrow (a \lor b) \cup (1,2) \ c)\)

No:
- if the “next” \(c\) is considered w.r.t when \(a\) occurs, it cannot happen in interval \((1,2)\)
- if a successive occurrence of \(c\) is considered, it is preceded by at least another occurrence of \(c\), which is not admitted by \(a \lor b\)
Exercises:
Region automaton construction
Build the region automaton for:

\[
\begin{aligned}
&x := 0 \quad x := 0 \\
&x = 1 \quad x = 1 \\
&\text{a} \quad \text{a}
\end{aligned}
\]
Build the region automaton for:
Build the region automaton for:

- **S1**: $x, y := 0$
- **S2**: $y := 0$
- **S3**: $0 < x, y < 1$

Transitions:
- From S1 to S2 on 'a'
- From S2 to S3 on 'b'
- From S3 back to S1 on 'c'
Build the region automaton for:

$S_1 \quad x = y = 0$

$S_2 \quad x = 0$
- $0 < y < 1$
- $y = 1$
- $y > 1$

$S_3 \quad y = 0$
- $0 < x < 1$
- $x = 1$
- $x > 1$

Transitions:
- $a$: $x = 0$ from $S_2$ to $S_1$
- $b$: $y = 0$ from $S_3$ to $S_2$
- $c$: $x, y := 0$ from $S_1$ to $S_2$

States:
- $0 < x, y < 1$
- $x := 0$
- $y := 0$
Build the region automaton for:

Example from: Alur & Dill, 1994
Build the region automaton for:

Example from: Alur & Dill, 1994