Verification of temporal logics on infinite-state systems

Day 2, Lecture 2
Temporal logics for specification and verification of infinite-state transition systems

Stéphane Demri and Valentin Goranko

ESSLLI 2007, Dublin, July 2007
Extension of $K_t$ with reachability modalities

We consider the case of basic transition systems of type $(S, R)$.

Extend $K_t$ to $K^*_t$ by adding:

- **Reachability modality** $\langle R^* \rangle$ with Kripke semantics:
  \[ M, u \models \langle R^* \rangle \phi \text{ iff } M, w \models \phi \text{ for some } R^*-\text{successor } w \text{ of } v, \]
i.e., some $w$ (forward) reachable from $u$ by a finite $R$-path.

- **Backward reachability modality** $\langle R^{-*} \rangle$ with semantics:
  \[ M, u \models \langle R^{-*} \rangle \phi \text{ iff } M, w \models \phi \text{ for some } R^*-\text{predecessor } w \text{ of } v, \]
i.e., some $w$ backward reachable from $u$ by a finite $R$-path.

$\langle R^* \rangle$ is also denoted by $F$ and called ‘sometime in the future’ (possibly at the current state), while $\langle R^{-*} \rangle$ is usually denoted by $P$ and called ‘sometime in the past’.

The dual operators are $[R^*] := \neg \langle R^* \rangle \neg$, also denoted by $G$ and called ‘always in the future’ (including the current state), and $[R_{a^{-*}}] := \neg \langle R^{-*} \rangle \neg$, denoted by $H$, called ‘always in the past’.
Expressing properties of computations in $K_t^*$

Safety, invariance:

$G \neg (\text{The-bad-thing}).$

Partial correctness of a post-condition $\psi$ with respect to a pre-condition $\varphi$:

$\varphi \rightarrow G(\text{terminal} \rightarrow \psi).$

Liveness, eventuality:

$F(\text{The-good-thing}).$

Total correctness of a post-condition $\psi$ with respect to a pre-condition $\varphi$:

$\varphi \rightarrow F(\text{terminal} \land \psi).$
Expressing reachability in $K_t^*$

Using the reachability modality, one can express plain existential reachability properties, e.g.:

$$M, u \models \phi_I \rightarrow \langle R^* \rangle \phi_T$$

says that whenever a state $u$ in the model $M$ satisfies $\phi_I$ meaning that it belongs to the set of initial states $I$, then it can reach a target state, satisfying $\phi_T$.

Constrained reachability can be expressed by adding the binary operator \textbf{Until} with semantics:

$$M, u \models \phi U \psi \text{ iff } M, w \models \psi \text{ for some } w \in M \text{ reachable from } u \text{ by a finite } R\text{-path } u = u_0, \ldots, u_n, \text{ such that } M, u_i \models \phi \text{ for every } i < n.$$ 

Likewise, the past analogue \textbf{Since} can be added.

Expressing constrained reachability:

$$M, u \models \phi_I \rightarrow \phi_C U \phi_T,$$

where $\phi_C$ represents the constraint $C$. 

Expressing universal and recurrent reachability

Can $K^*_t$ express plain universal reachability?
Can it express recurrent (existential) reachability?

What about the formulas

$\phi_I \rightarrow [R^*]\phi_T$?

or, $\phi_I \rightarrow \langle R^*\rangle[R^*]\phi_T$?

Does $\phi_I \rightarrow [R^*](\phi_T \rightarrow \langle R^*\rangle \phi_T)$ express recurrent (existential or universal) reachability?

Neither of these works, because the semantics of $K^*_t$ cannot restrict the valuation of the formula to a fixed run (computation).
LTL is the temporal logic of single computations, proposed by Pnueli in 1977.

The formulae of LTL:

\[ \varphi := p \mid \bot \mid \varphi_1 \rightarrow \varphi_2 \mid \Diamond \varphi \mid \varphi_1 \mathcal{U} \varphi_2 \]

The semantics is based on a single computation in a transition system, and formulae are evaluated at states of that computation.

► \( \Diamond \varphi \) claims the formula \( \varphi \) is true at the immediate successor of the current state along the fixed computation;

► \( \varphi \mathcal{U} \psi \) claims that the formula \( \psi \) will become true at some future state (possibly the current one), and until then \( \varphi \) will hold true.
Some LTL miscellania

Some definable operators in LTL:

\[ F\varphi := \top U \varphi; \ G\varphi := \neg F \neg \varphi; \]

\[ G^\infty \varphi := FG\varphi \text{ meaning: } \varphi \text{ will hold almost always;} \]

\[ F^\infty := GF\varphi \text{ meaning: } \varphi \text{ will hold infinitely often.} \]

This is precisely repeated reachability.

Closure of an LTL-formula \( \varphi \): \( cl(\varphi) \) obtained by taking all subformulae of \( \varphi \) and their negations, and then deleting the double negations, if any, occurring in the obtained formulae.

Example:

\[ cl(\neg Xp \to \top U \neg q) = \]

\[ \{ \neg Xp, Xp, p, \neg p, \top U \neg q, \neg (\top U \neg q), \top, \bot, \neg q, q \}. \]

Notation: for any \( \psi \in cl(\varphi) \), denote:

\( \sim \psi = \theta \) if \( \psi = \neg \theta \), otherwise \( \sim \psi = \neg \psi \).

Eventuality: any formula \( \chi U \psi \), in particular \( F\psi \).
The formal semantics of LTL

Let $M = \langle S, R, L \rangle$ be an interpreted transition system, i.e., a Kripke model, and $\sigma : \mathbb{N} \rightarrow S$ be a run in $M$. The pair $(M, \sigma)$: linear temporal model.

The truth definition:

- $M, \sigma, i \models X\phi$ iff $M, \sigma, i \models \phi$.

- $M, \sigma, i \models \phi_1 U \phi_2$ iff there is $j \geq i$ such that $M, \sigma, i \models \phi_2$ and $M, \sigma, k \models \phi_1$ for every $i \leq k < j$.
Semantics of LTL: satisfiability

Now, we define:

- $\sigma$ satisfies $\varphi$ in $M$, denoted $M, \sigma \models \varphi$, if $M, \sigma, 0 \models \varphi$;
- $s$ satisfies $\varphi$ in $M$, denoted $M, s \models \varphi$ if $M, \sigma \models \varphi$ for every run $\sigma$ such that $\sigma_0 = s$.
- If $s$ does not satisfy $\varphi$ in $M$, we say that $s$ violates $\varphi$.
- $\varphi$ is satisfiable if it is true at some state of some linear temporal model.
Expressing fairness and precedence properties in LTL

Fairness: *if a request* $(\rho)$ *holds almost always then it is eventually granted* $(\tau)$:

$$FG\rho \rightarrow F\tau.$$  

Strong fairness: *if a request* $(\rho)$ *is repeated infinitely often then it is eventually granted* $(\tau)$:

$$GF\rho \rightarrow F\tau.$$  

The operator before: $\varphi B \psi$. Possible interpretations:

Weak ‘before’: *The event $\varphi$ will occur before the event $\psi$, which may or may not occur at all:* $\varphi B^w \psi := (\neg \psi) U (\varphi \land \neg \psi)$.

Strong ‘before’: *The event $\varphi$ will occur before the event $\psi$, which will occur, too:* $\varphi B^s \psi := (\neg \psi) U (\varphi \land \neg \psi) \land F\psi$.

Exercise:
Express in LTL “If $\psi$ ever occurs, then $\varphi$ will occur before $\psi$.”
The branching time temporal logic CTL*

LTL cannot express quantified statements about paths and computations in transition systems. The computation tree logic CTL* (Clarke, Emerson, Halpern, Sistla ’1983-86), extends LTL with path quantifiers:

- \( \forall \varphi \), meaning “\( \varphi \) is true on every computation passing through the current state”,
- \( \exists \varphi \), meaning “\( \varphi \) is true on some computation passing through the current state”.

Formulae of CTL*:
\[
\varphi := p \mid \bot \mid \varphi_1 \rightarrow \varphi_2 \mid X \varphi \mid \varphi_1 U \varphi_2 \mid \forall \varphi
\]

Two types of CTL*-formulae: state formulae, evaluated at states, and path formulae, evaluated at runs (computations).

Thus, LTL is the path formulae fragment of CTL*.

The semantics of the path quantifier:
\( M, s \models \forall \varphi \) if \( M, \sigma, 0 \models \varphi \) for every run \( \sigma \) in \( M \) with \( \sigma_0 = s \).
Example

\[
\text{PROP} = \{p, q\}
\]

\[
\begin{align*}
    s_0 & \vdash q \land \exists \mathcal{X} q \\
    s_0 & \vdash \exists \mathcal{G} q \land \neg \exists \mathcal{G} p
\end{align*}
\]

\[
\begin{align*}
    s_0 & \vdash \forall \mathcal{X} \exists \mathcal{X} q \\
    s_0 & \vdash \forall p \mathcal{U} q
\end{align*}
\]
Expressing properties of computations in CTL*  
CTL* can be used to express various global properties:  

- **partial correctness along every possible computation:**  
  \[ \varphi \rightarrow \forall G(\text{terminal} \rightarrow \psi). \]  
- **partial correctness along some possible computation:**  
  \[ \varphi \rightarrow \exists G(\text{terminal} \rightarrow \psi). \]  
- **likewise, total correctness along every possible computation:**  
  \[ \varphi \rightarrow \forall F(\text{terminal} \land \psi). \]  
- **and total correctness along some possible computation:**  
  \[ \varphi \rightarrow \exists F(\text{terminal} \land \psi). \]  
- **fairness along every possible computation:**  
  \[ \forall (G F(\text{resource requested}) \rightarrow F(\text{resource granted})) \]
Expressing universal and recurrent reachability in CTL

Plain universal reachability:

\[ M, u \models \phi_I \rightarrow \forall F \phi_T, \]

Recurrent existential reachability:

\[ M, u \models \phi_I \rightarrow \exists GF \phi_T, \]

Recurrent universal reachability:

\[ M, u \models \phi_I \rightarrow \forall GF \phi_T. \]
The branching time temporal logic CTL

CTL* is too expressive and has high computational complexity: satisfiability is 2EXPTIME-complete, model checking is PSPACE-complete.

A good compromise: the fragment CTL (Clarke, Emerson ’80-81), with essentially the same language and semantics as those of CTL*, but with restricted syntax: there are only state formulae; the path formulae $X\varphi$ and $\varphi U\psi$ must be immediately quantified by path quantifiers.

Thus, for instance, $\forall GF\varphi$ or $\exists(F\varphi \land \chi U\psi)$ are not CTL -formulae.

Formulae of CTL:

$$\varphi ::= p \mid \bot \mid \varphi_1 \rightarrow \varphi_2 \mid \forall X \varphi \mid \forall(\varphi_1 U \varphi_2) \mid \exists(\varphi_1 U \varphi_2)$$

Definable operators: $\exists X \varphi ::= \neg \forall X \neg \varphi$; $\forall F \varphi ::= \forall(\top U \varphi)$, $\exists F \varphi ::= \exists(\top U \varphi)$, $\forall G \varphi ::= \neg \exists F \neg \varphi$, $\exists G \varphi ::= \neg \forall F \neg \varphi$.

CTL can express existential and universal partial and total correctness, as well as universal reachability, but not fairness, neither recurrent reachability.
Recall: interpreted transition system = Kripke model.

Model-checking problems for CTL:

- **Local model checking**: for a Kripke model $\mathcal{M}$, state $s$ in $\mathcal{M}$, and a CTL-formula $\varphi$, determine whether $\mathcal{M}, s \models \varphi$.

- **Global model checking**: for a Kripke model $\mathcal{M}$ and a CTL-formula $\varphi$, determine (in some effective way) the set $\mathcal{M} \models \varphi$ of states where $\varphi$ is true.

- **Satisfiability in a model**: for a Kripke model $\mathcal{M}$ and a CTL-formula $\varphi$, determine whether $\mathcal{M} \models \varphi \neq \emptyset$. 
Model-checking problems for LTL and CTL*:

Model-checking problems for LTL:

- **Linear (path-) model checking**: for a given run $\sigma$ in a Kripke model $\mathcal{M}$, and an LTL-formula $\varphi$, determine whether $\mathcal{M}, \sigma \models \varphi$.

- **Local model checking**: for a Kripke model $\mathcal{M}$, state $s$ in $\mathcal{M}$, and an LTL-formula $\varphi$, determine whether $\mathcal{M}, s \models \varphi$.

- **Global model checking**: for a Kripke model $\mathcal{M}$ and an LTL-formula $\varphi$, determine (in some effective way) the set $\llbracket \varphi \rrbracket_\mathcal{M}$ of states where $\varphi$ is true.

Model-checking problems for CTL*: combine those for CTL and LTL.