1

test

hello :)

Model Checking

Linear Temporal Logic, Part 2

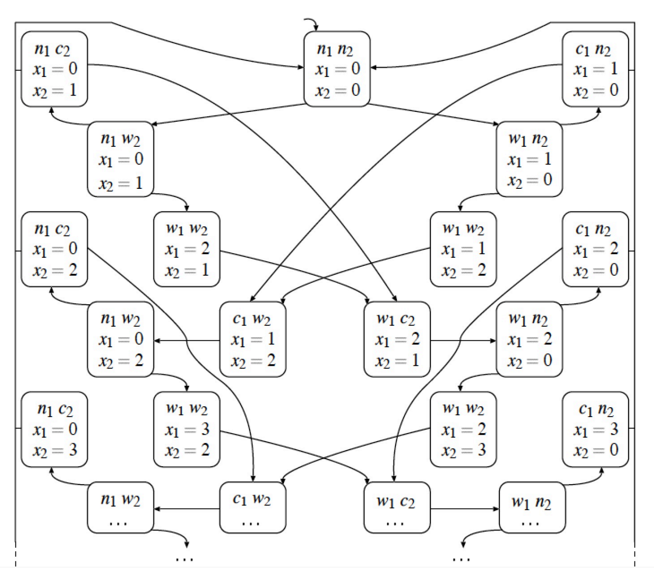
[Baier & Katoen, Chapter 5.1]

Prof. Dr. Nils Jansen
Radboud University, 2025

Credit to the slides: Prof. Dr. Dr.h.c. Joost-Pieter Katoen

What is a model?

What is a model?



Do transition systems have any practical use?

How do we specify properties?

Summary

- Transition systems are a general formal model to capture real life (programing) problems
- Mind the state space explosion!
- LT properties are finite sets of infinite words over 2^{AP} (= traces)

- An invariant requires a condition Φ to hold in any reachable state

- Each trace refuting a safety property has a finite prefix causing this
  - invariants are safety properties with bad prefix $\Phi^*(\neg\Phi)$

  $\Rightarrow$ safety properties constrain finite behaviours

Is There a Proper Logic to Define Properties?

Who would tell an engineer to write regular expressions for bad prefixes?

LTL Syntax

Recap: LTL syntax
BNF grammar for LTL formulas with proposition $a \in AP$:

$$\varphi ::= \text{true} \;\Big|\; a \;\Big|\; \varphi_1 \wedge \varphi_2 \;\Big|\; \neg\varphi \;\Big|\; \underbrace{\bigcirc\varphi \;\Big|\; \varphi_1 \,\mathsf{U}\, \varphi_2}_{\text{temporal}}$$

$\ell_1 \ \ell_1 \ \ell_1 \ \underline{\ell_2}$

ℓ_2

LTL Syntax

Recap: LTL syntax
BNF grammar for LTL formulas with proposition $a \in AP$:

$$\varphi \ ::= \ \text{true} \ \big| \ a \ \big| \ \varphi_1 \wedge \varphi_2 \ \big| \ \neg\varphi \ \big| \ \bigcirc\varphi \ \big| \ \varphi_1 \,\mathsf{U}\, \varphi_2$$

- Propositional logic
  - $a \in AP$ — atomic proposition
  - $\neg\varphi$ and $\varphi \wedge \psi$ — negation and conjunction
- Temporal modalities
  - $\bigcirc\varphi$ — neXt state fulfills φ
  - $\varphi \,\mathsf{U}\, \psi$ — φ holds Until a ψ-state is reached

Linear Temporal Logic (LTL) is a logic to describe LT properties

Recap: Derived Operators

$$
\begin{aligned}
\varphi \lor \psi &\equiv \neg(\neg\varphi \land \neg\psi) \\
\varphi \Rightarrow \psi &\equiv \neg\varphi \lor \psi \\
\varphi \Leftrightarrow \psi &\equiv (\varphi \Rightarrow \psi) \land (\psi \Rightarrow \varphi) \\
\varphi \oplus \psi &\equiv (\varphi \land \neg\psi) \lor (\neg\varphi \land \psi) \\
\mathsf{true} &\equiv \varphi \lor \neg\varphi \\
\mathsf{false} &\equiv \neg\,\mathsf{true}
\end{aligned}
$$

Recap: Derived Operators

$\varphi \lor \psi \equiv$

$\varphi \Rightarrow \psi \equiv$

$\varphi \Leftrightarrow \psi \equiv$

$\varphi \oplus \psi \equiv$

$\text{true} \equiv$

$\text{false} \equiv$

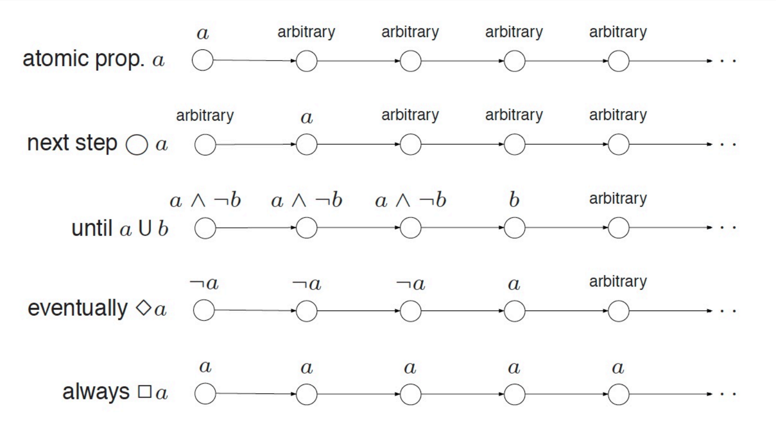
$\Diamond \varphi \equiv$ "some time in the future" "eventually" "finally"

$\Box \varphi \equiv$ "from now on forever"

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

$\neg$ and $\bigcirc$ bind equally strong. U takes precedence over $\land$, $\lor$, and $\Rightarrow$

Recap: Intuitive Semantics



Example: Traffic Light Properties

- The traffic light becomes green eventually: $\Diamond\, green$

Example: Traffic Light Properties

- The traffic light becomes green eventually: $\Diamond\, \mathit{green}$
- Once red, the light cannot become green immediately:

$$\Box\,(\mathit{red} \;\Rightarrow\; \neg \bigcirc \mathit{green})$$

Example: Traffic Light Properties

- The traffic light becomes green eventually: $\Diamond\, \mathit{green}$
- Once red, the light cannot become green immediately:

$$\Box\,(\mathit{red} \;\Rightarrow\; \neg \bigcirc \mathit{green})$$

- Once red, the light becomes green eventually: $\Box\,(\mathit{red} \;\Rightarrow\; \Diamond\, \mathit{green})$

Example: Traffic Light Properties

a $\qquad \bigcirc a \, \mathrm{U} b$

- The traffic light becomes green eventually: $\Diamond \, green$
- Once red, the light cannot become green immediately:

$$\Box \, (red \;\Rightarrow\; \neg \bigcirc green)$$

- Once red, the light becomes green eventually: $\Box \, (red \;\Rightarrow\; \Diamond \, green)$
- Once red, the light always becomes green eventually after being yellow for some time inbetween:

$$\Box(red \;\Rightarrow\; \bigcirc \, (red \, \mathrm{U} \, (yellow \wedge \bigcirc (yellow \, \mathrm{U} \, green))))$$

Overview

LTL Equivalence

Definition: LTL equivalence
LTL formulas φ, ψ (both over AP) are equivalent:

$$\varphi \equiv_{LTL} \psi \quad \text{if and only if} \quad \mathit{Words}(\varphi) = \mathit{Words}(\psi).$$

If it is clear from the context that we deal with LTL-formulas, we simply write $\varphi \equiv \psi$.

Equivalently:

$$\varphi \equiv_{LTL} \psi \text{ iff } \big(\text{ for all transition systems } TS : TS \models \varphi \text{ iff } TS \models \psi \ \big).$$

Duality and Idempotence

Duality:

$$\neg \Box \varphi \equiv \Diamond \neg \varphi$$

$$\neg \Diamond \varphi \equiv \Box \neg \varphi$$

$$\neg \bigcirc \varphi \equiv \bigcirc \neg \varphi$$

Duality and Idempotence

Duality:

$$\neg \Box \varphi \equiv \Diamond \neg \varphi$$

$$\neg \Diamond \varphi \equiv \Box \neg \varphi$$

$$\neg \bigcirc \varphi \equiv \bigcirc \neg \varphi$$

Idempotence:

$$\Box \Box \varphi \equiv \Box \varphi$$

$$\Diamond \Diamond \varphi \equiv \Diamond \varphi$$

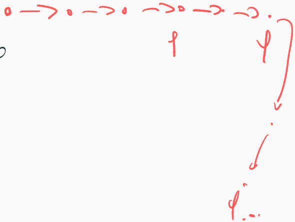
$$\varphi \, \mathsf{U} \, (\varphi \, \mathsf{U} \, \psi) \equiv \varphi \, \mathsf{U} \, \psi$$

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

Absorption and Distributive

Absorption: $\Diamond \Box \Diamond \varphi \equiv \Box \Diamond \varphi$

$\Box \Diamond \Box \varphi \equiv \Diamond \Box \varphi$



Absorption and Distributive

$$\text{Absorption:} \quad \Diamond\Box\Diamond\varphi \equiv \Box\Diamond\varphi$$

$$\Box\Diamond\Box\varphi \equiv \Diamond\Box\varphi$$

$$\text{Distributive:} \quad \bigcirc(\varphi \,\mathsf{U}\, \psi) \equiv (\bigcirc\varphi)\,\mathsf{U}\,(\bigcirc\psi)$$

$$\Diamond(\varphi \vee \psi) \equiv \Diamond\varphi \vee \Diamond\psi$$

$$\Box(\varphi \wedge \psi) \equiv \Box\varphi \wedge \Box\psi$$

Absorption and Distributive

Absorption:

$$\Diamond\Box\Diamond\varphi \equiv \Box\Diamond\varphi$$

$$\Box\Diamond\Box\varphi \equiv \Diamond\Box\varphi$$

Distributive:

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

$$\Diamond(\varphi \vee \psi) \equiv \Diamond\varphi \vee \Diamond\psi$$

$$\Box(\varphi \wedge \psi) \equiv \Box\varphi \wedge \Box\psi$$

$\Box(\varphi \, \mathsf{U} \, \psi)$

$\varphi \quad \varphi \quad \psi \quad \varphi \quad \psi \quad \psi$

$(\Box\varphi) \, \mathsf{U} \, (\Box\psi)$

but ......:

$$\Box(\varphi \, \mathsf{U} \, \psi) \not\equiv (\Box\varphi) \, \mathsf{U} \, (\Box\psi)$$

$$\Diamond(\varphi \wedge \psi) \not\equiv \Diamond\varphi \wedge \Diamond\psi$$

$$\Box(\varphi \vee \psi) \not\equiv \Box\varphi \vee \Box\psi$$

$\underbrace{\varphi \quad \varphi \quad \varphi}_{\Box\varphi} \quad \underbrace{\psi \quad \psi \quad \psi}_{\Box\psi}$

Definition: the weak-until-operator
The weak-until (or: unless) operator is defined by

$$\varphi \mathsf{W} \psi = (\varphi \mathsf{U} \psi) \vee \Box\varphi.$$

In contrast to until, weak until does not require to establish ψ eventually

Weak Until

Definition: the weak-until-operator
The weak-until (or: unless) operator is defined by

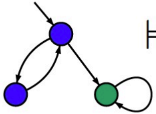
$$\varphi \,\mathsf{W}\, \psi \;=\; (\varphi \,\mathsf{U}\, \psi) \;\vee\; \Box\varphi.$$

In contrast to until, weak until does not require to establish ψ eventually

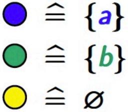
Until U and weak until W are dual:

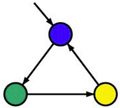
$$\begin{aligned} \neg(\varphi \,\mathsf{U}\, \psi) &\equiv (\varphi \wedge \neg\psi) \,\mathsf{W}\, (\neg\varphi \wedge \neg\psi) \\ \neg(\varphi \,\mathsf{W}\, \psi) &\equiv (\varphi \wedge \neg\psi) \,\mathsf{U}\, (\neg\varphi \wedge \neg\psi) \end{aligned}$$

Example

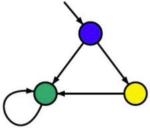


$\models a \, \mathbf{W} \, b$





$\models a \, \mathbf{W} \, b$ (even $a \, \mathbf{U} \, b$)

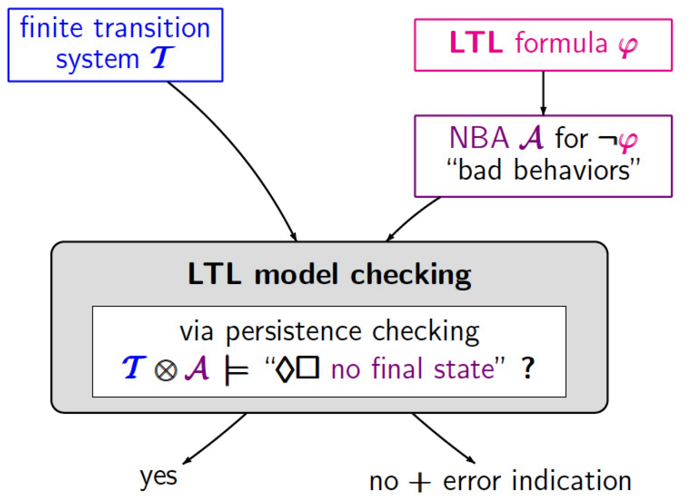


$\not\models a \, \mathbf{W} \, b$

Overview

Can We Do LTL Model Checking?

Automata-Based LTL Model Checking



Overview

1. LTL Equivalence
2. LTL Model Checking
3. Summary

Summary

- Linear temporal logic (LTL) is a logic to succinctly describe LT properties
- LTL-formulas are equivalent iff they describe the same LT properties