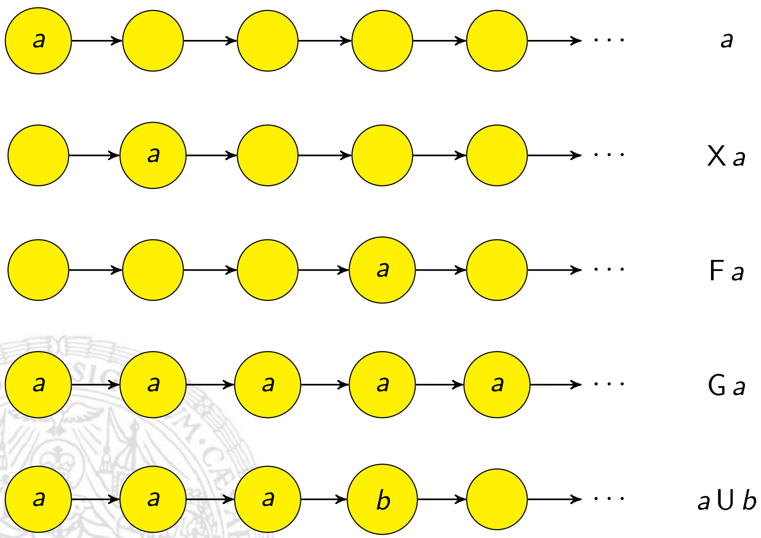
Introduction to Model Checking

René Thiemann

Institute of Computer Science
University of Innsbruck

WS 2007/2008

Last lecture: LTL



Properties expressable in LTL

- The traffic light never is red and green.
- Under the assumption that the traffic light is orange infinitely often, it is green infinitely often and red infinitely often.
- The sequence of lights is exactly red, red orange, green, orange, red, red orange, ...
- Whenever the traffic light shows red, at some moment before, both red and orange have been shown.

Semantics over words

The language induced by LTL formula φ over $AP = \{a_1, \ldots, a_n\}$ is:

$$\mathcal{L}(\varphi) \;=\; \left\{ w \in \left(2^{AP}\right)^{\omega} \mid w \models \varphi \right\}, \text{where } \models \text{ is defined as follows:}$$

$$
\begin{array}{lllll}
w & \models & a_i & \text{iff} & A_0 = (*, \ldots, *, \underbrace{1}_{i\text{-th pos.}}, *, \ldots, *)^T \text{ iff } A_0^i = 1 \\
w & \models & \varphi_1 \wedge \varphi_2 & \text{iff} & w \models \varphi_1 \text{ and } w \models \varphi_2 \\
w & \models & \neg \varphi & \text{iff} & w \not\models \varphi \\
w & \models & \mathsf{X}\, \varphi & \text{iff} & w[1..] = A_1 A_2 A_3 \ldots \models \varphi \\
w & \models & \varphi_1 \,\mathsf{U}\, \varphi_2 & \text{iff} & \exists j \geqslant 0.\ w[j..] \models \varphi_2 \text{ and } \forall 0 \leqslant i < j : w[i..] \models \varphi_1 \\
w & \models & \mathsf{F}\, \varphi & \text{iff} & \exists j \geqslant 0.\ w[j..] \models \varphi \\
w & \models & \mathsf{G}\, \varphi & \text{iff} & \forall j \geqslant 0.\ w[j..] \models \varphi
\end{array}
$$

Absorption and distributive laws

$$\text{Absorption:} \quad \mathsf{F}\,\mathsf{G}\,\mathsf{F}\,\varphi \equiv \mathsf{G}\,\mathsf{F}\,\varphi$$
$$\mathsf{G}\,\mathsf{F}\,\mathsf{G}\,\varphi \equiv \mathsf{F}\,\mathsf{G}\,\varphi$$

$$\text{Distribution:} \quad \mathsf{X}\,(\varphi\,\mathsf{U}\,\psi) \equiv (\mathsf{X}\,\varphi)\,\mathsf{U}\,(\mathsf{X}\,\psi)$$
$$\mathsf{F}\,(\varphi \vee \psi) \equiv \mathsf{F}\,\varphi \vee \mathsf{F}\,\psi$$
$$\mathsf{G}\,(\varphi \wedge \psi) \equiv \mathsf{G}\,\varphi \wedge \mathsf{G}\,\psi$$

$$\text{but \ldots\ldots:} \quad \mathsf{F}\,(\varphi \wedge \psi) \not\equiv \mathsf{F}\,\varphi \wedge \mathsf{F}\,\psi$$
$$\mathsf{G}\,(\varphi \vee \psi) \not\equiv \mathsf{G}\,\varphi \vee \mathsf{G}\,\psi$$

Distributive laws

$$\mathsf{F}\,(a \wedge b) \not\equiv \mathsf{F}\,a \wedge \mathsf{F}\,b \quad \text{and} \quad \mathsf{G}\,(a \vee b) \not\equiv \mathsf{G}\,a \vee \mathsf{G}\,b$$

$$TS \not\models \mathsf{F}\,(a \wedge \neg a) \text{ and } TS \models \mathsf{F}\,a \wedge \mathsf{F}\,\neg a$$

Expansion laws

$$\begin{aligned} \text{Expansion:} \quad \varphi \, \mathsf{U} \, \psi &\equiv \psi \vee (\varphi \wedge \mathsf{X}(\varphi \, \mathsf{U} \, \psi)) \\ \mathsf{F} \, \varphi &\equiv \varphi \vee \mathsf{XF} \, \varphi \\ \mathsf{G} \, \varphi &\equiv \varphi \wedge \mathsf{XG} \, \varphi \end{aligned}$$

Fischer Ladner Closure

Let φ be an LTL formula over predicates $a_1, \dots, a_n$.

Definition

The Fischer Ladner closure $cl(\varphi)$ is the list of sub-formulas of φ (starting from small formulas and ending with φ):

$$a_1, \dots, a_n, \dots, \varphi$$

Example

$$cl(\neg b \wedge (\mathsf{X}\, a \,\mathsf{U}\, b)) = a, b, \neg b, \mathsf{X}\, a, \mathsf{X}\, a \,\mathsf{U}\, b, \neg b \wedge (\mathsf{X}\, a \,\mathsf{U}\, b)$$

φ-Expansion

Idea: expand word by new row for each formula ψ in $cl(\varphi)$
write truth-values of ψ in i-th column for subword $w[i..]$

Definition

For $w \in (2^n)^\omega$ and LTL-formula φ with $cl(\varphi) = \varphi_1, \ldots, \varphi_m$ define the φ-expansion as word $v \in (2^m)^\omega$:

$$v[i]^j = 1 \text{ iff } w[i..] \models \varphi_j$$

Example

φ-expansion for $\varphi = \neg b \wedge (\mathsf{X}\, a \,\mathsf{U}\, b)$

Idea of LTL to NBA-Translation

- NBA guesses the φ-expansion of w
- ...and checks that guesses are correct
- ...and demands that value for whole formula is 1 for whole word w

Definition (Consistency Checks)

Consistency Checks and LTL-Models

Lemma

$w \models \varphi$ iff there exists an expansion $v \in (2^m)^\omega$ of w such that

1. *v satisfies the consistency checks*
2. $v[0..]^m = 1$
3. *whenever $\varphi_j = \varphi_{j_1} \mathsf{U} \varphi_{j_2}$ and $v[i..]^j = 1$ then there exists $i' \geqslant i$ such that $v[i'..]^{j_2} = 1$*

Translating LTL to GNBA

Definition (GNBA for an LTL formula φ)

Let $cl(\varphi) = a_1, \ldots, a_n, \varphi_{n+1}, \ldots, \varphi_m$ where $\varphi_m = \varphi$.
Define $\mathcal{A}_\varphi = (2^m \uplus \{q_0\}, 2^n, q_0, \delta, F_1, \ldots, F_k)$ where

- $(c_1, \ldots, c_m)^T \in \delta((b_1, \ldots, b_m)^T, (d_1, \ldots, d_n)^T)$ iff
  1. $c_j = d_j$ for all $j \leqslant n$ (expansion)
  2. $(b_1, \ldots, b_m)^T$ $(c_1, \ldots, c_m)^T$ is consistent (consistent expansion)
- $(c_1, \ldots, c_m)^T \in \delta(q_0, (d_1, \ldots, d_n)^T)$ iff
  1. $c_j = d_j$ for all $j \leqslant n$ (expansion)
  2. $(c_1, \ldots, c_m)^T$ is consistent (consistent expansion)
  3. $c_m = 1$ (φ is satisfied)

Soundness of Translation

Theorem

For every LTL formula φ

$$\mathcal{L}(\varphi) = \mathcal{L}(\mathcal{A}_\varphi)$$

Proof of Lemma.

By induction on φ using the consistency checks. ■

Proof of Theorem.

- Construction of $\mathcal{A}_\varphi$ directly corresponds to requirements 1 and 2 in Lemma
- Remaining difficulty:
  Show that visiting F_i infinitely often is the same as requirement 3 in Lemma for i-th U-subformula $\varphi_j = \varphi_{j_1} \mathsf{U} \varphi_{j_2}$ ■

Exercises

Construct the NBA for the formula $a \, \mathsf{U} \, \mathsf{X} \, b$

- intuitively by hand
- using the construction on Slide 17