Home Page

Title Page

Page 1 of 23

Go Back

Full Screen

Close

Quit

Linear-time Temporal Logic

October 2005

S. Arun-Kumar

sak@cse.iitd.ernet.in

Department of Computer Science and Engineering

I. I. T. Delhi, Hauz Khas, New Delhi 110 016.

October 25, 2005

1. Linear-time Temporal Logic

Syntax & Semantics of LTL

$$\varphi ::= p \mid \neg\varphi \mid \varphi \wedge \varphi \mid \varphi \vee \varphi \mid X\varphi \mid \varphi \, U \varphi \mid F\varphi \mid G\varphi$$

$p \in AP$ the set of atomic propositions.

<u>Def</u>: For any LTL formula φ, the set $sub(\varphi)$ of <u>subformulas of φ</u> is defined by induction on the structure of φ as follows:

$sub(p) = \{p\}$ for every $p \in AP$.

$sub(o_1 \psi) = \{o_1 \psi\} \cup sub(\psi)$ for $o_1 \in \{\neg, X, F, G\}$

$sub(\psi \, o_2 \, \theta) = \{\psi \, o_2 \, \theta\} \cup sub(\psi) \cup sub(\theta)$ for $o_2 \in \{\wedge, \vee, U\}$.

<u>Semantics</u>: Given any sequence of states $\sigma = s_0 s_1 s_2 \ldots$ of a Kripke structure $\mathcal{K} = \langle S, R, I, \mathcal{L} \rangle$

$s_j \models p$ iff $p \in \mathcal{L}(s_j)$

$s_j \models \varphi \wedge \psi$ iff $s_j \models \varphi$ and $s_j \models \psi$

$s_j \models \varphi \vee \psi$ iff $s_j \models \varphi$ or $s_j \models \psi$

$s_j \models \neg\varphi$ iff $s_j \not\models \varphi$

$s_j \models X\varphi$ iff $s_{j+1} \models \varphi$

$s_j \models \varphi \, U \psi$ iff $\exists m \geq j : (\forall k : j \leq k < m : s_k \models \varphi) \wedge s_m \models \psi$

$s_j \models F\varphi$ iff $\exists m \geq j : s_m \models \varphi$

$s_j \models G\varphi$ iff $\forall m \geq j : s_m \models \varphi$.

$\boxed{\sigma \models \varphi \text{ iff } s_0 \models \varphi}$

<u>$\mathcal{K}$-Validity</u>: $\mathcal{K} \models \varphi$ iff $\forall \sigma : s_0 \in I : \sigma \models \varphi$

<u>Validity</u>: $\models \varphi$ iff $\forall \mathcal{K} : \mathcal{K} \models \varphi$.

Classification of formulas (α and β)

α	α_1	α_2
$\varphi \wedge \psi$	φ	ψ
$G\varphi$	φ	$XG\varphi$
$\neg F\varphi$	$\neg\varphi$	$\neg XF\varphi$
$\neg(\varphi U \psi)$	$\neg\psi$	$\neg(\varphi \wedge X(\varphi U \psi))$
$\neg(\varphi \vee \psi)$	$\neg\varphi$	$\neg\psi$

β	β_1	β_2
$\varphi \vee \psi$	φ	ψ
$F\varphi$	φ	$XF\varphi$
$\varphi U \psi$	ψ	$\varphi,\ X(\varphi U \psi)$
$\neg(\varphi \wedge \psi)$	$\neg\varphi$	$\neg\psi$
$\neg G\varphi$	$\neg\varphi$	$\neg XG\varphi$

Note:

$$G\varphi \Leftrightarrow \varphi \wedge XG\varphi$$
$$F\varphi \Leftrightarrow \varphi \vee XF\varphi$$
$$\varphi U \psi \Leftrightarrow \psi \vee (\varphi \wedge X(\varphi U \psi))$$

These unfoldings are used in determining $\alpha_1, \alpha_2, \beta_1, \beta_2$ respectively for the temporal operators.

Home Page

Title Page

Page 4 of 23

Go Back

Full Screen

Close

Quit

Satisfiability of an LTL formula

For any formula φ, the $Cl(\varphi)$ is the set of formulas which can influence the truth of φ.

Def. $Cl(\varphi)$ is the smallest set of formulas such that $\varphi \in Cl(\varphi)$ and

(i) $\neg\psi \in Cl(\varphi)$ iff $\psi \in Cl(\varphi)$

(ii) $\psi \hat{\vee} \theta \in Cl(\varphi) \Rightarrow \psi \in Cl(\varphi)$ and $\theta \in Cl(\varphi)$

(iii) $X\psi \in Cl(\varphi) \Rightarrow \psi \in Cl(\varphi)$

(iv) $\neg X\psi \in Cl(\varphi) \Rightarrow X\neg\psi \in Cl(\varphi)$

(v) $\psi U \theta \in Cl(\varphi) \Rightarrow \psi, \theta, X(\psi U \theta) \in Cl(\varphi)$

(vi) $G\theta \in Cl(\varphi) \Rightarrow \theta, X\theta \in Cl(\varphi)$

(vii) $F\theta \in Cl(\varphi) \Rightarrow \theta, X\theta \in Cl(\varphi)$

Claim: $|Cl(\varphi)| \leq 4|\varphi|$

$\vdash$ Each subformula with a temporal operator ~~or a binary op~~ contributes two formulas according to (v),(vi),(vii) and two negative formulas by (i). All other subformulas contribute ~~≤ 4 formulas~~ at most two formulas to the closure $\dashv$.

By (i) the set $Cl(\varphi)$ may be partitioned into two equal cardinality sets $Cl^+(\varphi)$ and $Cl^-(\varphi)$ where $Cl^-(\varphi)$ is the set of all formulas whose root operator is "$\neg$". $Cl^+(\varphi)$ ~~is~~ consists of all others.

$$Cl(\varphi) = Cl^+(\varphi) \cup Cl^-(\varphi).$$

Molecules over φ. A molecule over φ is a subset $A \subseteq Cl(\varphi)$ satisfying the following conditions

- $\bigwedge A$ is satisfiable — A does not contain both ψ and $\neg\psi$ for any $\psi \in Cl(\varphi)$
- $\psi \in A$ iff $\neg\psi \notin A$ — A is exhaustive. For every $\psi \in Cl(\varphi)$ either ψ or $\neg\psi$ is in A
- For every α formula ψ in $Cl(\varphi)$, both $\alpha_1(\psi)$ and $\alpha_2(\psi) \in A$ iff $\psi \in A$
- For every β formula ψ in $Cl(\varphi)$

$$\psi \in A \text{ iff } \beta_1(\psi) \in A \text{ or } \beta_2(\psi) \subseteq A$$

A molecule represents a collection of formulas that may hold simultaneously at some state in the model

A set $S \subseteq Cl(\varphi)$ is simultaneously satisfiable if there exists a sequence $\sigma = s_0 s_1 \ldots$ and a position j such that $s_j \models \psi$ for every $\psi \in S$ ~~$Cl(\varphi)$~~.

Proposition. For any set $S \subseteq Cl(\varphi)$ of simultaneously satisfiable formulas there exists a molecule A over φ with $S \subseteq A$.

$\vdash$ Let S be simultaneously satisfiable at s_j. Define

$$A = \{\psi \in Cl(\varphi) \mid s_j \models \psi\}.$$ Clearly $S \subseteq A$.

Claim: A is a molecule over φ. $\dashv$

Basic formulas. Rather than use the full closure we define the tableau states as consisting of some "basic" formulas.

Def. A formula is basic if it is either atomic or has the form $X\psi$.

The set of basic formulas of a formula φ is defined by induction on the structure of φ as follows:

(a) Let AP_φ be the set of atomic propositions occurring in φ. Then for any subformula ψ of φ

(b) $basic(p) = \{p\}$ if ~~$p \in AP_\varphi$~~ $\psi \equiv p$

$basic(\neg\psi) = basic(\psi)$

$basic(\psi \overset{\wedge}{\vee} \theta) = basic(\psi) \cup basic(\theta)$

$basic(X\psi) = \{X\psi\} \cup basic(\psi)$

$basic(\psi \, U \, \theta) = \{X(\psi U \theta)\} \cup basic(\psi) \cup basic(\theta)$

$basic(F\psi) = \{XF\psi\} \cup basic(\psi)$

$basic(G\psi) = \{XG\psi\} \cup basic(\psi)$

(c) Claim: Each operator of φ contributes at most one basic formula. Hence

$$\boxed{Cl(\varphi) \text{ contains } \leq |\varphi| \text{ basic formulas}}$$

Basic formulas. ~~Given any~~ formula is basic if it is either atomic or has the form $X\psi$

Claim: $Cl(\varphi)$ contains $\leq |\varphi|$ basic formulas. Since each subformula may contribute at most one basic formula.

$$\text{Basic}(\varphi \equiv Gp \wedge F\neg p)$$

$$= \{p, XGp, XF\neg p\}.$$

Basic formulas determine the molecule.

Given a collection B of basic formulas we build the molecule A as follows:

- For each basic ψ, $\psi \notin B \Rightarrow \neg\psi \in A$.
- If both $p, XGp \in B \Rightarrow Gp \in A$.
  else $\Rightarrow \neg Gp \in A$.
- If either $\neg p$ or $XF\neg p \in A \Rightarrow F\neg p \in A$.
  else $\Rightarrow \neg F \neg p \in A$.
- If either θ or (both ψ and $X(\psi U \theta)) \in A \Rightarrow \psi U \theta \in A$
  else $\Rightarrow \neg(\psi U \theta) \in A$.

Algorithm: Construction of a molecule.

- Let $\psi_1, \dots, \psi_m \in Cl^+(\varphi)$ be all the basic formulas
- Construct all 2^m combinations of $\{\overline{\psi_1}, \dots, \overline{\psi_m}\}$, where $\overline{\psi_i}$ is either ψ_i or $\neg\psi_i$ for $1 \le i \le m$.
- Complete each combination into a full molecule.

Algorithm Construction of the tableau

- The nodes of the tableau are the molecules of φ.
- Given molecules A, B $A \longrightarrow B$ provided ~~following connection requirements are satisfied~~.

either $X\psi \in A$ and $\psi \in B$.
or $\neg X\psi \in A$ and $\neg\psi \in B$

Since $Cl(\varphi)$ contains at most $|\varphi|$ basic formulas we have that the number of molecules over φ is determined by the number of different subsets of the $|\varphi|$ basic formulas and hence the tableau size is $\le 2^{|\varphi|}$ states.

To construct the tableau $\mathcal{T}_\varphi$

$$\mathcal{T}_\varphi = \langle S_\varphi, R_\varphi, \mathcal{L}_\varphi \rangle$$

where $S_\varphi = 2^{basic(\varphi)}$ is the set of states of the tableau.

For each subformula ψ of φ, we require to define the set of states that satisfy ψ.

$$sat(b) = \{ s \in S_\varphi \mid b \in s \} \text{ if } \psi \equiv b \in basic(\varphi)$$

$$sat(\neg\psi) = \{ s \in S_\varphi \mid s \notin sat(\psi) \}$$

$$sat(\psi \vee \theta) = sat(\psi) \cup sat(\theta)$$

$$sat(\psi \wedge \theta) = sat(\psi) \cap sat(\theta)$$

$$sat(\psi \,\mathsf{U}\, \theta) = sat(\theta) \cup (sat(\psi) \cap sat(\mathsf{X}(\psi \,\mathsf{U}\, \theta)))$$

$$sat(\mathsf{F}\psi) = sat(\psi) \cup sat(\mathsf{XF}\psi)$$

$$sat(\mathsf{G}\psi) = sat(\psi) \cap sat(\mathsf{XG}\psi)$$

The transition relation R_φ is defined by

(i) ~~such that~~ If $\mathsf{X}\psi \in s \in S_\varphi$ then all successors of s should satisfy ψ.

(ii) If $\mathsf{X}\psi \notin s \in S_\varphi$ then $\neg\mathsf{X}\psi \in s$ and hence no successor of s should satisfy ψ (which implies that every successor of s should satisfy $\neg\psi$)

Hence

$$\boxed{s \to s' \Leftrightarrow \bigwedge_{X\psi \in basic(\varphi)} s \in sat(X\psi) \Leftrightarrow s' \in sat(\psi)}$$

The labelling function $\mathcal{L}_\varphi$ is defined

$$\boxed{\mathcal{L}_\varphi(s) = \{ p \in s \mid p \in AP_\varphi \}}$$

However the definition of R_φ does not guarantee that eventuality properties are fulfilled. This is because a state with a formula of the form $XF\psi$ may loop forever (without ever reaching a state satisfying ψ). Hence we require the following additional condition

A ~~state~~ path $\sigma = s_0 s_1 \ldots$ with $s_0 \in sat(\varphi)$ will satisfy φ iff

- for every subformula $\psi U \theta$ and for every s_i,

  $s_i \in sat(\psi U \theta) \Rightarrow$ ~~$s_i \in sat(\theta) \vee$~~ $\exists j \geqslant i : s_j \in sat(\theta)$
- for every subformula $F\psi$ and for every s_i, $s_i \in sat(F\psi) \Rightarrow \exists j \geqslant i : s_j \in sat(\psi)$

Example 1. $\varphi \equiv Gp \wedge F\neg p$

$$Cl^{+}(\varphi) = \{ Gp \wedge F\neg p,\ Gp,\ F\neg p,\ p,\ XGp,\ XF\neg p \}$$

$$Cl^{-}(\varphi) = \{ \neg(Gp \wedge F\neg p),\ \neg Gp,\ \neg F\neg p,\ \neg p,\ \neg XGp,\ \neg XF\neg p \}.$$

$Basic(\varphi) = \{p, XGp, XF\neg p\}$. There are 2^3 combinations of the basic formulas

$B_0 = \{\}$, $B_1 = \{p\}$, $B_2 = \{XF\neg p\}$

$B_3 = \{p, XF\neg p\}$, $B_4 = \{XGp\}$

$B_5 = \{XGp, p\}$, $B_6 = \{XGp, XF\neg p\}$.

$B_7 = \{XGp, XF\neg p, p\}$.

Corresponding to these we have

$A_0 = \{\neg p, \neg XF\neg p, \neg XGp, \neg Gp, F\neg p, \neg\varphi\}$

$A_1 = \{p, \neg XF\neg p, \neg XGp, \neg Gp, \neg F\neg p, \neg\varphi\}$.

$A_2 = \{\neg p, \neg XGp, XF\neg p, \neg Gp, F\neg p, \neg\varphi\}$

$A_3 = \{p, \neg XGp, XF\neg p, \neg Gp, F\neg p, \neg\varphi\}$

$A_4 = \{\neg p, XGp, \neg XF\neg p, \neg Gp, F\neg p, \neg\varphi\}$

$A_5 = \{p, XGp, \neg XF\neg p, Gp, \neg F\neg p, \neg\varphi\}$.

$A_6 = \{\neg p, XGp, XF\neg p, \neg Gp, F\neg p, \neg\varphi\}$

Home Page

Title Page

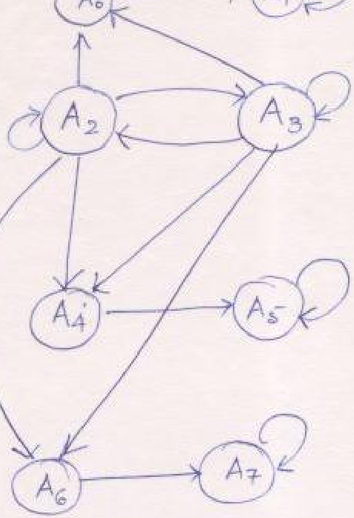
Page 12 of 23

Go Back

Full Screen

Close

Quit


A2
A3
A4
A5
A6
A7

Home Page

Title Page

Page 14 of 23

Go Back

Full Screen

Close

Quit

Sufficiency of the tableau. We need to show that corresponding to every path $\tau = t_0 t_1 \ldots$ in an arbitrary Kripke structure which satisfies the formula φ, there exists a path $\sigma = s_0 s_1 \cdots$ in $\mathcal{T}_\varphi$ such that $s_0 \models \varphi$ and the labels on each s_i are subsets of the labels on the corresponding t_i.

Notice that $\mathcal{K}$ and τ may satisfy many temporal formulas. However for each formula φ that τ satisfies $AP_\varphi \subseteq AP_\mathcal{K}$ where $AP_\mathcal{K}$ is the set of all atomic propositions used in describing the properties that $\mathcal{K}$ satisfies.

Def: $label(\tau) = \mathcal{L}_\mathcal{K}(t_0), \mathcal{L}_\mathcal{K}(t_1), \ldots$

$label(\sigma) = \mathcal{L}_\varphi(s_0), \mathcal{L}_\varphi(s_1), \ldots$

$label(\tau)\big|_{AP_\varphi} = \mathcal{L}_\mathcal{K}(t_0)\big|_{AP_\varphi}, \mathcal{L}_\mathcal{K}(t_1)\big|_{AP_\varphi}, \ldots$

where "$\big|_{AP_\varphi}$" denotes the restriction to the set AP_φ.

i.e. $\mathcal{L}_\mathcal{K}(t_i)\big|_{AP_\varphi} = \mathcal{L}_\mathcal{K}(t_i) \cap AP_\varphi$.

Def: For any φ let $sub(\varphi)$ denote the set of all subformulas of φ.

Def: For $\tau = t_0 t_1 \ldots$, $\quad \tau_i = t_i t_{i+1} \ldots$

Home Page

Title Page

Page 15 of 23

Go Back

Full Screen

Close

Quit

Lemma. Let $\mathcal{K}$ be a Kripke structure and τ a path in $\mathcal{K}$ ($\tau = t_0 t_1 \ldots$). Let φ be any formula. Let $S_i = \{\psi \mid \psi \in basic(\varphi) \text{ and } \tau_i \models \psi\}$. Then for all $\theta \in sub(\varphi) \cup basic(\varphi)$,

$$\boxed{\tau_i \models \theta \quad \text{iff} \quad S_i \in sat(\theta)}$$

where $sat(\theta)$ is the set of all states in $\mathcal{K}$ that satisfy θ.

$\vdash$ By induction on the structure of θ.

1. $\theta \in basic(\varphi)$. It follows by definition of S_i that

$$\tau_i \models \theta \quad \text{iff} \quad S_i \in sat(\theta).$$

2. $\left.\begin{array}{l} \theta \equiv \neg\theta_1 \\ \theta \equiv \theta_1 \wedge \theta_2 \\ \theta \equiv \theta_1 \vee \theta_2 \end{array}\right\}$ By the induction hypothesis and def of sat it follows.

3. $\theta \equiv \theta_1 \mathcal{U} \theta_2$. Clearly $\tau_i \models \theta$ iff $\tau_i \models \theta_2$ or ($\tau_i \models \theta_1$ and $\tau_i \models X(\theta_1 \mathcal{U} \theta_2)$). The rest follows by induction hypothesis and case 1. which includes all formulas of type $X(\ldots)$.

Go Back ●Full Screen ●Close ●Quit

<u>Lemma</u>. Let τ be a path in $\mathcal{K}$. Let s_i be the tableau state defined in the previous lemma for each s_i. Then $\sigma = s_0 s_1 \ldots$ is a path in T_φ.

$\vdash$ Clearly each $s_i \in S_\varphi$. By the previous lemma and the definition of X it is easy to show that for all $i \geq 0$

$$\left.\begin{array}{ll} & s_i \in sat(X\psi) \\ \text{iff} & \tau_i \models X\psi \\ \text{iff} & \tau_{i+1} \models \psi \\ \text{iff} & s_{i+1} \in sat(\psi) \end{array}\right\} \Rightarrow \quad s_i \rightarrow s_{i+1} \text{ in } T_\varphi \text{ for all } i \geq 0.$$

Hence σ is a path in T_φ.

<u>Theorem</u>. Let T_φ be a tableau for a formula φ. Then for every Kripke structure $\mathcal{K}$ and every infinite path τ in $\mathcal{K}$,

$\tau \models \varphi$ implies

there exists a path σ in T_φ with $s_0 \models \varphi$ such that $label(\tau)|_{AP_\varphi} = label(\sigma)$.

$\vdash$ By the previous lemma we can find a path σ in T_φ corresponding to each τ and by the first lemma $s_0 \models \varphi$. By the definition of s_i we have $\mathcal{L}(s_i) = \mathcal{L}(t_i)|_{AP}$ and hence $label(\tau)|_{AP_\varphi} = label(\sigma)$

While the tableau for a formula φ contains a path corresponding to every satisfying path in every Kripke structure, the tableau does contain paths which may not correspond to a satisfying paths in a Kripke structure. In other words the converse of the theorem may not hold.

Def: Let φ be a formula, $\mathcal{K}$ a Kripke structure with $\tau \models \varphi$. Let σ be the path in $\mathcal{T}_\varphi$ such that $label(\tau)\big|_{AP_\varphi} = label(\sigma)$. Then σ is the path induced by τ.

In the example the state A_7 has a self-loop. This implies a path $\sigma = A_7^\omega$. However $XF\neg p \in A_7$ even though the path σ never satisfies $F\neg p$.

In other words, the state A_7 "promises" the eventuality formula but σ "never fulfills" it.

Def: A formula $\psi \in Cl(\varphi)$ promises another formula θ if ψ is of one of the following forms:

$$F\theta, \quad \chi \cup \theta, \quad \neg G \neg \theta \quad \text{if } \cancel{\psi \in Cl^{+}(\varphi)}$$

and $\neg G \theta'$ if $\theta' \equiv \neg\theta$. ψ is called a promising formula

Note: In each of the above cases $\boxed{\psi \Rightarrow F\theta}$

Proposition. Let ψ promise θ. Then for any infinite path ~~$\sigma = s_0 s_1 s_2 \ldots$~~ ~~$\sigma$ in T_φ~~ $\tau = t_0 t_1 t_2 \cdots$ in a Kripke structure

$\tau \models \psi$ implies there are infinitely many positions $j \geq 0$ such that $t_j \models \neg\psi$ or $t_j \models \theta$.

Proof: Let $\tau \models \psi$ and suppose τ contains only finitely many positions satisfying $\neg\psi$ or θ. Then there must be only a finite number of positions satisfying $\neg\psi$. Hence (since σ is an infinite path) there must be an infinite number of positions satisfying ψ.

But ~~at~~ $\psi \Rightarrow F\theta$ since ψ promises θ. Hence for each of the infinite positions satisfying ψ there is a position that satisfies θ.

Claim: The number of positions satisfying θ is infinite.

$\vdash$ If the number of such positions were finite there must be a maximum position $m \geq 0$ such that $t_m \models \theta$ and for all $n > m$, $t_n \not\models \theta$. But this is impossible since there are positions $m' > m$ where ψ holds and hence there must be positions $n \geq m'$ where θ holds. $\dashv$

Def: Let ψ promise θ. A state $s \in \mathcal{T}_\varphi$ fulfills $\psi \in Cl(\varphi)$ if $s \models \neg\psi$ or $s \models \theta$. A path σ in $\mathcal{T}_\varphi$ with $\sigma = s_0 s_1 s_2 \ldots$ is fulfilling if $s_0 \models \varphi$ and σ contains infinitely many states that fulfill ψ.

Theorem. If σ is induced by a path $\tau \models \varphi$ then σ must be fulfilling.

$\vdash$ Let $\psi \in Cl(\varphi)$ and ψ promises θ. By the last proposition there are an infinite number of positions satisfying $\neg\psi$ or θ. Since σ is induced by τ, σ also has an infinite number of positions satisfying $\neg\psi$ or θ. Hence σ is fulfilling. $\dashv$

Theorem. If σ is a fulfilling path in $\mathcal{T}_\varphi$ then there exists a path τ in some (particular) Kripke structure such that τ induces σ.

$\vdash$ Let $\sigma = s_0 s_1 s_2 \ldots$ in $\mathcal{T}_\varphi$. Now construct the sequence τ Kripke structure $\mathcal{K}$ ensuring that

$\forall j: \forall p \in AP_\varphi: \; p \in s_j \Leftrightarrow p \in \mathcal{L}_\mathcal{K}(t_j)$

and using the conditions for connecting states to define the transition relations.

Home Page

Title Page

Page 20 of 23

Go Back

Full Screen

Close

Quit

Claim. For all $\psi \in Cl(\varphi)$

$$s_j \models \psi \quad \text{iff} \quad t_j \models \psi.$$

$\vdash$ By induction on the structure of ψ.
The basis viz. atomic propositions easily hold and further for compound propositions also therefore the ~~holds~~ claim holds. For the formulas ~~key~~ of the form $X\_$ the connection conditions ensure the truth of the claim. So we consider only the cases of other temporal formulae.

Case $\psi \equiv F\theta$. Assume that (IH) σ and τ both agree on θ. i.e. $s_j \models \theta$ iff $t_j \models \theta$ for all $j \geq 0$.

~~Now since σ is fulfilling it~~

($\Rightarrow$) Suppose $s_j \models \psi$. Since σ is fulfilling it contains infinitely many positions $k \geq j$ ~~such that~~ that fulfill ψ. Let k be the smallest index $\geq j$ such that ~~$s_k \models \psi$. If~~ s_k fulfills ψ. If $k = j$ then since $s_j \models F\theta$, $s_j \not\models \neg\psi$ and hence $s_j \models \theta$. If $k > j$ then s_{k-1} does not fulfill ψ and ~~must~~ which therefore ~~satisfy~~ $s_{k-1} \not\models \neg\psi$ and $s_{k-1} \not\models \theta$ implies $\underbrace{s_{k-1} \models \psi}_{\Downarrow}$ and $s_{k-1} \models \neg\theta$

$s_{k-1} \models F\theta \Rightarrow s_{k-1} \models XF\theta \Rightarrow \underbrace{s_k \models F\theta}_{s_k \models \psi}$

Since $s_k \models \psi$, the only way it can fulfill ψ is by allowing $s_k \models \theta$. Hence there exists $k \geq j$ such that ~~s_k~~ $s_k \models \theta$. By the induction hypothesis $t_k \models \theta$ which implies $t_k \models F\theta$ i.e. $t_k \models \psi$.

~~We may similarly argue about the other cases.~~

($\Leftarrow$) In the reverse direction, assume $t_j \models \psi$ but $s_j \not\models \psi$ i.e. $s_j \models \neg\psi$ i.e. $s_j \models \neg F\theta$. This implies for all $k \geq j$ $s_k \not\models \theta$ and $s_k \not\models F\theta$. This means $s_k \models \neg\theta$ and $s_k \models \neg F\theta$. By the induction hypothesis this implies $t_k \models \neg\theta$ for all $k \geq j$ which contradicts $t_j \models F\theta$. $\dashv$

The other cases may be similarly proven.

<u>Theorem</u>. φ is satisfiable iff $\mathcal{T}_\varphi$ contains a fulfilling path $\sigma = s_0 s_1 s_2 \ldots$ with $s_0 \models \varphi$.

$\vdash$ ($\Leftarrow$) Assume σ is a fulfilling path with $s_0 \models \varphi$. ~~By~~ There is a path τ in some Kripke structure which induces σ and such that $\tau \models \varphi$

($\Rightarrow$) Let $\tau \models \varphi$ in some Kripke structure. Then clearly τ induces a fulfilling path σ in $\mathcal{T}_\varphi$ with $\sigma \models \varphi$. $\dashv$

Remarks:

1. For any formula φ in LTL, it is clear that the two tableaus $\mathcal{T}_\varphi$ and $\mathcal{T}_{\neg\varphi}$ are the same. Depending upon whether we want to check the satisfiability of φ or $\neg\varphi$ the sets of initial ~~sets~~ states will be disjoint and partition $S_\varphi = S_{\neg\varphi}$ into two sets.

MODEL-CHECKING

2. φ is logically valid ($\models \varphi$) iff $\neg\varphi$ is unsatisfiable.

3. φ is valid over a Kripke-structure $\mathcal{K}$ ($\mathcal{K}$-validity or $\mathcal{K} \models \varphi$) iff φ holds for all sequences produced by $\mathcal{K}$.

4. φ is satisfiable over $\mathcal{K}$ iff there exists an ~~path~~ infinite path in $\mathcal{K}$ starting from an initial state of $\mathcal{K}$ in which φ holds.

5. $\mathcal{K} \models \varphi$ iff $\neg\varphi$ is unsatisfiable over $\mathcal{K}$.

> Hence an effective algorithm to check satisfiability over a "given $\mathcal{K}$" is necessary.

6. φ is not satisfiable over $\mathcal{K}$ if it is not satisfiable at all. Hence we require to ensure satisfiability along with satisfiability over $\mathcal{K}$.

The product construction

Given a formula φ and a Kripke structure $\mathcal{K} = \langle S_{\mathcal{K}}, R_{\mathcal{K}}, I_{\mathcal{K}}, \mathcal{L}_{\mathcal{K}} \rangle$ the product structure $\mathcal{P} = \langle S_{\mathcal{P}}, R_{\mathcal{P}}, I_{\mathcal{P}}, \mathcal{L}_{\mathcal{P}} \rangle$ is defined by

$$S_{\mathcal{P}} = \{ \langle s,t \rangle \in S_{\varphi} \times S_{\mathcal{K}} \mid \mathcal{L}_{\mathcal{K}}(t)|_{AP_{\varphi}} = \mathcal{L}_{\varphi}(s) \}.$$

$$R_{\mathcal{P}} = \{ \langle s,t \rangle \longrightarrow \langle s',t' \rangle \mid s \rightarrow s', t \rightarrow t' \}.$$

$$\mathcal{L}_{\mathcal{P}}(\langle s,t \rangle) = \mathcal{L}_{\varphi}(s).$$

Home Page
Title Page
Page 23 of 23
Go Back
Full Screen
Close
Quit
●Go Back ●Full Screen ●Close ●Quit