Introduction to Model Checking

René Thiemann

Institute of Computer Science

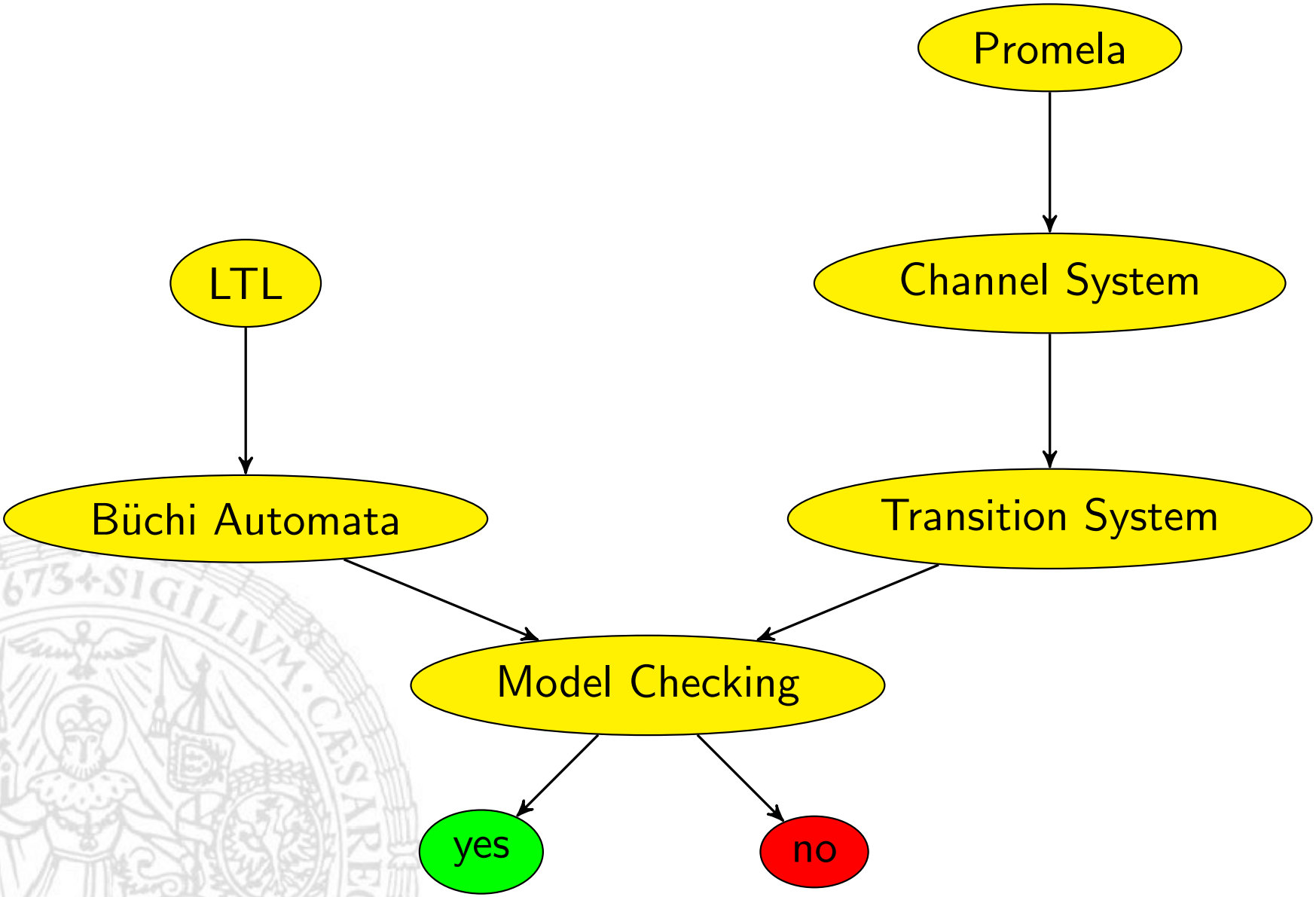
University of Innsbruck

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-emptyness 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



Syntax of Linear Temporal Logic

modal logic over infinite sequences [Pnueli 1977]

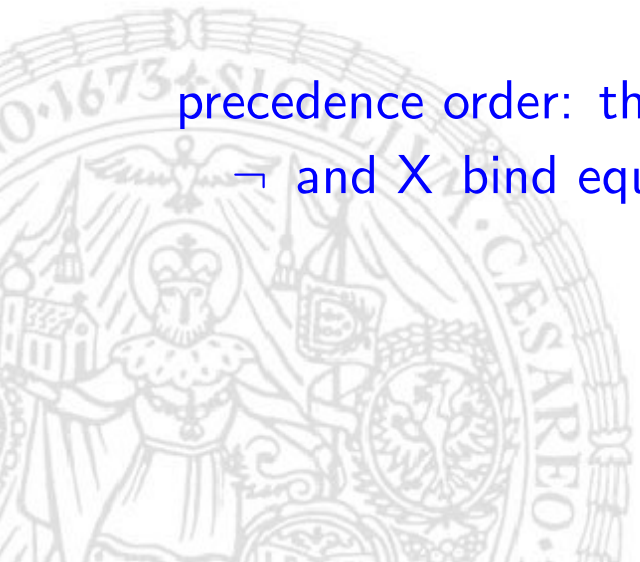
- Propositional logic
  - $a, \mathit{red}, \mathit{want\_sprite}, \ldots \in AP$ — atomic proposition
  - $\neg\varphi$ and $\varphi \wedge \psi$ — negation and conjunction
- Temporal operators
  - $\mathsf{X}\,\varphi$ — neXt state fulfills φ
  - $\mathsf{F}\,\varphi$ — sometimes in the Future φ will hold
  - $\mathsf{G}\,\varphi$ — φ Globally holds
  - $\varphi\,\mathsf{U}\,\psi$ — φ holds Until a ψ-state is reached

linear temporal logic is a logic for describing linear time properties

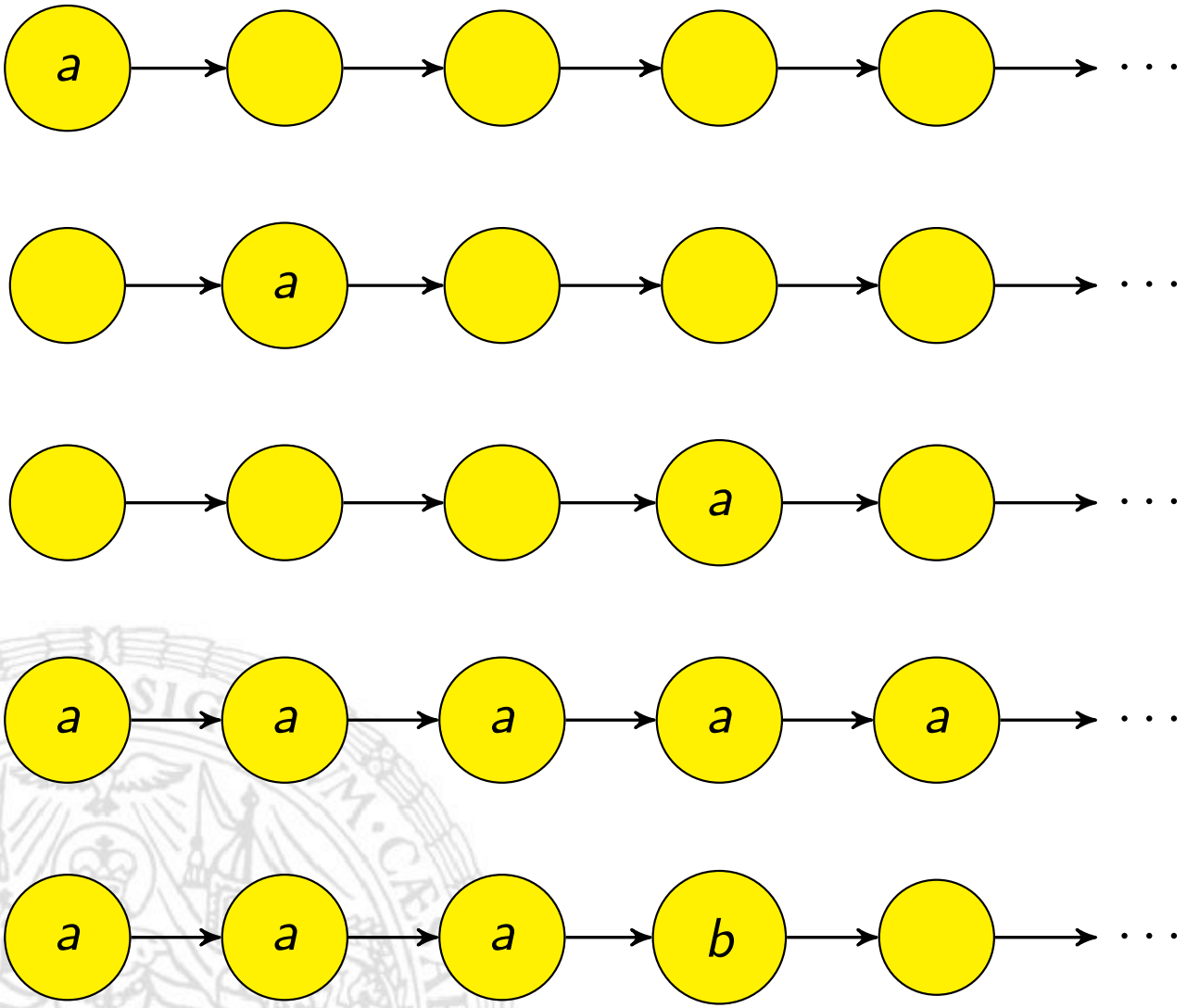
Derived operators

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

precedence order: the unary operators bind stronger than the binary ones. $\neg$ and X bind equally strong. U takes precedence over $\wedge$, $\vee$, and $\Rightarrow$



Intuitive semantics



Traffic light properties

- Once red, the light cannot become green immediately:

$$\mathsf{G}\,(\mathit{red} \;\Rightarrow\; \neg\,\mathsf{X}\,\mathit{green})$$

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

$$\mathsf{G}\,(\mathit{red} \Rightarrow \mathsf{X}\,(\mathit{red}\,\mathsf{U}\,(\mathit{yellow} \wedge \mathsf{X}\,(\mathit{yellow}\,\mathsf{U}\,\mathit{green}))))$$

Practical properties in LTL

- Reachability
  - reachability $\mathsf{F}\,\psi$
  - conditional reachability $\varphi\,\mathsf{U}\,\psi$
  - reachability from any state not expressible
- Safety $\mathsf{G}\,\neg\varphi$
- Liveness $\mathsf{G}\,(\varphi \Rightarrow \mathsf{F}\,\psi)$ and others
- Fairness $\mathsf{G}\,\mathsf{F}\,\varphi$ and others

Semantics over words

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

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

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

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

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

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

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

$$w \models \varphi_1 \,\mathsf{U}\, \varphi_2 \quad \text{iff} \quad \exists j \geqslant 0.\ w[j..] \models \varphi_2 \text{ and } \forall 0 \leqslant i < j : w[i..] \models \varphi_1$$

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

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

Equivalence of LTL formula, Deriving F and G

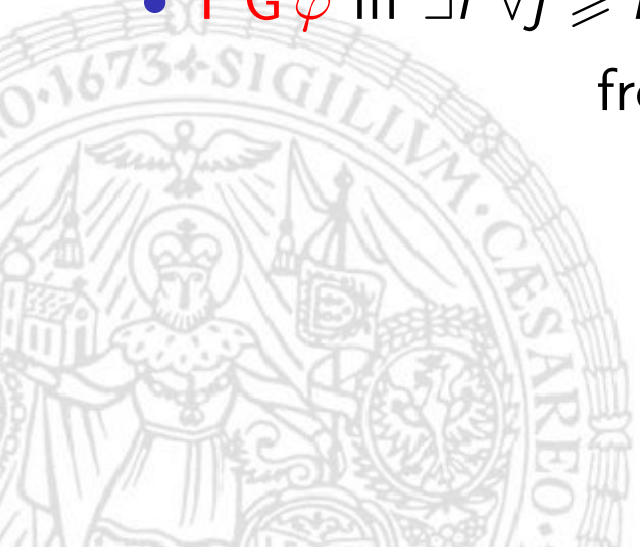
Often used constructs

- $\mathsf{G}\,\mathsf{F}\,\varphi$ iff $\forall i\ \exists j \geqslant i : w[j..] \models \varphi$ iff

  infinitely often φ is satisfied

- $\mathsf{F}\,\mathsf{G}\,\varphi$ iff $\exists i\ \forall j \geqslant i : w[j..] \models \varphi$ iff

  from some point onwards φ is satisfied



Semantics for Transition Systems

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

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

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

$$\mathcal{L}(\neg\varphi) = \left(2^{AP}\right)^{\omega} \setminus \mathcal{L}(\varphi)$$

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:

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

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:

$$\neg \mathsf{G}\,\varphi \equiv \mathsf{F}\,\neg\varphi$$
$$\neg \mathsf{F}\,\varphi \equiv \mathsf{G}\,\neg\varphi$$
$$\neg \mathsf{X}\,\varphi \equiv \mathsf{X}\,\neg\varphi$$

Idempotency:

$$\mathsf{G}\,\mathsf{G}\,\varphi \equiv \mathsf{G}\,\varphi$$
$$\mathsf{F}\,\mathsf{F}\,\varphi \equiv \mathsf{F}\,\varphi$$
$$\varphi\,\mathsf{U}\,(\varphi\,\mathsf{U}\,\psi) \equiv \varphi\,\mathsf{U}\,\psi$$
$$(\varphi\,\mathsf{U}\,\psi)\,\mathsf{U}\,\psi \equiv \varphi\,\mathsf{U}\,\psi$$

Expansion laws

Expansion:

$$\varphi \,\mathsf{U}\, \psi \equiv \psi \vee (\varphi \wedge \mathsf{X}(\varphi \,\mathsf{U}\, \psi))$$

$$\mathsf{F}\,\varphi \equiv \varphi \vee \mathsf{XF}\,\varphi$$

$$\mathsf{G}\,\varphi \equiv \varphi \wedge \mathsf{XG}\,\varphi$$

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
  - $\mathsf{G}\,(a \wedge b) \quad \equiv \quad \mathsf{G}\,a \;\wedge\; \mathsf{G}\,b$
  - $\varphi\,\mathsf{U}\,(\varphi\,\mathsf{U}\,\psi) \quad \equiv \quad \varphi\,\mathsf{U}\,\psi$
  - $\varphi\,\mathsf{U}\,\psi \quad \equiv \quad \psi \;\vee\; (\varphi \wedge \mathsf{X}(\varphi\,\mathsf{U}\,\psi))$