Syntax and Semantics of Propositional Linear Temporal Logic

Defining Logics

$\langle \mathcal{L}, \mathcal{M}, \models \rangle$

$\mathcal{L}$ - the language of the logic

$\mathcal{M}$ - a class of models

$\models$ - satisfaction relation

$M \in \mathcal{M}, \varphi \in \mathcal{L}$: $M \models \varphi$ is read as "M satisfies φ"

Typical additional parameters to $\models$:

$\mathcal{A}, a, b \models \varphi(x, y)$ a, b are values for x, y;

$M, w \models \varphi$ w is a reference possible world

etc.

Syntax of *LTL*

A vocabulary $\mathbf{L}$ of propositional variables $p, q, \ldots \in \mathbf{L}$

$\varphi ::=$	$\bot \mid \top \mid$	logical constants false and true
	$p \mid$	propositional variable
	$\neg\varphi \mid$	negation
	$(\varphi \vee \varphi) \mid (\varphi \wedge \varphi) \mid$	disjunction, conjunction
	$(\varphi \Rightarrow \varphi) \mid (\varphi \Leftrightarrow \varphi) \mid$	implication, equivalence
	$\circ\varphi \mid$	circle, "nexttime"
	$\Diamond\varphi \mid$	diamond, "now or sometimes in the future"
	$\Box\varphi \mid$	box, "now and always in the future"
	$(\varphi \mathrm{U} \varphi)$	until, $(p\mathrm{U}q)$ is read as "p until q"

$\varphi \in \mathbf{L}$ - "φ is a formula written in the vocabulary $\mathbf{L}$"

Binding strengh of LTL connectives

$$\varphi ::= \quad \bot \mid \top \mid p \mid \neg\varphi \mid (\varphi \vee \varphi) \mid (\varphi \wedge \varphi) \mid (\varphi \Rightarrow \varphi) \mid (\varphi \Leftrightarrow \varphi)$$
$$\circ\varphi \mid \Diamond\varphi \mid \Box\varphi \mid (\varphi \mathsf{U} \varphi)$$

The LTL connectives in decreasing order of their binding strength:

$\neg$, $\circ$, $\Diamond$, $\Box$

$\wedge$

$\vee$

$\Rightarrow$, $\Leftrightarrow$

(.U.) - we always write (and) around U.

Models and satisfaction

Vocabulary $\mathbf{L}$

$\sigma : \omega \rightarrow \mathcal{P}(\mathbf{L})$ an LTL model for $\mathbf{L}$

σ, $n < \omega$, $\varphi \in \mathbf{L}$

$\sigma, n \models \varphi$ - "φ is satisfied at position n of σ."

$$
\begin{array}{lll}
\sigma, n \not\models \bot & & \\
\sigma, n \models p & \text{if} & p \in \sigma_n \\
\sigma, n \models \varphi \Rightarrow \psi & \text{if} & \text{either } \sigma, n \not\models \varphi \text{ or } \sigma, n \models \psi \\
\sigma, n \models \circ\varphi & \text{if} & \sigma, n+1 \models \varphi \\
\sigma, n \models \Diamond\varphi & \text{if} & \sigma, n+i \models \varphi \text{ for some } i < \omega \\
\sigma, n \models \Box\varphi & \text{if} & \sigma, n+i \models \varphi \text{ for all } i < \omega \\
\sigma, n \models (\varphi \mathsf{U} \psi) & \text{if} & \text{there exists a } k < \omega \text{ such that} \\
 & & \sigma, n+i \models \varphi \text{ for all } i < k \text{ and } \sigma, n+k \models \psi
\end{array}
$$

On the form of $\models$

$\circ$, $\Diamond$, $\Box$ and (.U.) are future temporal operators:

$\sigma, n \models \circ\varphi$ $\sigma, n \models \Diamond\varphi$, etc. depend only on

$$\sigma|_{\{n,n+1,\ldots\}}.$$

Let $\sigma^{(i)}$ denote $\lambda j.\sigma_{i+j}$. Then

$$\sigma, i \models \varphi \text{ is equivalent to } \sigma^{(i)}, 0 \models \varphi.$$

Using the $\sigma^{(.)}$ notation, mentioning positions can be avoided:

$$\begin{array}{lll} \sigma \models \circ\varphi & \text{if} & \sigma^{(1)} \models \varphi \\ \ldots & & \\ \sigma \models (\varphi \mathsf{U} \psi) & \text{if} & \text{there exists a } k < \omega \text{ such that} \\ & & \sigma^{(i)} \models \varphi \text{ for all } i < k \text{ and } \sigma^{(k)} \models \psi \end{array}$$

Abbreviations

$\top$, $\neg$, $\wedge$, $\vee$ and $\Leftrightarrow$ abbreviate formulas built using just $\perp$ and $\Rightarrow$

$$\Diamond\varphi \rightleftharpoons (\top \mathsf{U} \varphi)$$

$$\Box\varphi \rightleftharpoons \neg\Diamond\neg\varphi$$

Conversely

$$\Diamond\varphi \rightleftharpoons \neg\Box\neg\varphi$$

To keep proofs by induction on the structure of formulas short, we take

$\perp$, $\Rightarrow$, $\circ$, and $(.\mathsf{U}.)$ as the basic connectives.

Validity in LTL

Definition 1 $\models_{LTL} \varphi$ if $\sigma, n \models \varphi$ for all models σ and all $n < \omega$

$\models_{LTL} \varphi$ is equivalent to $\models_{LTL} \Box\varphi$

$\models_{LTL} \varphi$ is equivalent to $\sigma, 0 \models \varphi$ for all models σ

Replacement of equivalents

φ and ψ are equivalent, if $\models_{LTL} \varphi \Leftrightarrow \psi$

Proposition 1 (replacement of equivalents) Let

$$\models_{LTL} \varphi_i \Leftrightarrow \psi_i, \qquad i = 1, \ldots, n.$$

Then

$$[\varphi_1/p_1, \ldots, \varphi_n/p_n]\chi \text{ is equivalent to } [\psi_1/p_1, \ldots, \psi_n/p_n]\chi.$$

Proof: Induction on the construction of χ. $\dashv$

Proposition 2 Let $\models_{LTL} \chi$. Then

$$\models_{LTL} [\varphi_1/p_1, \ldots, \varphi_n/p_n]\chi.$$

Exercises

Exercise 1 Prove the validity of the following formulas:

$\Diamond\varphi \Leftrightarrow (\top \mathsf{U} \varphi)$, $\Box\varphi \Leftrightarrow \neg\Diamond\neg\varphi$

$\neg \circ \varphi \Leftrightarrow \circ\neg\varphi$, $\circ(\varphi \vee \psi) \Leftrightarrow \circ\varphi \vee \circ\psi$, $\circ(\varphi \wedge \psi) \Leftrightarrow \circ\varphi \wedge \circ\psi$

$\Diamond(\varphi \vee \psi) \Leftrightarrow \Diamond\varphi \vee \Diamond\psi$, $\Box(\varphi \wedge \psi) \Leftrightarrow \Box\varphi \wedge \Box\psi$

$\Diamond\Diamond\varphi \Leftrightarrow \Diamond\varphi$, $\Box\Box\varphi \Leftrightarrow \Box\varphi$

$\circ(\varphi \Rightarrow \psi) \Rightarrow (\circ\varphi \Rightarrow \circ\psi)$, $\Box(\varphi \Rightarrow \psi) \Rightarrow (\Box\varphi \Rightarrow \Box\psi)$

$\Box\varphi \Rightarrow \varphi \wedge \circ\Box\varphi$

$\Box(\varphi \Rightarrow \circ\varphi) \Rightarrow (\varphi \Rightarrow \Box\varphi)$

$(\varphi \mathsf{U} \psi) \Leftrightarrow \psi \vee (\varphi \wedge \circ(\varphi \mathsf{U} \psi))$

Exercises

Exercise 2 Let φ, ψ_i, χ_i, $i = 1, \ldots, n$, be arbitrary formulas. Prove that

$$\models_{LTL} \bigwedge_{i=1}^{n} \Box(\psi_i \Leftrightarrow \chi_i) \Rightarrow ([\psi_1/p_1, \ldots, \psi_n/p_n]\varphi \Leftrightarrow [\chi_1/p_1, \ldots, \chi_n/p_n]\varphi).$$

Exercises

Consider the derived operators (.W.) and (.R.):

$$(\varphi \mathsf{W} \psi) \rightleftharpoons (\varphi \mathsf{U} \psi) \vee \Box\varphi, \qquad (\varphi \mathsf{R} \psi) \rightleftharpoons (\varphi \mathsf{U}(\psi \wedge \varphi)).$$

Exercise 3 Write clauses that define $\models$ for formulas built using (.W.) and (.R.). The clauses should not refer to the meaning of $\models$ for other temporal operators.

Exercise 4 Show that (.U.) can be regarded as an abbreviation in systems of LTL with (.W.) or (.R.) as a basic temporal operator instead of (.U.).

Exercise 5 Prove that, using (.W.) along with (.U.), every LTL formula can be transformed into an equivalent one in which $\neg$ occurs only immediately before propositional variables.

Exercises

Definition 2 The formulas $\alpha_1, \ldots, \alpha_n$ form a full system if $\models \neg(\alpha_i \wedge \alpha_j)$ for $1 \leq i < j \leq n$ and $\models \bigvee_{i=1}^{n} \alpha_i$.

Exercise 6 Prove that every LTL formula has an equivalent one of the form

$$\bigvee_i \alpha_i \wedge \circ\beta_i,$$

where α_i are purely propositional and form a full system. No restrictions are imposed on the form of the β_is.

A clausal normal form for LTL

First proposed by Michael Fisher; useful in proof by temporal resolution:

$$\xi \wedge \Box \bigwedge_i (\pi_i \Rightarrow \varphi_i)$$

ξ - purely propositional

π_i - conjunctions of possibly negated propositional variables

φ_i - disjunctions of p, $\circ p$ and $\Diamond p$.

Definition 3 Given vocabularies $\mathbf{L}$ and $\mathbf{L}'$, $\mathbf{L} \subseteq \mathbf{L}'$, model σ' for $\mathbf{L}'$ extends model σ for $\mathbf{L}$ if

$$\sigma'(i) \cap \mathbf{L} = \sigma(i) \text{ for all } i < \omega.$$

Theorem 1 For every formula φ there exists a formula ψ in the normal form s. t. $\mathrm{Var}(\varphi) \subseteq \mathrm{Var}(\psi)$ and every linear model σ for the vocabulary $\mathrm{Var}(\varphi)$ such that $\sigma, 0 \models \varphi$ can be uniquely extended to a model for $\mathrm{Var}(\psi)$ such that $\sigma', 0 \models \psi$.

A clausal normal form for LTL - the proof

Add fresh p and use the transformations

$$[\circ\alpha/p]\varphi \rightarrow \varphi \wedge \Box(p \Leftrightarrow \circ\alpha) \text{ and } [(\alpha \mathsf{U} \beta)/p]\varphi \rightarrow \varphi \wedge \Box(p \Leftrightarrow (\alpha \mathsf{U} \beta))$$

bottom up to eliminate nested $\circ$ and $(.\mathsf{U}.)$ and reach

$$\xi \wedge \Box \bigwedge_i (p_i \Leftrightarrow \eta_i)$$

with η_i being $(.\mathsf{U}.)$- and $\circ$-formulas with propositional operands.

A clausal normal form for LTL - the proof

$$p \Leftrightarrow (\alpha \mathsf{U} \beta) \text{ is equivalent to } p \Leftrightarrow (\beta \vee (\alpha \wedge \circ p)) \wedge \Diamond\beta,$$

which is in turn equivalent to

$$(p \Rightarrow \beta \vee \alpha) \wedge (p \Rightarrow \beta \vee \circ p) \wedge p \Rightarrow \Diamond\beta) \wedge (\beta \Rightarrow p) \wedge (\alpha \wedge \circ p \Rightarrow p \vee \Box\neg\beta).$$

To eliminate $\Box\neg\beta$, we replace

$$(\alpha \wedge \circ p \Rightarrow p \vee \Box\neg\beta) \text{ by } (\alpha \wedge \circ p \Rightarrow p \vee q) \wedge (q \Leftrightarrow \neg\beta \wedge \circ q).$$

Exercise 7 Find the normal form conjunctive members for $p \Leftrightarrow \circ\alpha$.

Since fresh propositional variables p are only added in defining clauses of the form $\Box(p \Leftrightarrow \ldots)$, extended satisfying models are determined uniquely.

The expressive power of just $\circ$ and $\Diamond$

Restrict the syntax to

$$\varphi ::= \bot \mid p \mid \varphi \Rightarrow \varphi \mid \circ\varphi \mid \Diamond\varphi$$

Exercise 8 Prove that every formula with the above syntax can be transformed into an equivalent one with no occurrences of $\bot$, $\Rightarrow$ or $\Diamond$ in the scope of $\circ$.

Hence we can restrict the syntax to

$\varphi ::= \bot \mid \psi \mid \varphi \Rightarrow \varphi \mid \circ\varphi \mid \Diamond\varphi$

$\psi ::= p \mid \circ\psi$

without (further) loss of expressive power.

Just $\circ$ and $\diamond$ concluded

Let $\mathbf{L} = \{p, q\}$, $n < \omega$. Consider

$$\sigma = \underbrace{\{p\} \ldots \{p\}}_{2n-1 \text{ times}}\{p,q\}\left(\underbrace{\{p\} \ldots \{p\}}_{n-1 \text{ times}}\emptyset\underbrace{\{p\} \ldots \{p\}}_{n-1 \text{ times}}\{p,q\}\right)^{\omega}$$

Proposition 3 Let φ have less than $n-1$ occurrences of $\circ$. Then

$\sigma, 0 \models \varphi$ iff $\sigma, 2n \models \varphi$.

Exercise 9 Prove the above proposition.

However,

$\sigma, 0 \models (p\mathsf{U}q)$ whereas $\sigma, 2n \not\models (p\mathsf{U}q)$.

Kripke models for LTL. Model-checking LTL properties
Decidability and the small model property for LTL

Systems with multiple behaviours

Linear LTL models $\sigma : \omega \to \mathcal{P}(\mathbf{L})$ encode individual behaviours.

Systems can have many behaviours. Possible reasons for non-determinism:

1. The system receives data from the envirnoment.
2. The system is part of some bigger system, but is being modelled separately. Without the complementing behaviour of the other parts, the behaviour of the considered part remains underspecified.
3. The system is obtained by abstraction (simplification) of a more complex system in order to become tractable. Parts of its state which are involved in making choices for its behaviour have been abstracted away.

Kripke models

Kripke frame: $\langle W, R, I \rangle$

$W \neq \emptyset$ - a set of states (possible worlds)

$R \subseteq W \times W$ - a transition relation

$I \subseteq W$, $I \neq \emptyset$ - a set of initial states

We require R to be serial: $\forall w' \exists w'' R(w', w'')$.

Kripke model for a vocabulary $\mathbf{L}$: $\langle W, R, I, V \rangle$

W, R and I as in Kripke frames

$V : W \to \mathcal{P}(\mathbf{L})$ - a valuation of the variables from $\mathbf{L}$.

A linear model σ can be viewed as the Kripke model

$$\langle \omega, \prec, \{0\}, \sigma \rangle$$

Behaviours in Kripke models

$M = \langle W, R, I, V \rangle$ - a Kripke model for $\mathbf{L}$.

$s = s_0 s_1 \dots s_n \dots \in W^\omega$ is a behaviour in M, if

$$s_0 \in I \text{ and } R(s_i, s_{i+1}) \text{ for all } i < \omega.$$

A linear LTL model σ_s corresponding to s:

$(\sigma_s)_i = V(s_i)$ for all $i < \omega$.

Definition 4 φ is satisfiable in M if M has a behaviour s s.t. $\sigma_s, 0 \models \varphi$.

If M is clear from the context, we write

$$s, k \models \dots \text{ instead of } \sigma_s, k \models \dots.$$

Overview of the model-checking algorithm

In a linear model σ we have the mapping $i \to \{\varphi \in \mathbf{L} : \sigma, i \models \varphi\}$

No mapping of the form $w \to \{\varphi \in \mathbf{L} : M, w \models \varphi\}$ is possible for Kripke models.

$w \to \{\psi : M, s \models \psi$ for s which start at $w\}$ is impossible too:

$\psi = \circ p$, wRw_0, wRw_1, $p \in V(w_0)$, $p \notin V(w_1)$.

Solution:

Let $\mathrm{Cl}(\varphi)$ be the formulas "relevant" to calculating φ. $\mathrm{Cl}(\varphi)$ includes $\mathrm{Subf}(\varphi)$ and some other formulas.

"Expand" M to a bigger model M_φ where:

the same behaviours as in M can be observed;

all s starting at $w = s_0$ satisfy the same $\circ$-formulas from $\mathrm{Cl}(\varphi)$.

$\mathrm{Cl}(.)$ - **the Fischer-Ladner closure in** LTL

Γ - a finite set of LTL formulas.

The Fischer-Ladner closure of Γ, written $\mathrm{Cl}(\Gamma)$, is the least Δ s.t.

$\Gamma \subseteq \Delta$;

$\varphi \Rightarrow \psi \in \Delta \to \varphi, \psi \in \Delta$;

$\varphi \in \Delta \to \varphi \Rightarrow \bot \in \Delta$, unless φ is a negation itself;

$\circ\varphi \in \Delta \to \varphi \in \Delta$;

$(\varphi \mathsf{U} \psi) \in \Delta \to \varphi, \psi, \circ(\varphi \mathsf{U} \psi) \in \Delta$.

We abbreviate $\mathrm{Cl}(\{\varphi\})$ to $\mathrm{Cl}(\varphi)$.

Fischer-Ladner closure in LTL

Proposition 4 $|\mathrm{Cl}(\varphi)| \leq 4|\varphi|$.

Proof:

$\mathrm{Subf}(\varphi)$ - the subformulas of φ, including φ itself.

$|\mathrm{Subf}(\varphi)| \leq |\varphi|$.

Let

$$\Phi_0 = \mathrm{Subf}(\varphi) \cup \{\circ(\psi \mathsf{U} \chi) : (\psi \mathsf{U} \chi) \in \mathrm{Subf}(\varphi)\}.$$

Then

$$\mathrm{Cl}(\varphi) = \Phi_0 \cup \{\neg\psi : \psi \in \Phi_0, \psi \text{ is not a negation itself}\}.$$

$\dashv$

Corollary 1 If Γ is a finite set of formulas, then $\mathrm{Cl}(\Gamma)$ is finite too.

The model M_φ: atoms

We fix $\mathbf{L}$, φ, $M = \langle W, R, I, V \rangle$ for $\mathbf{L}$. We assume $\mathbf{L} = \mathrm{Var}(\varphi)$.

Atom - $\langle w, \Delta \rangle \in W \times \mathcal{P}(\mathrm{Cl}(\varphi))$:

$\Delta \cap \mathbf{L} = V(w)$; $\quad \bot \notin \Delta$;

$\psi \Rightarrow \chi \in \Delta$ iff either $\psi \notin \Delta$ or $\chi \in \Delta$;

$(\psi \mathsf{U} \chi) \in \Delta$ iff either $\chi \in \Delta$ or $\psi, \circ(\psi \mathsf{U} \chi) \in \Delta$.

Δ is a maximal subset of $\mathrm{Cl}(\varphi)$ which is appoximately consistent wrt temporal operators and agrees with w on atomic propositions.

Exercises on atoms

$M = \langle W, R, I, V \rangle$

Atom - $\langle w, \Delta \rangle \in W \times \mathcal{P}(\mathrm{Cl}(\varphi))$:

$\Delta \cap \mathbf{L} = V(w)$; $\qquad \bot \notin \Delta$;

$\psi \Rightarrow \chi \in \Delta$ iff either $\psi \notin \Delta$ or $\chi \in \Delta$;

$(\psi \mathsf{U} \chi) \in \Delta$ iff either $\chi \in \Delta$ or $\psi, \circ(\psi \mathsf{U} \chi) \in \Delta$.

Exercise 10 Let s be a behaviour in M and $i < \omega$. Prove that $\langle s_i, \{\psi \in \mathrm{Cl}(\varphi) : \sigma_s, i \models \psi\} \rangle$ is an atom.

Exercise 11 Let $\langle w', \Delta' \rangle$ and $\langle w'', \Delta'' \rangle$ be atoms. Prove that if $w' = w''$ and Δ' and Δ'' contain the same formulas of the form $\circ\psi$, then $\Delta' = \Delta''$, that is, the two atoms are the same.

The model M_φ: initial approximation M_φ^0

$M_\varphi^0 = \langle W_\varphi^0, R_\varphi^0, I_\varphi^0, V_\varphi^0 \rangle$ for $\mathbf{L}$.

W_φ^0 consists of all the atoms;

$V_\varphi^0(\langle w, \Delta \rangle) = V(w)$ for all $\langle w, \Delta \rangle \in W_\varphi^0$;

$I_\varphi^0 = \{\langle w, \Delta \rangle \in W_\varphi^0 : w \in I\}$;

$\langle w', \Delta' \rangle R_\varphi^0 \langle w'', \Delta'' \rangle$ iff $w' R w''$ and $\{\varphi : \circ\varphi \in \Delta'\} \subseteq \Delta''$.

R_φ^0 is not guaranteed to be serial:

$$(\forall x \in W_\varphi^0)(\exists y \in W_\varphi^0) R_\varphi^0(x, y),$$

This is so because, if, e.g., $\circ p, \circ\neg p \in \Delta$, then obviously $\langle w, \Delta \rangle$ has no R_φ^0-successor.

The model M_φ

$M^0_\varphi = \langle W_\varphi, R_\varphi, I_\varphi, V_\varphi \rangle$

W_φ - the greatest subset of W^0_φ s.t.

$$(\forall x \in W_\varphi)(\exists y \in W_\varphi) R^0_\varphi(x, y).$$

W_φ is obtained from W^0_φ by removing the states with no R^0_φ-successor.

Exercise 12 Prove that it is impossible to get all the states removed from W^0_φ this way. Hint: states of the form $\langle s_i, \{\psi \in \mathrm{Cl}(\varphi) : \sigma_s, i \models \psi\}\rangle$ where s is a behaviour in M and $i < \omega$ cannot be removed this way.

$$V_\varphi = V^0_\varphi|_{W_\varphi}, \qquad I_\varphi = I^0_\varphi \cap W_\varphi, \qquad R_\varphi = R^0_\varphi \cap W_\varphi \times W_\varphi.$$

Proposition 5 $|W_\varphi| \leq |W^0_\varphi| \leq 2^{|\mathrm{Cl}(\varphi)|}|W|$.

Exercise 13 Give a more accurate upper bound for $|W_\varphi|$ using Exercise 11.

The correspondence between M and M_φ

Proposition 6 Let s be a behaviour in M. Let

$$\Delta_i = \{\psi \in \mathrm{Cl}(\varphi) : \sigma_s, i \models \psi\},\ i < \omega.$$

Then $\langle s_0, \Delta_0\rangle\langle s_1, \Delta_1\rangle \dots \langle s_n, \Delta_n\rangle \dots$

is a behaviour in M_φ and

$$\sigma_s, i \models \psi \text{ is equivalent to } \langle s_0, \Delta_0\rangle\langle s_1, \Delta_1\rangle \dots \langle s_n, \Delta_n\rangle \dots, i \models \psi$$

for all $\psi \in \mathrm{Cl}(\varphi)$ and all $i < \omega$.

Furthermore, for all $i < \omega$,

$$\text{if } (\psi \mathsf{U} \chi) \in \Delta_i, \text{ then there exists a } j < \omega \text{ such that } \chi \in \Delta_{i+j}.$$

Proof: Direct check. $\dashv$

The correspondence between M and M_φ

Proposition 7 Let $\langle s_0, \Delta_0\rangle\langle s_1, \Delta_1\rangle \ldots \langle s_n, \Delta_n\rangle \ldots$

be a behaviour in M_φ and let

$$\text{if } (\psi \mathsf{U} \chi) \in \Delta_i, \text{ then there exists a } j < \omega \text{ such that } \chi \in \Delta_{i+j}. \tag{1}$$

hold for all $i < \omega$. Then s is a behaviour in M, and for all $i \in \omega$ and $\psi \in \mathrm{Cl}(\varphi)$, $\psi \in \Delta_i$ is equivalent to both

$$s, i \models \psi \text{ and } \langle s_0, \Delta_0\rangle\langle s_1, \Delta_1\rangle \ldots \langle s_n, \Delta_n\rangle \ldots, i \models \psi.$$

Proof: Direct check by induction on the construction of φ. $\dashv$

Summary: Behaviours in M correspond to behaviours in M_φ which satisfy the condition (1).

Strongly connected components (SCC) in Kripke models

$M = \langle W, R, I, V \rangle$, R^* - the reflexive and transitive closure of R.

$W' \subseteq W$ is a strongly connected component (SCC), if $W' \times W' \subseteq R^*$.

Proposition 8 Let $|W| < \omega$ and let s be a behaviour in M. Then there exists an $i < \omega$ such that $\{s_{i+j} : j < \omega\}$ is an SCC.

Proposition 9 Let $W' \subseteq W_\varphi$ be an SCC in M_φ s. t. for all $\langle w, \Delta \rangle \in W'$ and all $(\psi \mathsf{U} \chi) \in \mathrm{Cl}(\varphi)$

$$\langle w, \Delta \rangle \in W' \text{ and } (\psi \mathsf{U} \chi) \in \Delta, \text{ imply } \chi \in \Delta' \text{ for some } \langle w', \Delta' \rangle \in W'.$$

Let $\langle w_0, \Delta_0 \rangle \ldots \langle w_k, \Delta_k \rangle$ be a behaviour prefix in M_φ, $\varphi \in \Delta_0$ and $\langle w_k, \Delta_k \rangle \in W'$.

Then φ is satisfiable at M. A satisfying behaviour for φ in M can be obtained by concatenating $w_0 \ldots w_k$ with any loop in R_φ that goes through all the members of W'.

Strongly connected components (SCC) in Kripke models

Conversely, if s is a behaviour in M, then the corresponding behaviour

$$\langle s_0, \Delta_0\rangle\langle s_1, \Delta_1\rangle \ldots \langle s_n, \Delta_n\rangle \ldots$$

in M_φ can be partitioned into a finite prefix

$$\langle s_0, \Delta_0\rangle\langle s_1, \Delta_1\rangle \ldots \langle s_j, \Delta_j\rangle$$

and an SCC

$$W' = \{\langle s_i, \Delta_i\rangle : j \leq i\}$$

which satisfies the condition

$$\langle w, \Delta\rangle \in W' \text{ and } (\psi \mathsf{U} \chi) \in \Delta, \text{ imply } \chi \in \Delta' \text{ for some } \langle w', \Delta'\rangle \in W'$$

for all $\langle w, \Delta\rangle \in W'$ and all $(\psi \mathsf{U} \chi) \in \mathrm{Cl}(\varphi)$.

The size of M_φ

N_φ - the number of the sets $\Delta \subseteq \mathrm{Cl}(\varphi)$ s.t. $\langle w, \Delta \rangle$ is an atom for some $w \in W$.

M_φ has at most $N_\varphi |W|$ states.

A Δ contains either ψ or an equivalent to $\neg\psi$ for every $\psi \in \mathrm{Cl}(\varphi)$.

Hence, since $|\mathrm{Cl}(\varphi)| \leq 4|\varphi|$, $N_\varphi \leq 2^{2|\varphi|}$.

Consequently,

$$|W_\varphi| \leq 2^{2|\varphi|}|W|.$$

The small (finite) model property for LTL: Synopsis

Satisfiability of LTL formulas without regard of a particular model.

If an LTL formula is satisfiable at all, then it is satisfiable at a finite Kripke model of size that is exponential in the length of the formula.

LTL is satisfiable iff it is satisfiable at a linear model in which, from a certain state on, the same finite sequence of states is repeated infinitely many times.

The equivalence between satisfiability of individual formulas in general and in finite models is known as the small (finite) model property in modal logic.

We first show that if a formula φ is satisfiable, then it is satisfiable in a concrete model which is built using the vocabulary of the formula $\mathrm{Var}(\varphi)$.

Simulations

$M_i = \langle W_i, R_i, I_i, V_i \rangle$, $i = 1, 2$ - Kripke models for the same $\mathbf{L}$.

$S \subseteq W_1 \times W_2$ is a simulation of M_1 into M_2 if:

for every $w_1 \in W_1$ there exists a $w_2 \in W_2$ such that $w_1 S w_2$;

if $w_1 S w_2$, then $V_1(w_1) = V_2(w_2)$;

if $w_1 S w_2$ and $w_1 \in I_1$, then $w_2 \in I_2$;

if $w_1 S w_2$ and $w_1 R_1 w_1'$, then there is a $w_2' \in W_2$ s.t. $w_2 R_2 w_2'$ and $w_1' S w_2'$.

Proposition 10 Let S be a simulation of M_1 into M_2 and let $\varphi \in \mathbf{L}$ be satisfiable in M_1. Then it is satisfiable in M_2 too.

Proof: Let $\sigma_s, 0 \models \varphi$ in M_1. We construct $s' \in W_2^\omega$:

$$s_0' \in S(s_0); \qquad s_{i+1}' \in S(s_{i+1}) \cap R_2(s_i').$$

A direct check shows that $\sigma_{s'}, 0 \models \varphi$. $\dashv$

Bisimulations

$M_i = \langle W_i, R_i, I_i, V_i \rangle$, $i = 1, 2$, - Kripke models for the same $\mathbf{L}$.

S is a bisimulation between M_1 and M_2, if

S is a simulation of M_1 into M_2 and

S^{-1} is a simulation of M_2 into M_1.

M_1 and M_2 which have a bisimulation are called bisimilar.

Corollary 2 Bisimilar models satisfy the same formulas.

The model $M_{\mathbf{L}}$

Fix a vocabulary $\mathbf{L}$

$M_{\mathbf{L}} = \langle W_{\mathbf{L}}, R_{\mathbf{L}}, I_{\mathbf{L}}, V_{\mathbf{L}} \rangle$ - a Kripke model for $\mathbf{L}$:

$W_{\mathbf{L}} = \mathcal{P}(\mathbf{L})$

$V_{\mathbf{L}}(s) = s$ for all $s \in W_{\mathbf{L}}$

$R_{\mathbf{L}} = W_{\mathbf{L}} \times W_{\mathbf{L}}$

$I_{\mathbf{L}} = W_{\mathbf{L}}$

Every sequence of states in $W_{\mathbf{L}}$ is a behaviour in $M_{\mathbf{L}}$.

$M = \langle W, R, I, V \rangle$ - an arbitrary model $\mathbf{L}$.

Let $S \subseteq W \times W_{\mathbf{L}}$, where $wSw' \leftrightarrow w' = V(w)$, is a simulation of M into $M_{\mathbf{L}}$.

Corollary 3 If φ is satisfiable, then it is satisfiable in $M_{\mathrm{Var}(\varphi)}$.

$|W_{\mathrm{Var}(\varphi)}| = 2^{|\mathrm{Var}(\varphi)|}$.

The End