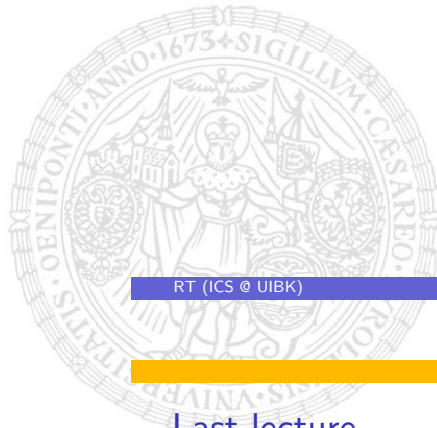


Introduction to Model Checking

René Thiemann

Institute of Computer Science
University of Innsbruck

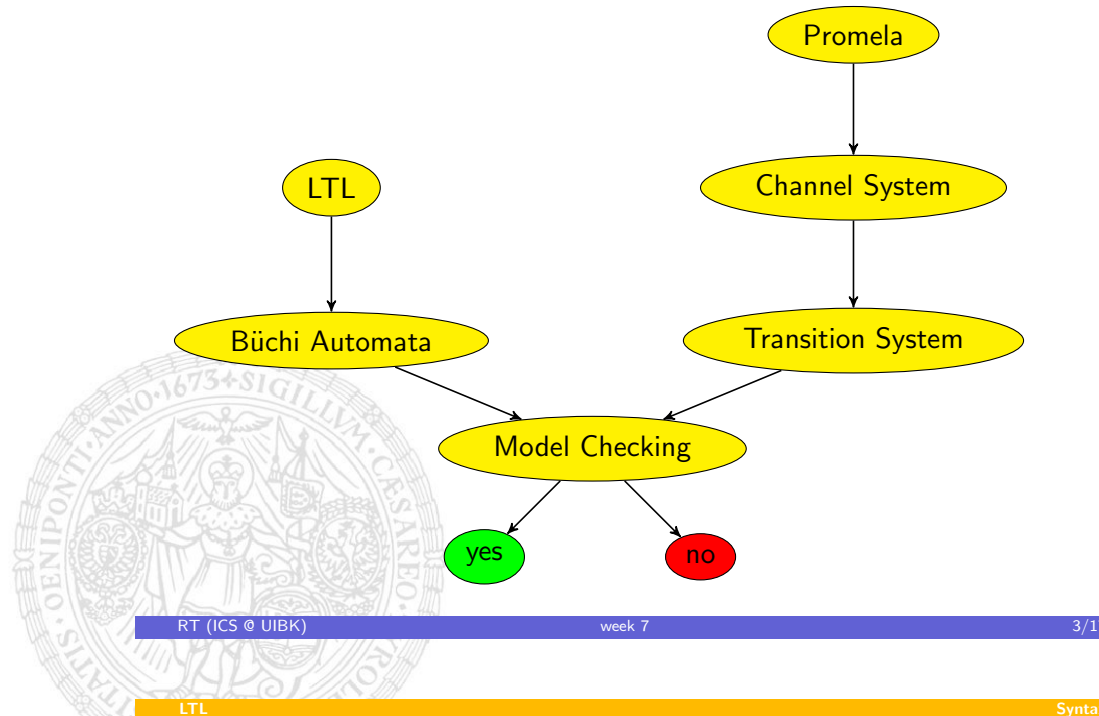
WS 2007/2008



Last lecture

- Languages recognized by NBA = ω -regular languages
- DBA are less powerful than NBA
 - fail, e.g., to represent the language "only finitely many B "
- Generalized NBA require repeated visits for several acceptance sets
 - the languages recognized by GNBA = ω -regular languages
- Checking an ω -regular property = checking non-emptiness on product of NBA and TS
 - no path to an SCC containing an "accept state"
- Checking can be done in linear size of TS and NBA (if NBA for complement is given)

The need for logic



RT (ICS @ UIBK)

week 7

3/17

LTL

Syntax

Syntax of Linear Temporal Logic

modal logic over infinite sequences [Pnueli 1977]

- **Propositional logic**

- $a, red, want_sprite, \dots \in AP$
- $\neg\varphi$ and $\varphi \wedge \psi$

atomic proposition
negation and conjunction

- **Temporal operators**

- $X\varphi$
- $F\varphi$
- $G\varphi$
- $\varphi U \psi$

neXt state fulfills φ
sometimes in the Future φ will hold
 φ Globally holds
 φ holds Until a ψ -state is reached

linear temporal logic is a logic for describing linear time properties

RT (ICS @ UIBK)

week 7

5/17

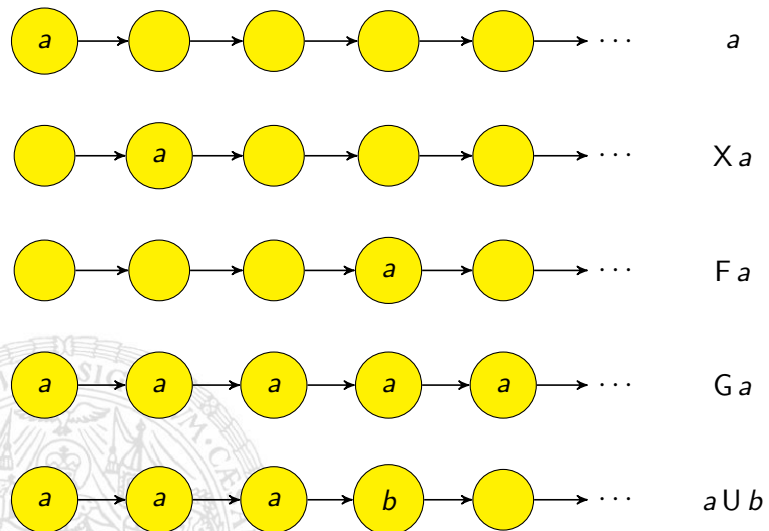
Derived operators

$$\begin{aligned}
 \text{false} &\equiv \varphi \wedge \neg \varphi \\
 \text{true} &\equiv \neg \text{false} \\
 \varphi \vee \psi &\equiv \neg(\neg \varphi \wedge \neg \psi) \\
 \varphi \Rightarrow \psi &\equiv \neg \varphi \vee \psi \\
 \varphi \Leftrightarrow \psi &\equiv (\varphi \Rightarrow \psi) \wedge (\psi \Rightarrow \varphi) \\
 \varphi \oplus \psi &\equiv \neg(\varphi \Leftrightarrow \psi)
 \end{aligned}$$

precedence order: the unary operators bind stronger than the binary ones.

\neg and \times bind equally strong. \cup takes precedence over \wedge , \vee , and \Rightarrow

Intuitive semantics



Traffic light properties

- Once red, the light cannot become green immediately:

$$G(\text{red} \Rightarrow \neg X \text{green})$$

- The green light becomes green eventually: $F \text{green}$
- Once red, the light becomes green eventually: $G(\text{red} \Rightarrow F \text{green})$
- Once red, the light always becomes green eventually after being yellow for some time inbetween:

$$G(\text{red} \Rightarrow X(\text{red} \cup (\text{yellow} \wedge X(\text{yellow} \cup \text{green}))))$$

Practical properties in LTL

- **Reachability**
 - reachability
 - conditional reachability
 - reachability from any state

 $F \psi$
 $\varphi \cup \psi$

not expressible

- **Safety**

 $G \neg \varphi$

- **Liveness**

 $G(\varphi \Rightarrow F \psi)$ and others

- **Fairness**

 $GF \varphi$ and others

Semantics over words

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

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

(Let $w = A_0 A_1 A_2 \dots$ and $w[i..] = A_i A_{i+1} A_{i+2} \dots$ is the suffix of w from index i on)

$$w \models a_i \quad \text{iff} \quad A_0 = (*, \dots, *, \underbrace{1}_{i\text{-th pos.}}, *, \dots, *)^{\text{transposed}} \quad \text{iff} \quad A_0^i = 1$$

$$w \models \varphi_1 \wedge \varphi_2 \quad \text{iff} \quad w \models \varphi_1 \text{ and } w \models \varphi_2$$

$$w \models \neg \varphi \quad \text{iff} \quad w \not\models \varphi$$

$$w \models X \varphi \quad \text{iff} \quad w[1..] = A_1 A_2 A_3 \dots \models \varphi$$

$$w \models \varphi_1 U \varphi_2 \quad \text{iff} \quad \exists j \geq 0. w[j..] \models \varphi_2 \text{ and } \forall 0 \leq i < j : w[i..] \models \varphi_1$$

$$w \models F \varphi \quad \text{iff} \quad \exists j \geq 0. w[j..] \models \varphi$$

$$w \models G \varphi \quad \text{iff} \quad \forall j \geq 0. w[j..] \models \varphi$$

Equivalence of LTL formula, Deriving F and G

Often used constructs

- $GF\varphi$ iff $\forall i \exists j \geq i : w[j..] \models \varphi$ iff
infinitely often φ is satisfied
- $FG\varphi$ iff $\exists i \forall j \geq i : w[j..] \models \varphi$ iff
from some point onwards φ is satisfied

Semantics for Transition Systems

Semantics is defined via set inclusion (as for NBAs):

$$TS \models \varphi \text{ iff } \text{Traces}(TS) \subseteq \mathcal{L}(\varphi)$$

A small note:

For trace w , it holds $w \models \varphi$ if and only if $w \not\models \neg\varphi$ since:

$$\mathcal{L}(\neg\varphi) = (2^{AP})^w \setminus \mathcal{L}(\varphi)$$

But: $TS \not\models \varphi$ and $TS \models \neg\varphi$ are *not* equivalent in general

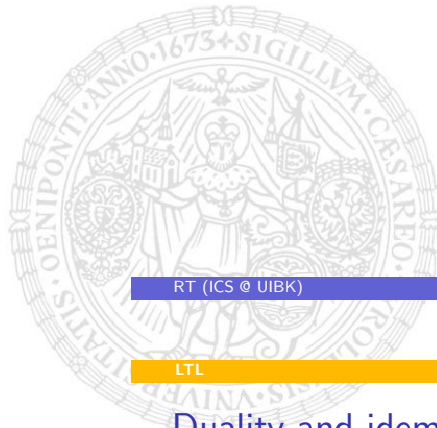
It holds: $TS \models \neg\varphi$ implies $TS \not\models \varphi$. Not always the reverse!

Note that:

$$\begin{aligned} TS \not\models \varphi & \text{ iff } \text{Traces}(TS) \not\subseteq \mathcal{L}(\varphi) \\ & \text{ iff } \text{Traces}(TS) \setminus \mathcal{L}(\varphi) \neq \emptyset \\ & \text{ iff } \text{Traces}(TS) \cap \mathcal{L}(\neg\varphi) \neq \emptyset \end{aligned}$$

TS neither satisfies φ nor $\neg\varphi$ if there are traces w_1 and w_2 in TS such that $w_1 \models \varphi$ and $w_2 \models \neg\varphi$

Example



Duality and idempotence laws

Duality:

$$\neg G\varphi \equiv F\neg\varphi$$

$$\neg F\varphi \equiv G\neg\varphi$$

$$\neg X\varphi \equiv X\neg\varphi$$

Idempotency:

$$GG\varphi \equiv G\varphi$$

$$FF\varphi \equiv F\varphi$$

$$\varphi U (\varphi U \psi) \equiv \varphi U \psi$$

$$(\varphi U \psi) U \psi \equiv \varphi U \psi$$

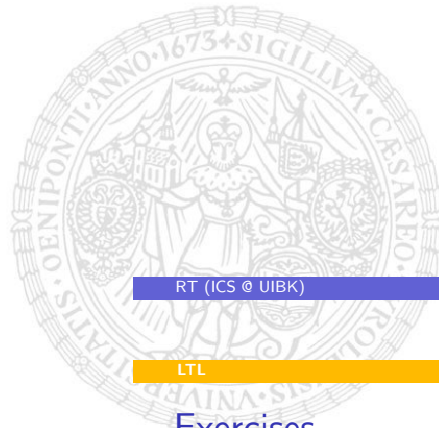


Expansion laws

Expansion: $\varphi \text{ U } \psi \equiv \psi \vee (\varphi \wedge \text{X}(\varphi \text{ U } \psi))$

$$\text{F } \varphi \equiv \varphi \vee \text{X F } \varphi$$

$$\text{G } \varphi \equiv \varphi \wedge \text{X G } \varphi$$



Exercises

- Formalize the following statements 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.
- Prove the following equivalences
 - $\text{G}(a \wedge b) \equiv \text{G}a \wedge \text{G}b$
 - $\varphi \text{ U } (\varphi \text{ U } \psi) \equiv \varphi \text{ U } \psi$
 - $\varphi \text{ U } \psi \equiv \psi \vee (\varphi \wedge \text{X}(\varphi \text{ U } \psi))$

