Introduction to Formal Methods
Chapter 07: LTL Symbolic Model Checking

Roberto Sebastiani

DISI, Università di Trento, Italy – roberto.sebastiani@unitn.it
URL: http://disi.unitn.it/rseba/DIDATTICA/fm2020/
Teaching assistant: Enrico Magnago – enrico.magnago@unitn.it

CDLM in Informatica, academic year 2019-2020

last update: Monday 18th May, 2020, 14:48

Outline

1. The problem
2. The general algorithm
   - Compute the tableau T_ψ
   - Compute the product $M \times T_\psi$
   - Check the emptiness of $\mathcal{L}(M \times T_\psi)$
3. An example
4. Exercises

The problem

- Given a Kripke structure M and an LTL specification φ, does M satisfy φ?:

$$M \models \varphi$$

- Equivalent to the CTL* M.C. problem:

$$M \models \mathbf{A}\varphi$$

- Dual CTL* M.C. problem:

$$M \models \mathbf{E}\neg\varphi$$

LTL Symbolic M.C.

- Let M be a Kripke model and φ be an LTL formula:

$$
\begin{array}{ll}
& M \models \mathbf{A}\varphi \text{ (CTL}^*\text{)} \\
\Longleftrightarrow & M \models \varphi \quad \text{(LTL)} \\
\Longleftrightarrow & \mathcal{L}(M) \subseteq \mathcal{L}(\varphi) \\
\Longleftrightarrow & \mathcal{L}(M) \cap \overline{\mathcal{L}(\varphi)} = \emptyset \\
\Longleftrightarrow & \mathcal{L}(M) \cap \mathcal{L}(\neg\varphi) = \emptyset \\
\Longleftrightarrow & \mathcal{L}(M) \cap \mathcal{L}(T_{\neg\varphi}) = \emptyset \\
\Longleftrightarrow & \mathcal{L}(M \times T_{\neg\varphi}) = \emptyset \\
\Longleftrightarrow & M \times T_{\neg\varphi} \not\models \mathbf{EG}\textit{true}
\end{array}
$$

- $T_{\neg\varphi}$ is a fair Kripke structure, called Tableau, which represents all and only the paths that satisfy $\neg\varphi$ (do not satisfy φ)

$\Longrightarrow$ $M \times T_{\neg\varphi}$ represents all and only the paths appearing in M and not in φ.

LTL Symbolic M.C. (dual version)

- Let M be a Kripke model and $\psi \stackrel{\text{def}}{=} \neg\varphi$ be an LTL formula:

$$\begin{array}{rl} & M \models \mathbf{E}\psi \\ \Longleftrightarrow & M \not\models \mathbf{A}\neg\psi \\ \Longleftrightarrow & \ldots \\ \Longleftrightarrow & \mathcal{L}(M \times T_\psi) \neq \emptyset \\ \Longleftrightarrow & M \times T_\psi \models \mathbf{EG}\mathit{true} \end{array}$$

- T_ψ is a fair Kripke structure, called Tableau, which represents all and only the paths that satisfy the LTL formula ψ

$\Longrightarrow$ $M \times T_\psi$ represents all and only the paths appearing in both M and T_ψ.

LTL Symbolic Model Checking

Three steps:

(i) Compute the tableau T_ψ
(T_ψ is a fair Kripke structure)

(ii) Compute the product $M \times T_\psi$
($M \times T_\psi$ is a fair Kripke structure)

(iii) Check the emptiness of $\mathcal{L}(M \times T_\psi)$
(e.i., check that $M \times T_\psi \not\models \textbf{EG}\,True$)

Building the tableau T_ψ for ψ: the set of states

- Elementary subformulas of ψ: $el(\psi)$
  - $el(p) := \{p\}$
  - $el(\neg\varphi_1) := el(\varphi_1)$
  - $el(\varphi_1 \wedge \varphi_2) := el(\varphi_1) \cup el(\varphi_2)$
  - $el(\mathbf{X}\varphi_1) = \{\mathbf{X}\varphi_1\} \cup el(\varphi_1)$
  - $el(\varphi_1 \mathbf{U} \varphi_2) := \{\mathbf{X}(\varphi_1 \mathbf{U} \varphi_2)\} \cup el(\varphi_1) \cup el(\varphi_2)$
- Intuition: $el(\psi)$ is the set of propositions and **X**-formulas occurring ψ', ψ' being the result of applying recursively the tableau expansion rules to ψ
- The set of states S_{T_ψ} of T_ψ is given by $2^{el(\psi)}$
- The labeling function L_{T_ψ} of T_ψ comes straightforwardly (the label is the Boolean component of each state)

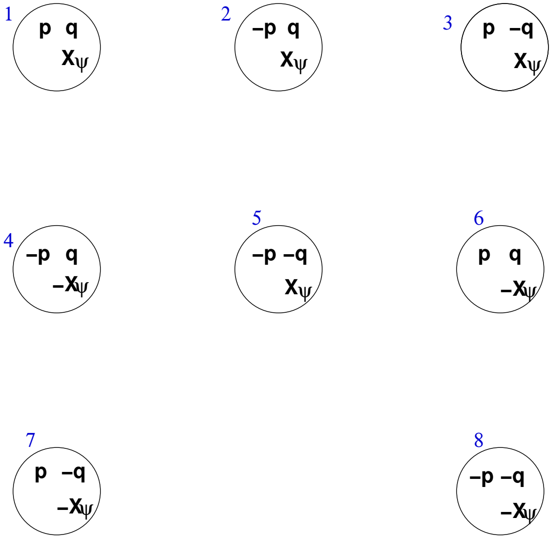
Example: $\psi := p\mathbf{U}q$

- $el(p\mathbf{U}q) = el((q \vee (p \wedge \mathbf{X}(p\mathbf{U}q))) = \{p, q, \mathbf{X}(p\mathbf{U}q)\}$
  $\Longrightarrow S_{T_\psi} = \{$

$$
\begin{array}{lll}
1: & \{p, q, \mathbf{X}(p\mathbf{U}q)\}, & [p\mathbf{U}q] \\
2: & \{\neg p, q, \mathbf{X}(p\mathbf{U}q)\}, & [p\mathbf{U}q] \\
3: & \{p, \neg q, \mathbf{X}(p\mathbf{U}q)\}, & [p\mathbf{U}q] \\
4: & \{\neg p, q, \neg\mathbf{X}(p\mathbf{U}q)\}, & [p\mathbf{U}q] \\
5: & \{\neg p, \neg q, \mathbf{X}(p\mathbf{U}q)\}, & [\neg p\mathbf{U}q] \\
6: & \{p, q, \neg\mathbf{X}(p\mathbf{U}q)\}, & [p\mathbf{U}q] \\
7: & \{p, \neg q, \neg\mathbf{X}(p\mathbf{U}q)\}, & [\neg p\mathbf{U}q] \\
8: & \{\neg p, \neg q, \neg\mathbf{X}(p\mathbf{U}q)\} & [\neg p\mathbf{U}q]
\end{array}
$$

$\}$

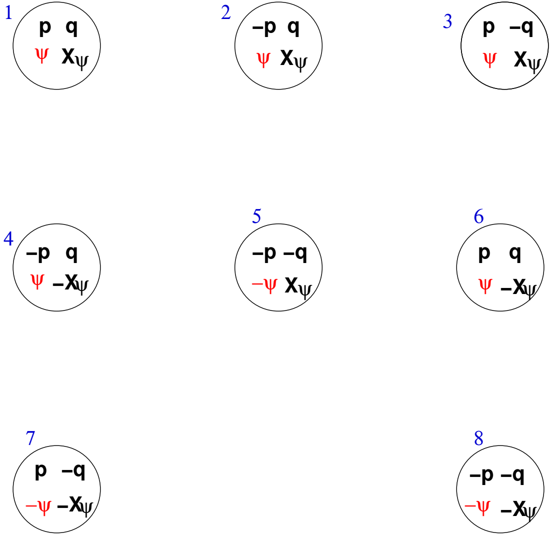
Example: $\psi := p\mathbf{U}q$ [cont.]



Building the tableau T_ψ for ψ: *sat*()

- Set of states in S_{T_ψ} satisfying φ_i: $sat(\varphi_i)$
  - $sat(\varphi_1) := \{s \mid \varphi_1 \in s\}$, $\varphi_1 \in el(\psi)$
  - $sat(\neg\varphi_1) := S_{T_\psi} / sat(\varphi_1)$
  - $sat(\varphi_1 \wedge \varphi_2) := sat(\varphi_1) \cap sat(\varphi_2)$
  - $sat(\varphi_1 \mathbf{U} \varphi_2) := sat(\varphi_2) \cup (sat(\varphi_1) \cap sat(\mathbf{X}(\varphi_1 \mathbf{U} \varphi_2)))$
- intuition: *sat*() establishes in which states subformulas are true

Example: $\psi := p\mathbf{U}q$ [cont.]



Building the tableau T_ψ for ψ: initial states and transition relation

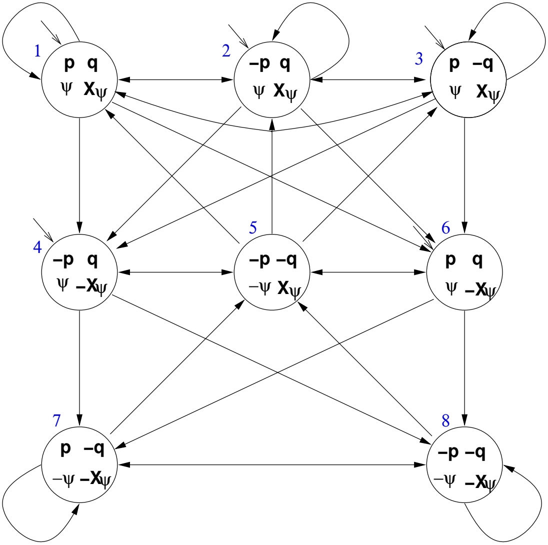
- Set of states in S_{T_ψ} satisfying φ_i: $sat(\varphi_i)$
  - $sat(\varphi_1) := \{s \mid \varphi_1 \in s\}$, $\varphi_1 \in el(\psi)$
  - $sat(\neg\varphi_1) := S_{T_\psi} / sat(\varphi_1)$
  - $sat(\varphi_1 \wedge \varphi_2) := sat(\varphi_1) \cap sat(\varphi_2)$
  - $sat(\varphi_1 \mathbf{U} \varphi_2) := sat(\varphi_2) \cup (sat(\varphi_1) \cap sat(\mathbf{X}(\varphi_1 \mathbf{U} \varphi_2)))$
- Intuition: $sat()$ establishes in which states subformulas are true
- The set of initial states I_{T_ψ} is defined as

$$I_{T_\psi} = sat(\psi)$$

- The transition relation R_{T_ψ} is defined as

$$R_{T_\psi}(s, s') = \bigcap_{\mathbf{X}\varphi_i \in el(\psi)} \{(s, s') \mid s \in sat(\mathbf{X}\varphi_i) \Leftrightarrow s' \in sat(\varphi_i)\}$$

Example: $\psi := p\mathbf{U}q$ [cont.]



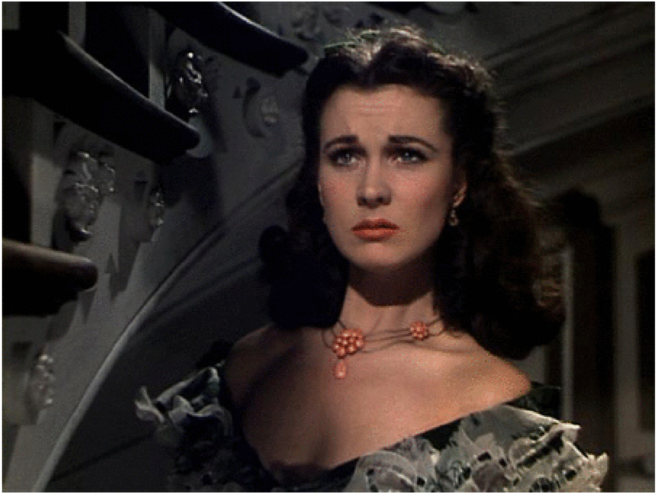
Problems with **U**-subformulas

- R_{T_ψ} does not guarantee that the **U**-subformulas are fulfilled
- Example: state 3 $\{p, \neg q, \mathbf{X}(p\mathbf{U}q)\}$:
  although state 3 belongs to

$$sat(p\mathbf{U}q) := sat(q) \cup (sat(p) \cap sat(\mathbf{X}(p\mathbf{U}q))),$$

  the path which loops forever in state 3 does not satisfy $p\mathbf{U}q$, as q never holds in that path.

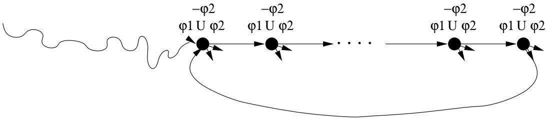
Tableaux rules: a quote



"After all... tomorrow is another day."
[Scarlett O'Hara, "Gone with the Wind"]

Fairness conditions for every **U**-subformula

- it must never happen that we get into a state s' from which we can enter a path π' in which $\varphi_1 \mathbf{U} \varphi_2$ holds forever and φ_2 never holds. In CTL*: $\neg \mathbf{EFEG}((\varphi_1 \mathbf{U} \varphi_2) \wedge \neg \varphi_2)$ ("bad loop")

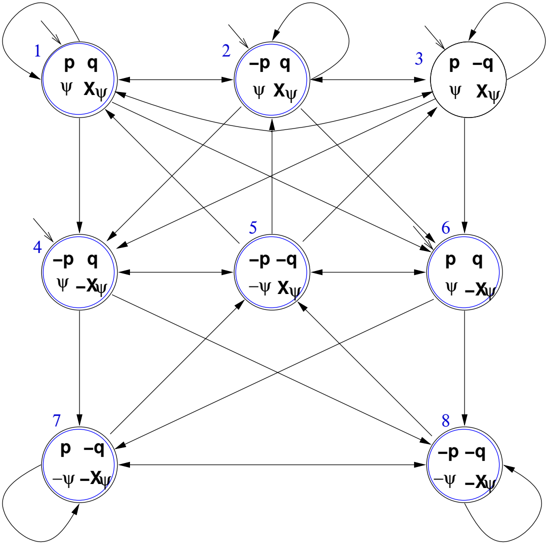


$\Longrightarrow$ For every [positive] **U**-subformula $\varphi_1 \mathbf{U} \varphi_2$ of ψ, we must add a fairness CTL* condition $\mathbf{AGAF}(\neg(\varphi_1 \mathbf{U} \varphi_2) \vee \varphi_2)$
(in LTL: $\mathbf{GF}(\neg(\varphi_1 \mathbf{U} \varphi_2) \vee \varphi_2)$)
If no [positive] U-subformulas, then add one fairness condition $\mathbf{AGAF}\top$.

$\Longrightarrow$ We restrict the admissible paths of T_ψ to those which verify the fairness condition: $T_\psi := \langle S_{T_\psi}, I_{T_\psi}, R_{T_\psi}, L_{T_\psi}, F_{T_\psi} \rangle$

$$F_{T_\psi} := \{sat(\neg(\varphi_1 \mathbf{U} \varphi_2) \vee \varphi_2)) \; s.t. \; (\varphi_1 \mathbf{U} \varphi_2) \; occurs \; [positively] in \; \psi\}$$

Example: $\psi := p\mathbf{U}q$ [cont.]



Symbolic representation of T_ψ

- State variables: one Boolean variable for each formula in $el(\psi)$
  - EX: p, q and x and primed versions p', q' and x'
    [x is a Boolean label for $\mathbf{X}(p\mathbf{U}q)$]
- $sat(\varphi_i)$:
  - $sat(p) := p$, s.t. p Boolean state variable
  - $sat(\neg\varphi_1) := \neg sat(\varphi_1)$
  - $sat(\varphi_1 \wedge \varphi_2) := sat(\varphi_1) \wedge sat(\varphi_2)$
  - $sat(\mathbf{X}\varphi_i) := x_{[\mathbf{X}\varphi_i]}$, s.t. $x_{[\mathbf{X}\varphi_i]}$ Boolean state variable
  - $sat(\varphi_1\mathbf{U}\varphi_2) := sat(\varphi_2) \vee (sat(\varphi_1) \wedge sat(\mathbf{X}(\varphi_1\mathbf{U}\varphi_2)))$

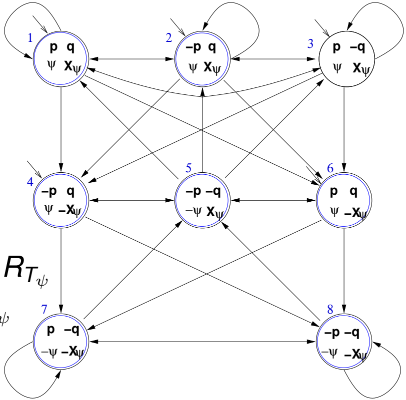
  $\Longrightarrow$ $sat(\varphi_1\mathbf{U}\varphi_2) := sat(\varphi_2) \vee (sat(\varphi_1) \wedge x_{[\mathbf{X}\varphi_1\mathbf{U}\varphi_2]})$
- ...

Symbolic representation of T_ψ [cont.]

- ...
- Initial states: $I_{T_\psi} = sat(\psi)$
  - EX: $I(p, q, x) = q \vee (p \wedge x)$
- Transition Relation:
  $R_{T_\psi}(s, s') = \bigcap_{\mathbf{X}\varphi_i \in el(\psi)} \{(s, s') \mid s \in sat(\mathbf{X}\varphi_i) \Leftrightarrow s' \in sat(\varphi_i)\}$
  - $R_{T_\psi} = \bigwedge_{\mathbf{X}\varphi_i \in el(\psi)} (sat(\mathbf{X}\varphi_i) \leftrightarrow sat'(\varphi_i))$
    where $sat'(\varphi_i)$ is $sat(\varphi_i)$ on primed variables
  - EX: $R_{T_\psi}(p, q, x, p', q', x') = x \leftrightarrow (q' \vee (p' \wedge x'))$
- Fairness Conditions:
  $F_{T_\psi} := \{sat(\neg(\varphi_1 \mathbf{U} \varphi_2) \vee \varphi_2))\ s.t.\ (\varphi_1 \mathbf{U} \varphi_2)\ occurs\ [positively] in\ \psi\}$
  - EX: $F_{T_\psi}(p, q, x) = \neg(q \vee (p \wedge x)) \vee q = ... = \neg p \vee \neg x \vee q$

Symbolic representation of T_ψ: examples

- $I_{T_\psi}(p, q, x) = q \vee (p \wedge x)$
  - $1: \quad \{p, q, x\} \models I_{T_\psi}$
  - $3: \quad \{p, \neg q, x\} \models I_{T_\psi}$
  - $\not{5}: \quad \{\neg p, \neg q, x\} \not\models I_{T_\psi}$
- $R_{T_\psi}(p, q, x, p', q', x') = x \leftrightarrow (q' \vee (p' \wedge x'))$
  - $1 \Rightarrow 1: \quad \{p, q, x, p', q', x'\} \models R_{T_\psi}$
  - $6 \Rightarrow 7: \quad \{p, q, \neg x, p', \neg q', \neg x'\} \models R_{T_\psi}$
  - $6 \not\Rightarrow 1: \quad \{p, q, \neg x, p', q', x'\} \not\models R_{T_\psi}$
- $F_{T_\psi}(p, q, x) = \neg p \vee \neg x \vee q$
  - $1: \quad \{p, q, x\} \models F_{T_\psi}$
  - $5: \quad \{\neg p, \neg q, x\} \models F_{T_\psi}$
  - $\not{3}: \quad \{p, \neg q, x\} \not\models F_{T_\psi}$



Computing the product $P := T_\psi \times M$

- Given $M := \langle S_M, I_M, R_M, L_M \rangle$ and $T_\psi := \langle S_{T_\psi}, I_{T_\psi}, R_{T_\psi}, L_{T_\psi}, F_{T_\psi} \rangle$, we compute the product $P := T_\psi \times M = \langle S, I, R, L, F \rangle$ as follows:
  - $S := \{(s, s') \mid s \in S_{T_\psi},\ s' \in S_M \textit{ and } L_M(s')|_\psi \ = \ L_{T_\psi}(s)\}$
  - $I := \{(s, s') \mid s \in I_{T_\psi},\ s' \in I_M \textit{ and } L_M(s')|_\psi \ = \ L_{T_\psi}(s)\}$
  - Given $(s, s'), (t, t') \in S$, $((s, s'), (t, t')) \in R$ iff $(s, t) \in R_{T_\psi}$ and $(s', t') \in R_M$
  - $L((s, s')) = L_{T_\psi}(s) \cup L_M(s')$
- Extension of *sat*() and F_{T_ψ} to P:
  $(s, s') \in sat(\psi) \Longleftrightarrow s \in sat(\psi)$
  $F := \{sat(\neg(\varphi_1 \mathbf{U} \varphi_2) \vee \varphi_2)\ s.t.\ (\varphi_1 \mathbf{U} \varphi_2)\ occurs\ [positively] in\ \psi\}$

Computing the product $P := T_\psi \times M$ symbolically

Let V, W be the array of Boolean state variables of T_ψ and M respectively:

- Initial states: $I(V \cup W) = I_{T_\psi}(V) \wedge I_M(W)$
- Transition Relation: $R(V \cup W, V' \cup W') = R_{T_\psi}(V, V') \wedge R_M(W, W')$
- Fairness conditions:
  $\{F_1(V \cup W), ..., F_k(V \cup W)\} = \{F_{T_\psi 1}(V), ..., F_{T_\psi k}(V)\}$

Main theorem [Clarke, Grumberg & Hamaguchi; 94]

Theorem

THEOREM: $M.s' \models \mathbf{E}\psi$ iff there is a state s in T_ψ s.t. $(s, s') \in sat(\psi)$ and $T_\psi \times M, (s, s') \models \mathbf{EG}true$ under the fairness conditions:

$$\{sat(\neg(\varphi_1 \mathbf{U} \varphi_2) \vee \varphi_2)) \; s.t. \; (\varphi_1 \mathbf{U} \varphi_2) \; occurs \; in \; \psi\}.$$

$\Longrightarrow$ $M \models \mathbf{E}\psi$ iff $T_\psi \times M \models \mathbf{E}_f\mathbf{G}true$

$\Longrightarrow$ $M \models \neg\psi$ iff $T_\psi \times M \not\models \mathbf{E}_f\mathbf{G}true$

- LTL M.C. reduced to Fair CTL M.C.!!!
- Symbolic OBDD-based techniques apply.

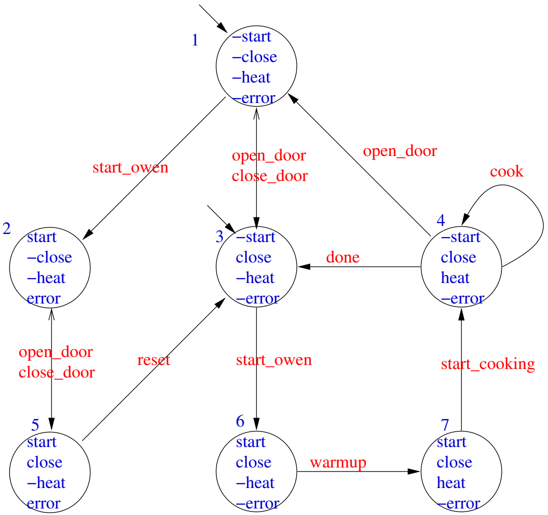
Note

The transition relation R of $T_\psi \times M$ may not be total.
$\Longrightarrow$ `Check_FairEG` does not need to consider states without successors, restricting R to the remaining states.

A microwave oven

- 4 variables: start, close, heat, error
- Actions (implicit): start_oven,open_door, close_door, reset, warmup, start_cooking, cook, done
- Error situation: if oven is started while the door is open
- Represented as a Kripke structure (and hence as a OBDD's)

A microwave oven [cont.]



A microwave oven: symbolic representation

- Initial states: $I_M(s, c, h, e) = \neg s \land \neg h \land \neg e$
- Transition relation: $R_M(s, c, h, e, s', c', h', e') =$ [a simplification of]

$$
\begin{array}{ll}
(\neg s \land \neg c \land \neg h \land \neg e \land \neg s' \land c' \land \neg h' \land \neg e') \lor & (close\_door,\ no\ error) \\
(s \land \neg c \land \neg h \land e \land s' \land c' \land \neg h' \land e') \lor & (close\_door,\ error) \\
(\neg s \land c \land \neg e \land \neg s' \land \neg c' \land \neg h' \land \neg e') \lor & (open\_door,\ no\ error) \\
(s \land c \land \neg h \land e \land s' \land \neg c' \land \neg h' \land e') \lor & (open\_door,\ error) \\
(\neg s \land c \land \neg h \land \neg e \land s' \land c' \land \neg h' \land \neg e') \lor & (start\_oven,\ no\ error) \\
(\neg s \land \neg c \land \neg h \land \neg e \land s' \land \neg c' \land \neg h' \land e') \lor & (start\_oven,\ error) \\
(s \land c \land \neg h \land e \land \neg s' \land c' \land \neg h' \land \neg e') \lor & (reset) \\
(s \land c \land \neg h \land \neg e \land s' \land c' \land h' \land \neg e') \lor & (warmup) \\
(s \land c \land h \land \neg e \land \neg s' \land c' \land h' \land \neg e') \lor & (start\_cooking) \\
(\neg s \land c \land h \land \neg e \land \neg s' \land c' \land h' \land \neg e') \lor & (cook) \\
(\neg s \land c \land h \land \neg e \land \neg s' \land c' \land \neg h' \land \neg e') & (done)
\end{array}
$$

Note: the third row represents two transitions: $3 \to 1$ and $4 \to 1$.

LTL specification

- "necessarily, the oven's door eventually closes and, till there, the oven does not heat":

$$M \models \mathbf{A}(\neg heat\ \mathbf{U}\ close),$$

i.e.,

$$M \models \neg\mathbf{E}\neg(\neg heat\ \mathbf{U}\ close)$$

Tableau construction for $\psi = \neg(\neg \textit{heat}\ \mathbf{U}\ \textit{close})$

- $\varphi := \neg\psi = (\neg \textit{heat}\ \mathbf{U}\ \textit{close})$
- Tableaux expansion:
  $\psi = \neg(\neg \textit{heat}\ \mathbf{U}\ \textit{close}) = \neg(\textit{close} \vee (\neg \textit{heat} \wedge \mathbf{X}(\neg \textit{heat}\ \mathbf{U}\ \textit{close})))$
- $el(\psi) = el(\varphi) = \{\textit{heat}, \textit{close}, \mathbf{X}\varphi\}$ $(\{h, c, \mathbf{X}\varphi\})$
- States:

$$
\begin{array}{l}
1 := \{\neg h, c, \mathbf{X}\varphi\},\ 2 := \{h, c, \mathbf{X}\varphi\},\ 3 := \{\neg h, \neg c, \mathbf{X}\varphi\},\\
4 := \{h, c, \neg\mathbf{X}\varphi\},\ 5 := \{h, \neg c, \mathbf{X}\varphi\},\ 6 := \{\neg h, c, \neg\mathbf{X}\varphi\},\\
7 := \{\neg h, \neg c, \neg\mathbf{X}\varphi\},\ 8 := \{h, \neg c, \neg\mathbf{X}\varphi\}
\end{array}
$$

Tableau construction for $\psi = \neg(\neg heat\ \mathbf{U}\ close)$ [cont.]

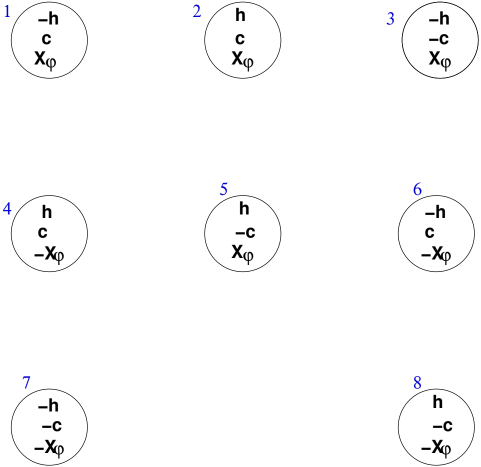


Tableau construction for $\psi = \neg(\neg heat\ \mathbf{U}\ close)$

- ...
- States:

$$1 := \{\neg h, c, \mathbf{X}\varphi\},\ 2 := \{h, c, \mathbf{X}\varphi\},\ 3 := \{\neg h, \neg c, \mathbf{X}\varphi\},$$
$$4 := \{h, c, \neg\mathbf{X}\varphi\},\ 5 := \{h, \neg c, \mathbf{X}\varphi\},\ 6 := \{\neg h, c, \neg\mathbf{X}\varphi\},$$
$$7 := \{\neg h, \neg c, \neg\mathbf{X}\varphi\},\ 8 := \{h, \neg c, \neg\mathbf{X}\varphi\}$$

- *sat*():

$$sat(h) = \{2, 4, 5, 8\} \implies sat(\neg h) = \{1, 3, 6, 7\},$$
$$sat(c) = \{1, 2, 4, 6\} \implies sat(\neg c) = \{3, 5, 7, 8\},$$
$$sat(\mathbf{X}\varphi) = \{1, 2, 3, 5\} \implies sat(\neg\mathbf{X}\varphi) = \{4, 6, 7, 8\},$$
$$sat(\varphi) = sat(c) \cup (sat(\neg h) \cap sat(\mathbf{X}(\neg h\ \mathbf{U}\ c))) = \{1, 2, 3, 4, 6\}$$
$$\implies sat(\psi) = sat(\neg\varphi) = \{5, 7, 8\}$$

Tableau construction for $\psi = \neg(\neg$*heat* **U** *close*$)$ [cont.]

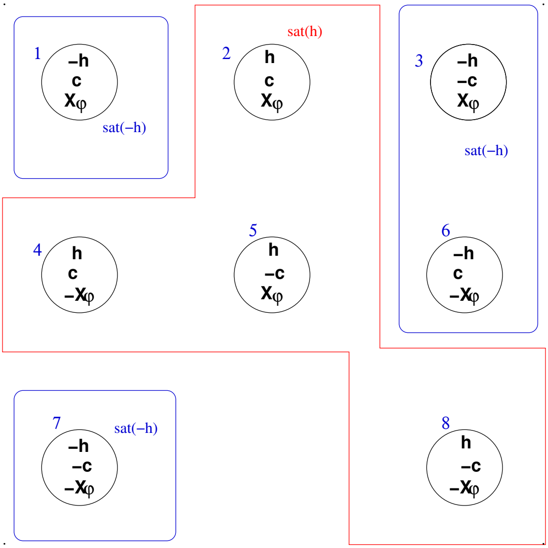


Tableau construction for $\psi = \neg(\neg heat\ \mathbf{U}\ close)$ [cont.]

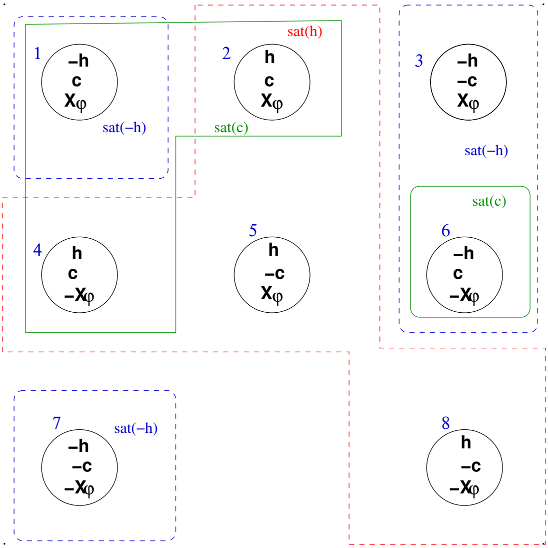


Tableau construction for $\psi = \neg(\neg heat \mathbf{U} close)$ [cont.]

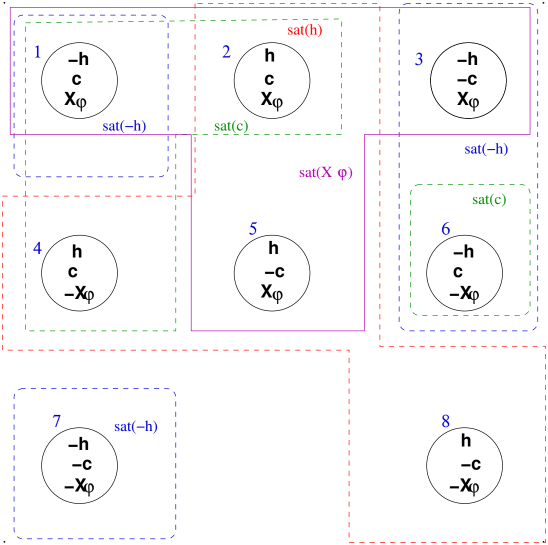


Tableau construction for $\psi = \neg(\neg heat\ \mathbf{U}\ close)$ [cont.]

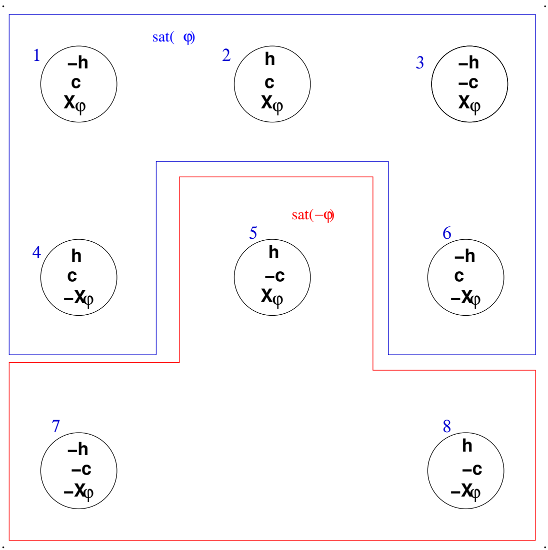


Tableau construction for $\psi = \neg(\neg heat \ \mathbf{U} \ close)$ [cont.]

- ...
- *sat*():

$$
\begin{array}{l}
sat(h) = \{2,4,5,8\} \implies sat(\neg h) = \{1,3,6,7\}, \\
sat(c) = \{1,2,4,6\} \implies sat(\neg c) = \{3,5,7,8\}, \\
sat(\mathbf{X}\varphi) = \{1,2,3,5\} \implies sat(\neg \mathbf{X}\varphi) = \{4,6,7,8\}, \\
sat(\varphi) = sat(c) \cup (sat(\neg h) \cap sat(\mathbf{X}(\neg h \ \mathbf{U} \ c))) = \{1,2,3,4,6\}
\end{array}
$$

- Initial states *I*: $sat(\psi) = sat(\neg\varphi) = \{5,7,8\}$
- Transition Relation *R*:
  - add an edge from every state in $sat(\mathbf{X}\varphi)$ to every state in $sat(\varphi)$
  - add an edge from every state in $sat(\neg\mathbf{X}\varphi)$ to every state in $sat(\neg\varphi)$

Tableau construction for $\psi = \neg(\neg$*heat* **U** *close*$)$ [cont.]

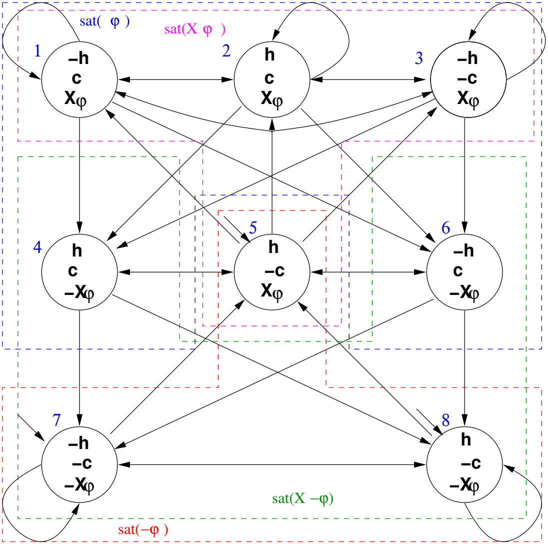
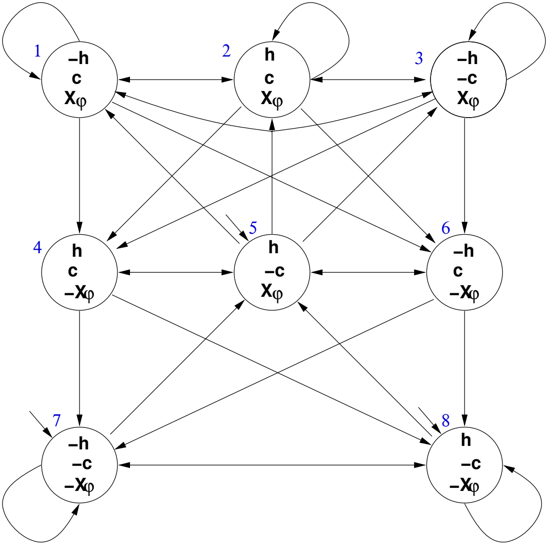


Tableau construction for $\psi = \neg(\neg$*heat* **U** *close*$)$ [cont.]



Problems with **U**-subformulas

- *R* does not guarantee that $\neg$*heat***U***close* is fulfilled
- Example: although state 3 belongs to *sat*($\neg$*heat***U***close*), the path which loops forever in 3 does not satisfy $\neg$*heat***U***close*, as close never holds in that path.
- We restrict the admissible paths of T_ψ to those which verify the fairness condition:

$$\{sat(\neg(\neg heat\ \mathbf{U} close) \vee close)\}$$

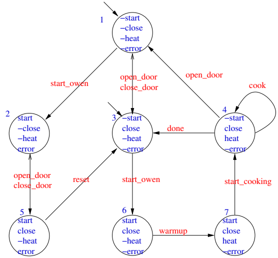
Remark

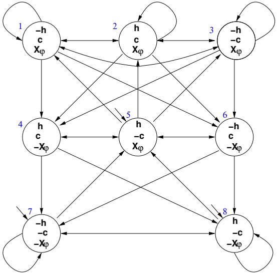
Alternatively, since ($\neg$*heat* **U***close*) occurs with negative polarity in ψ, here we can simply state the fairness condition "$\top$".

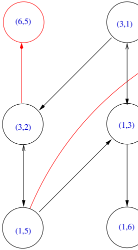
Symbolic representation of T_ψ, s.t. $\psi := \neg(\neg h \mathbf{U} c)$

- State variables: h, c and x and primed versions h', c' and x'
  [x is a Boolean label for $\mathbf{X}(\neg h \mathbf{U} c)$]
- Initial states: $I_{T_\psi} = sat(\psi)$
  $\Longrightarrow I(h, c, x) = \neg(c \vee (\neg h \wedge x))$
- Transition Relation: $R_{T_\psi} = \bigwedge_{\mathbf{X}\varphi_i \in el(\psi)} (sat(\mathbf{X}\varphi_i) \leftrightarrow sat'(\varphi_i))$
  $\Longrightarrow R_{T_\psi}(h, c, x, h', c', x') = x \leftrightarrow (c' \vee (\neg h' \wedge x'))$
- Fairness Property:
  $F_{T_\psi} := \{sat(\neg(\varphi_1 \mathbf{U} \varphi_2) \vee \varphi_2))\ s.t.\ (\varphi_1 \mathbf{U} \varphi_2)\ in\ \psi\}$
  $\Longrightarrow F_{T_\psi}(h, c, x) = \neg(c \vee (\neg h \wedge x)) \vee c = ... = h \vee \neg x \vee c$
- Alternative (due to negative polarity of $(\neg heat\ \mathbf{U} close)$ in ψ):
  $F_{T_\psi}(h, c, x) = \top$

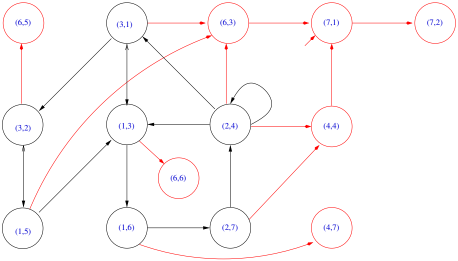
Product $P = T_\psi \times M$

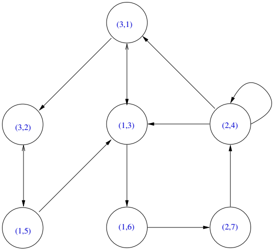






Product $P = T_\psi \times M$ [cont.]





- $P = T_\psi \times M$ (reachable states only)

Product $P = T_\psi \times M$: symbolic representation

- Initial states: $I(s,c,h,e,x) = (\neg s \wedge \neg h \wedge \neg e) \wedge \neg(c \vee (\neg h \wedge x)) = \neg s \wedge \neg h \wedge \neg e \wedge \neg c \wedge \neg x$
- Transition relation: $R(s,c,h,e,x,s',c',h',e',x') =$ (an OBDD for)

$$
\begin{array}{ll}
(x \leftrightarrow (c' \vee (\neg h' \wedge x'))) \wedge (& \\
(\ \neg s \wedge \neg c \wedge \neg h \wedge \neg e \wedge \neg s' \wedge c' \wedge \neg h' \wedge \neg e') \vee & (close\_door,\ no\ error) \\
(\ s \wedge \neg c \wedge \neg h \wedge e \wedge s' \wedge c' \wedge \neg h' \wedge e') \vee & (close\_door,\ error) \\
(\ \neg s \wedge c \wedge \neg e \wedge \neg s' \wedge \neg c' \wedge \neg h' \wedge \neg e') \vee & (open\_door,\ no\ error) \\
(\ s \wedge c \wedge \neg h \wedge e \wedge s' \wedge \neg c' \wedge \neg h' \wedge e') \vee & (open\_door,\ error) \\
(\ \neg s \wedge c \wedge \neg h \wedge \neg e \wedge s' \wedge c' \wedge \neg h' \wedge \neg e') \vee & (start\_oven,\ no\ error) \\
(\ \neg s \wedge \neg c \wedge \neg h \wedge \neg e \wedge s' \wedge \neg c' \wedge \neg h' \wedge e') \vee & (start\_oven,\ error) \\
(\ s \wedge c \wedge \neg h \wedge e \wedge \neg s' \wedge c' \wedge \neg h' \wedge \neg e') \vee & (reset) \\
(\ s \wedge c \wedge \neg h \wedge \neg e \wedge s' \wedge c' \wedge h' \wedge \neg e') \vee & (warmup) \\
(\ s \wedge c \wedge h \wedge \neg e \wedge \neg s' \wedge c' \wedge h' \wedge \neg e') \vee & (start\_cooking) \\
(\ \neg s \wedge c \wedge h \wedge \neg e \wedge \neg s' \wedge c' \wedge h' \wedge \neg e') \vee & (cook) \\
(\ \neg s \wedge c \wedge h \wedge \neg e \wedge \neg s' \wedge c' \wedge \neg h' \wedge \neg e') & (done) \\
) &
\end{array}
$$

[**EG** *true*]: symbolic representation

- Emerson-Lei returns (an OBDD equivalent to):

$$
\begin{array}{ll}
\mathbf{EG}\mathit{true} = & \\
(\neg s \wedge \neg c \wedge \neg h \wedge \neg e \wedge x) \vee & (3,1) \\
(s \wedge \neg c \wedge \neg h \wedge e \wedge x) \vee & (3,2) \\
(\neg s \wedge c \wedge \neg h \wedge \neg e \wedge x) \vee & (1,3) \\
(\neg s \wedge c \wedge h \wedge \neg e \wedge x) \vee & (2,4) \\
(s \wedge c \wedge \neg h \wedge e \wedge x) \vee & (1,5) \\
(s \wedge c \wedge \neg h \wedge \neg e \wedge x) \vee & (1,5) \\
(s \wedge c \wedge h \wedge \neg e \wedge x) \vee & (2,7) \\
\ldots & \text{(other unreachables states)}
\end{array}
$$

- Initial states: $I(s, c, h, e, x) = \neg s \wedge \neg h \wedge \neg e \wedge \neg c \wedge \neg x$

$\Longrightarrow$ $I(s, c, h, e, x) \not\models \mathbf{EG}\mathit{true}$

$\Longrightarrow$ $I \not\subseteq [\mathbf{EG}\mathit{true}]$

$\Longrightarrow$ $T_{\psi} \times M \not\models \mathbf{EG}\mathit{true}$

$\Longrightarrow$ Property verified!

The property verified is...

Ex: Symbolic LTL Model Checking

Given the following LTL formula: $\varphi \stackrel{\text{def}}{=} \neg((\mathbf{GF}p \wedge \mathbf{GF}q) \rightarrow \mathbf{GF}r)$

(*a*) Compute the Negative Normal Form of φ ($NNF(\varphi)$).

[Solution:

$$\begin{aligned} \varphi &\iff \neg((\mathbf{GF}p \wedge \mathbf{GF}q) \rightarrow \mathbf{GF}r) \\ &\iff \neg(\neg(\mathbf{GF}p \wedge \mathbf{GF}q) \vee \mathbf{GF}r) \\ &\iff (\mathbf{GF}p \wedge \mathbf{GF}q \wedge \neg\mathbf{GF}r) \\ &\iff (\mathbf{GF}p \wedge \mathbf{GF}q \wedge \mathbf{FG}\neg r) \iff NNF(\varphi) \end{aligned}$$

]

(*b*) Compute the set of elementary subformulas of φ.

[Solution: First write the formula in terms of **X** and **U**'s (write "$\mathbf{F}\psi$" for "$\top\mathbf{U}\psi$"):

$$\begin{aligned} \varphi &\iff \neg((\mathbf{GF}p \wedge \mathbf{GF}q) \rightarrow \mathbf{GF}r) \\ &\iff \neg((\neg\mathbf{F}\neg\mathbf{F}p \wedge \neg\mathbf{F}\neg\mathbf{F}q) \rightarrow \neg\mathbf{F}\neg\mathbf{F}r) \end{aligned}$$

$el(\mathbf{F}\neg\mathbf{F}p) = \{\mathbf{XF}\neg\mathbf{F}p\} \cup el(\neg\mathbf{F}p) = \{\mathbf{XF}\neg\mathbf{F}p\} \cup \{\mathbf{XF}p\} \cup el(p) = \{\mathbf{XF}\neg\mathbf{F}p, \mathbf{XF}p, p\}$.

Hence:

$$\begin{aligned} el(\varphi) &= el(\neg((\neg\mathbf{F}\neg\mathbf{F}p \wedge \neg\mathbf{F}\neg\mathbf{F}q) \rightarrow \neg\mathbf{F}\neg\mathbf{F}r)) \\ &= el(\mathbf{F}\neg\mathbf{F}p) \cup el(\mathbf{F}\neg\mathbf{F}q) \cup el(\mathbf{F}\neg\mathbf{F}r) \\ &= \{\mathbf{XF}\neg\mathbf{F}p, \mathbf{XF}p, p, \mathbf{XF}\neg\mathbf{F}q, \mathbf{XF}q, q, \mathbf{XF}\neg\mathbf{F}r, \mathbf{XF}r, r\} \end{aligned}$$

]

(*c*) What is the (maximum) number of states of a fair Kripke Model representing φ?

[Solution: By definition it is $2^{|el(\varphi)|} = 2^9 = 512$.]

Ex: Symbolic LTL Model Checking

Given the following LTL formula $\psi \stackrel{\text{def}}{=} \neg\mathbf{F}\neg p$, compute and draw the tableau $\mathcal{T}_\psi$ of ψ. [Solution:

(i) The set of elementary subformulas of ψ is $el(\psi) \stackrel{\text{def}}{=} \{p, \mathbf{XF}\neg p\}$. Hence, the set of states is

$$\{s_1 : (p, \neg\mathbf{XF}\neg p),\ s_2 : (p, \mathbf{XF}\neg p),\ s_3 : (\neg p, \neg\mathbf{XF}\neg p),\ s_4 : (\neg p, \mathbf{XF}\neg p)\}$$

(ii) The set of initial states of $\mathcal{T}_\psi$ is $sat(\psi) \stackrel{\text{def}}{=} S \setminus (sat(\neg p) \cup sat(\mathbf{XF}\neg p)) = \{s_1\}$.

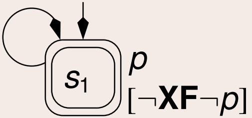
(iii) Since s_1 is the only state in $sat(\neg\mathbf{F}\neg p)$, then s_1 is the only successor of itself, so that the only relevant transition is a self-loop over s_1.
(One can also —un-necessarily— draw all transitions from states where $\neg\mathbf{XF}\neg p$ holds into $\{s_1\}$ and from from states where $\mathbf{XF}\neg p$ holds into $\{s_2, s_3, s_4\}$.)

(iv) There is one **U**-subformula, $\mathbf{F}\neg p$, so that there is one fairness condition defined as $sat(\neg\mathbf{F}\neg p \vee \neg p)$. Since $\mathbf{F}\neg p$ is false in s_1, then s_1 is part of the fairness condition.
[Alternatively: there is no positive **U**-subformula, so that we must add a $\mathbf{AGAF}\top$ fairness condition, which is equivalent to say that all states belong to the fairness condition.]

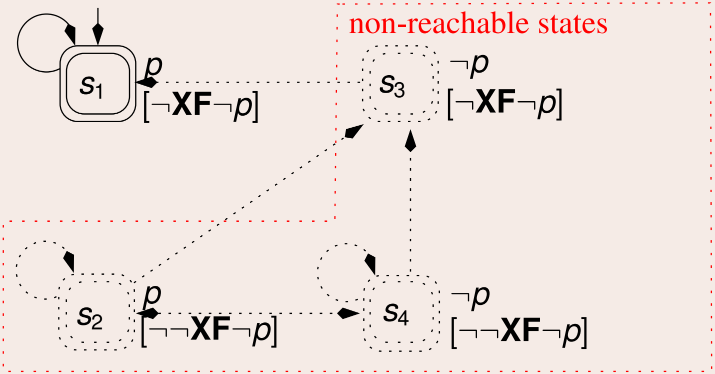
]

Ex: Symbolic LTL Model Checking (cont.)

[Solution:



or, alternatively without simplifications:



]

Ex: Symbolic LTL Model Checking

Given the following LTL formula $\psi \stackrel{\text{def}}{=} \mathbf{G}p$, compute and draw the tableau $\mathcal{T}_\psi$ of ψ.
[Without converting anything into $\mathbf{X}, \mathbf{U}$].

[Solution:

(i) The set of elementary subformulas of ψ is $el(\psi) \stackrel{\text{def}}{=} \{p, \mathbf{XG}p\}$. Hence, the set of states is

$$\{s_1 : (p, \mathbf{XG}p),\ s_2 : (p, \neg\mathbf{XG}p),\ s_3 : (\neg p, \mathbf{XG}p),\ s_4 : (\neg p, \neg\mathbf{XG}p)\}$$

(ii) The set of initial states of $\mathcal{T}_\psi$ is $sat(\psi) \stackrel{\text{def}}{=} sat(p) \cap sat(\mathbf{XG}p) = \{s_1\}$.

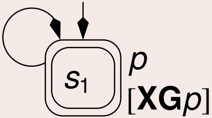
(iii) Since s_1 is the only state in $sat(\mathbf{G}p)$, then s_1 is the only successor of itself, so that the only relevant transition is a self-loop over s_1.
(One can also —un-necessarily— draw all transitions from states where $\mathbf{XG}p$ holds into $\{s_1\}$ and from from states where $\neg\mathbf{XG}p$ holds into $\{s_2, s_3, s_4\}$.)

(iv) Since there is no "$\mathbf{U}$" subformula, we must add a $\mathbf{AGAF}\top$ fairness condition, which is equivalent to say that all states belong to the fairness condition.

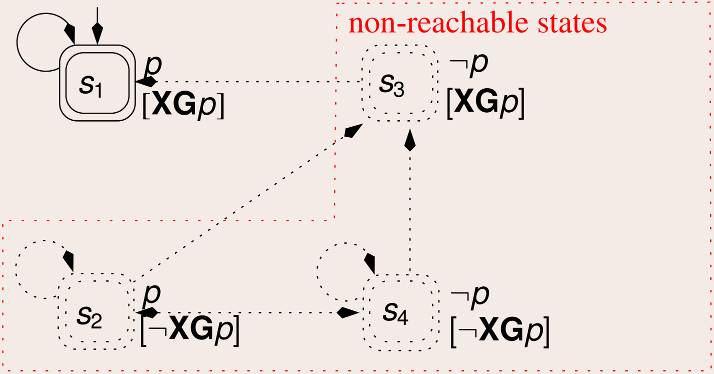
]

Ex: Symbolic LTL Model Checking (cont.)

[Solution:



or, alternatively without simplifications:



]