Software Verification
Exercise class:
Real Time Systems

Carlo A. Furia
In all these exercises, we assume the nonnegative real numbers as time domain, unless explicitly stated otherwise.
Exercises:
Does the property hold?
Does the property hold?

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

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

\[
\begin{array}{c}
S1 \\
S2 \\
\end{array}
\]

\[
\begin{array}{c}
x := 0 \\
x = 1 \\
a \\
x := 0 \\
x = 1 \\
a \\
\end{array}
\]

\[\texttt{[]} (<>=1 \ a )\]
Does the property hold?

\[
\lbrack \lbrack ( \langle \rangle = 1 \ a ) \rbrack \rbrack
\]

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?

\[ (\text{[]}[\text{a}] = 1 \text{a} ) \]
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?

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

\[ \Box \left( a \Rightarrow \leftrightarrow(0,1) \ c \right) \]

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 \((0,1)\)
Does the property hold?

\[ \Box \left( a \Rightarrow \leftrightarrow(0,1) \ b \right) \]
Does the property hold?

\[ \left[ \begin{array}{c} a \\ \Rightarrow \end{array} \right] (0,1) b \]

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?

\[
\Box \left( a \Rightarrow (a \lor b) \cup (0,1) \circ c \right)
\]
Does the property hold?

\[
[\] ( a \Rightarrow (a \lor b) \mathbf{U}(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?

\[ \Box \left( a \Rightarrow (a \lor b) \cup (1,2) \land c \right) \]
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:

\[ x := 0 \quad x := 0 \]

\[ x = 1 \quad x = 1 \]

\[ a \quad a \]
Build the region automaton for:
Build the region automaton for:

\[ S_1 \]

- \( 0 < x, y < 1 \)
- \( x := 0 \)

\[ S_2 \]

- \( y := 0 \)
- \( b \)

\[ S_3 \]

- \( x, y := 0 \)
- \( c \)
Build the region automaton for:
Build the region automaton for:

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

Example from: Alur & Dill, 1994
Exercises:
Semantics of derived operators
MTL derived operators: always

Prove that the satisfaction relation

\[ w, i \vDash []<a,b> F \]

for bounded always, defined as:

\[ []<a,b> F \triangleq \neg (\text{True} U<a,b> \neg F) \]

is equivalent to:

for all \( i \leq j \leq n \) such that \( t(j) - t(i) \in <a,b> \) it is: \( w, j \vDash F \)
MTL derived operators: always

\[ w, i \models \mathbf{[]}_{<a,b>} F \]

iff

\[ w, i \models \neg (\mathbf{U}_{<a,b>} \neg F) \]  \hspace{1cm} \text{(definition of bounded always)}

iff

It is not the case that:
for some \( i \leq j \leq n \) such that \( t(j) - t(i) \in <a,b> \) it is: \( w, j \models \neg F \)
and for all \( i \leq k < j \) it is \( w, k \models \text{True} \)

\text{(definition of bounded until)}

iff

for all \( i \leq j \leq n \) such that \( t(j) - t(i) \in <a,b> \) it is: \( \neg w, j \models \neg F \)
or for all \( i \leq k < j \) it is \( w, k \models \text{False} \)

\text{(push negation inward)}

iff

for all \( i \leq j \leq n \) such that \( t(j) - t(i) \in <a,b> \) it is: \( \neg w, j \models \neg F \)
\hspace{1cm} \text{(dropping false term in disjunction)}

iff

for all \( i \leq j \leq n \) such that \( t(j) - t(i) \in <a,b> \) it is: \( w, j \models \text{F} \)
\hspace{1cm} \text{(simplification of double negation)}
MTL derived operators: $X$ and $X^{-}$

Compare the semantics of:

\[ X^+ F \triangleq True \land U=1 \land F \]

with the semantics of:

\[ X^- F \triangleq F \land U>0 \land True \]
Semantic of $X^+$

$w, i \vDash X^+ F$

iff

$w, i \vDash \text{True U} = 1 F$ \hspace{1em} (definition of $X^+$)

iff

iff

for some $i \leq j \leq n$ such that $t(j) - t(i) = 1$ it is: $w, j \vDash F$

and for all $i \leq k < j$ it is $w, k \nvdash \text{True}$

(definition of bounded until)

iff

iff

for some $i \leq j \leq n$ such that $t(j) = t(i) + 1$ it is: $w, j \nvdash F$

(simplify term)
Semantic of $X$-

\[ w, i \models X \neg F \]

iff

\[ w, i \models F \neg U > 0 \ True \quad \text{(definition of } X \neg \text{)} \]

iff

\[ \text{for some } i \leq j \leq n \text{ such that } t(j) - t(i) > 0 \text{ it is: } w, j \models \text{True} \]

and for all \( i \leq k < j \) it is \( w, k \models F \)

(definition of bounded until)

iff

\[ \text{for some } i < j \leq n \text{ it is: } w, j \models \text{True} \text{ and for all } i \leq k < j \text{ it is } w, k \models F \]

(timestamaps are strictly increasing by assumption)

iff

\[ i < n \text{ and } w, i \models F \]

(take \( j = i+1 \) so that \([i, j) = [i, i]\))
Exercises:
Equivalence of MTL formulas
Comparison of formulas

Is formula:


satisfied by any timed word?
Is formula satisfied?

Semantics of: \( w \not\models [\cdot] \lll 0 \) True

for all positions \( 1 \leq i \leq n \): \( w,i \not\models \lll 0 \) True

Semantics of: \( w,i \models \lll 0 \) True

for some \( j > i \) it is: \( w,j \models \) True

i.e.: \( i < n \)

Hence: \( w \not\models [\cdot] \lll 0 \) True

holds only for the empty word!
Comparison of formulas

Is formula:

\[
[] \gg 0 \text{ True}
\]

satisfied by any (non-empty) timed word?
Is formula satisfied?

Semantics of: \( w \vDash [[] \llr 0 \text{ True} \) 
for all positions \( 1 \leq i \leq n \): \( w,i \vDash \llr 0 \text{ True} \)

Semantics of: \( w,i \vDash \llr 0 \text{ True} \)
for some \( j \geq i \) it is: \( w,j \vDash \text{ True} \)
i.e.: \( \text{True} \)
because one can always take \( j = i \)

Hence: \( w \vDash [[] \llr 0 \text{ True} \)
holds for any word.
Comparison of formulas

Is formula:

$\llbracket a, b \rrbracket \llbracket c, d \rrbracket \ \mathbf{q}$

equivalent or non-equivalent to:

$\llbracket a + c, b + d \rrbracket \ \mathbf{q}$
Inequivalent formulas

Informal meaning of: \(<[a,b]<>[c,d]\) \(q\)

- let i be the current position
- there exist a future position \(j > i\) in the word with time in \([a,b]\) relative to i such that:
  - there exist another future position \(k > j\) in the word with time in \([c,d]\) relative to j, where \(q\) holds
- in all, the time at which \(q\) holds is in \([a+c, b+d]\) relative to i

Informal meaning of: \(<[a+c,b+d]\) \(q\)

- let i be the current position
- there exist another future position \(k > i\) in the word with time in \([a+c,b+d]\) relative to i, where \(q\) holds

Hence, for instance: timed word \(w = (\{\}, 3) (\{q\}, 3+b+c)\)

is such that: \(w\) satisfies \(<[a+c,b+d]\) \(q\) but it does not satisfy \(<[a,b]<>[c,d]\) \(q\)

because there is no intermediate position between the first and the one where \(q\) holds