Verification

Lecture 12

Martin Zimmermann

UNIVERSITÄT
DES
SAARLANDES

Plan for today

- LTL
- Fairness in LTL
- LTL Model Checking

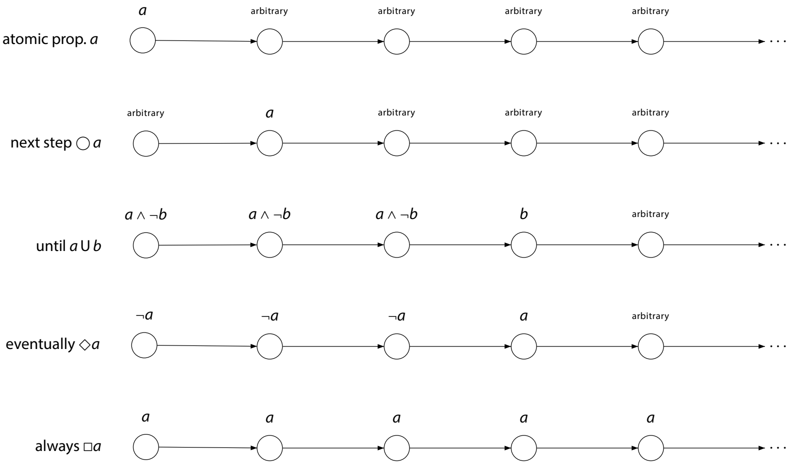
Review: Syntax

modal logic over infinite sequences [Pnueli 1977]

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

linear temporal logic is a logic for describing LT properties

Review: Intuitive semantics



Semantics over words

The LT-property induced by LTL formula φ over AP is:

$$Words(\varphi) = \left\{\sigma \in \left(2^{AP}\right)^{\omega} \mid \sigma \vDash \varphi\right\},$$ where $\vDash$ is the smallest relation satisfying:

$$
\begin{array}{lllll}
\sigma & \vDash & \text{true} & & \\
\sigma & \vDash & a & \text{iff} & a \in A_0 \quad (\text{i.e., } A_0 \vDash a) \\
\sigma & \vDash & \varphi_1 \wedge \varphi_2 & \text{iff} & \sigma \vDash \varphi_1 \text{ and } \sigma \vDash \varphi_2 \\
\sigma & \vDash & \neg\,\varphi & \text{iff} & \sigma \nvDash \varphi \\
\sigma & \vDash & \bigcirc\,\varphi & \text{iff} & \sigma[1..] = A_1 A_2 A_3 \ldots \vDash \varphi \\
\sigma & \vDash & \varphi_1 \,\mathsf{U}\, \varphi_2 & \text{iff} & \exists j \geq 0.\ \sigma[j..] \vDash \varphi_2 \text{ and } \sigma[i..] \vDash \varphi_1,\ 0 \leq i < j
\end{array}
$$

for $\sigma = A_0 A_1 A_2 \ldots$ we have $\sigma[i..] = A_i A_{i+1} A_{i+2} \ldots$ is the suffix of σ from index i on

Semantics over paths and states

Let $TS = (S, Act, \rightarrow, I, AP, L)$ be a transition system without terminal states, and let φ be an LTL-formula over AP.

- For infinite path fragment π of TS:

$$\pi \models \varphi \qquad \text{iff} \qquad trace(\pi) \models \varphi$$

- For state $s \in S$:

$$s \models \varphi \qquad \text{iff} \qquad (\forall \pi \in Paths(s).\ \pi \models \varphi)$$

- TS satisfies φ, denoted $TS \models \varphi$, if $Traces(TS) \subseteq Words(\varphi)$

Semantics for transition systems

$$TS \models \varphi$$

iff (* transition system semantics *)

$$Traces(TS) \subseteq Words(\varphi)$$

iff (* definition of $\models$ for LT-properties *)

$$TS \models Words(\varphi)$$

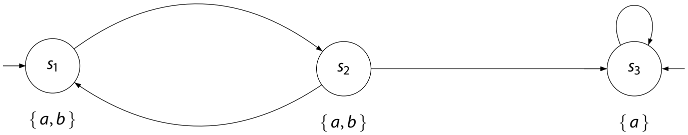
iff (* Definition of $Words(\varphi)$ *)

$$\pi \models \varphi \text{ for all } \pi \in Paths(TS)$$

iff (* semantics of $\models$ for states *)

$$s_0 \models \varphi \text{ for all } s_0 \in I \quad .$$

Example



Semantics of negation

For paths, it holds $\pi \vDash \varphi$ if and only if $\pi \nvDash \neg\varphi$ since:

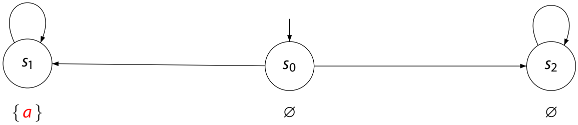
$$Words(\neg\varphi) = \left(2^{AP}\right)^{\omega} \setminus Words(\varphi) \quad .$$

But: $TS \nvDash \varphi$ and $TS \vDash \neg\varphi$ are not equivalent in general
It holds: $TS \vDash \neg\varphi$ implies $TS \nvDash \varphi$. Not always the reverse!
Note that:

$$\begin{aligned} TS \nvDash \varphi \quad & \text{iff} \quad Traces(TS) \nsubseteq Words(\varphi) \\ & \text{iff} \quad Traces(TS) \setminus Words(\varphi) \neq \varnothing \\ & \text{iff} \quad Traces(TS) \cap Words(\neg\varphi) \neq \varnothing \quad . \end{aligned}$$

TS neither satisfies φ nor $\neg\varphi$ if there are paths π_1 and π_2 in *TS* such that $\pi_1 \vDash \varphi$ and $\pi_2 \vDash \neg\varphi$

Example



A transition system for which $TS \not\models \Diamond a$ and $TS \not\models \neg \Diamond a$

Semantics of $\Box$, $\Diamond$, $\Box\Diamond$ and $\Diamond\Box$

$$
\begin{array}{llll}
\sigma & \models & \Diamond\varphi & \text{iff} \quad \exists j \geq 0.\ \sigma[j..] \models \varphi \\
\sigma & \models & \Box\varphi & \text{iff} \quad \forall j \geq 0.\ \sigma[j..] \models \varphi \\
\sigma & \models & \Box \Diamond \varphi & \text{iff} \quad \forall j \geq 0.\ \exists i \geq j.\ \sigma[i \ldots] \models \varphi \\
\sigma & \models & \Diamond \Box \varphi & \text{iff} \quad \exists j \geq 0. \forall i \geq j.\ \sigma[i \ldots] \models \varphi
\end{array}
$$

Equivalence

LTL formulas ϕ, ψ are equivalent, denoted $\phi \equiv \psi$, if:

$$Words(\phi) = Words(\psi)$$

Duality and idempotence laws

Duality:

$$\neg \Box \phi \equiv \Diamond \neg \phi$$

$$\neg \Diamond \phi \equiv \Box \neg \phi$$

$$\neg \bigcirc \phi \equiv \bigcirc \neg \phi$$

Idempotency:

$$\Box \Box \phi \equiv \Box \phi$$

$$\Diamond \Diamond \phi \equiv \Diamond \phi$$

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

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

Absorption and distributive laws

Absorption:

$$\Diamond \Box \Diamond \phi \equiv \Box \Diamond \phi$$

$$\Box \Diamond \Box \phi \equiv \Diamond \Box \phi$$

Distribution:

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

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

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

but . . . . . .:

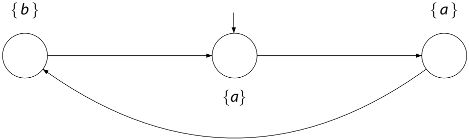
$$\Diamond(\phi \,\mathsf{U}\, \psi) \not\equiv (\Diamond\phi) \,\mathsf{U}\, (\Diamond\psi)$$

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

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

Distributive laws

$$\Diamond(a \wedge b) \not\equiv \Diamond a \wedge \Diamond b \quad \text{and} \quad \Box(a \vee b) \not\equiv \Box a \vee \Box b$$



$TS \not\models \Diamond(a \wedge b)$ and $TS \models (\Diamond a) \wedge (\Diamond b)$

$TS \not\models (\Box a) \vee (\Box b)$ and $TS \models \Box(a \vee b)$

Expansion laws

$$
\begin{aligned}
\text{Expansion:}\quad \phi \,\mathsf{U}\, \psi \quad &\equiv \quad \psi \lor (\phi \land \bigcirc(\phi \,\mathsf{U}\, \psi)) \\
\Diamond \phi \quad &\equiv \quad \phi \lor \bigcirc \Diamond \phi \\
\Box \phi \quad &\equiv \quad \phi \land \bigcirc \Box \phi
\end{aligned}
$$

Expansion for until

$P_{\mathsf{U}} = \mathit{Words}(\varphi \,\mathsf{U}\, \psi)$ satisfies:

$$P_{\mathsf{U}} = \mathit{Words}(\psi) \cup \left\{ A_0 A_1 A_2 \ldots \in \mathit{Words}(\varphi) \mid A_1 A_2 \ldots \in P_{\mathsf{U}} \right\}$$

and is the smallest LT-property P such that:

$$\mathit{Words}(\psi) \cup \left\{ A_0 A_1 A_2 \ldots \in \mathit{Words}(\varphi) \mid A_1 A_2 \ldots \in P \right\} \subseteq P \qquad (*)$$

Proof: $Words(\varphi \,\mathsf{U}\, \psi)$ is the smallest LT-prop. satisfying (*)

- Let P be any LT-property that satisfies (*). We show that $Words(\varphi \,\mathsf{U}\, \psi) \subseteq P$.
- Let $B_0 B_1 B_2 \ldots \in Words(\varphi \,\mathsf{U}\, \psi)$. Then there exists a $k \geq 0$ such that $B_i B_{i+1} B_{i+2} \ldots \in Words(\varphi)$ for every $0 \leq i < k$ and $B_k B_{k+1} B_{k+2} \ldots \in Words(\psi)$.
- We derive

$$
\begin{array}{ll}
 & B_k B_{k+1} B_{k+2} \ldots \in P \\
 & \text{because } B_k B_{k+1} B_{k+2} \ldots \in Words(\psi) \text{ and } Words(\psi) \subseteq P. \\
\Rightarrow & B_{k-1} B_k B_{k+1} B_{k+2} \ldots \in P \\
 & \text{because if } A_0 A_1 A_2 \ldots \in Words(\varphi) \text{ and } A_1 A_2 \ldots \in P \text{ then } A_0 A_1 A_2 \ldots \in P. \\
\Rightarrow & B_{k-2} B_{k-1} B_k B_{k+1} B_{k+2} \ldots \in P, \text{ analogously} \\
\Rightarrow & \ldots \\
\Rightarrow & B_0 B_1 B_2 \ldots \in P.
\end{array}
$$

Weak until

- The weak-until (or: unless) operator: $\varphi \, \mathsf{W} \, \psi \overset{\text{def}}{=} (\varphi \, \mathsf{U} \, \psi) \vee \Box \varphi$
  - as opposed to until, $\varphi \, \mathsf{W} \, \psi$ does not require a ψ-state to be reached
- Until U and weak until W are dual:

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

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

- Until and weak until are equally expressive:
  - $\Box\psi \equiv \psi \, \mathsf{W} \, \text{false}$ and $\varphi \, \mathsf{U} \, \psi \equiv (\varphi \, \mathsf{W} \, \psi) \wedge \neg \Box \neg\psi$
- Until and weak until satisfy the same expansion law
  - but until is the smallest, and weak until the largest solution!

Expansion for weak until

$P_{\mathsf{W}} = \mathit{Words}(\varphi \,\mathsf{W}\, \psi)$ satisfies:

$$P_{\mathsf{W}} = \mathit{Words}(\psi) \cup \left\{ A_0A_1A_2\ldots \in \mathit{Words}(\varphi) \mid A_1A_2\ldots \in P_{\mathsf{W}} \right\}$$

and is the greatest LT-property P such that:

$$\mathit{Words}(\psi) \cup \left\{A_0A_1A_2\ldots \in \mathit{Words}(\varphi) \mid A_1A_2\ldots \in P\right\} \supseteq P \quad (**)$$

Proof: $\mathit{Words}(\varphi \, \mathsf{W} \, \psi)$ is the greatest LT-prop. satisfying (**)

- Let P be any LT-property that satisfies (**). We show that $P \subseteq \mathit{Words}(\varphi \, \mathsf{W} \, \psi)$.
- Let $B_0 B_1 B_2 \ldots \notin \mathit{Words}(\varphi \, \mathsf{W} \, \psi)$. Then there exists a $k \geq 0$ such that $B_i B_{i+1} B_{i+2} \ldots \models \varphi \wedge \neg\psi$ for every $0 \leq i < k$ and $B_k B_{k+1} B_{k+2} \ldots \models \neg\varphi \wedge \neg\psi$.
- We derive

$$
\begin{array}{ll}
 & B_k B_{k+1} B_{k+2} \ldots \notin P \\
 & \text{because } B_k B_{k+1} B_{k+2} \ldots \notin \mathit{Words}(\psi) \text{ and} \\
 & B_k B_{k+1} B_{k+2} \ldots \notin \mathit{Words}(\varphi) \text{ and} \\
\Rightarrow & B_{k-1} B_k B_{k+1} B_{k+2} \ldots \notin P \\
 & \text{because } B_k B_{k+1} B_{k+2} \ldots \notin P \text{ and } B_{k-1} B_k B_{k+1} B_{k+2} \ldots \notin \mathit{Words}(\psi) \\
\Rightarrow & B_{k-2} B_{k-1} B_k B_{k+1} B_{k+2} \ldots \notin P, \text{ analogously} \\
\Rightarrow & \ldots \\
\Rightarrow & B_0 B_1 B_2 \ldots \notin P.
\end{array}
$$

(Weak-until) positive normal form

- Canonical form for LTL-formulas
  - negations only occur adjacent to atomic propositions
  - disjunctive and conjunctive normal form is a special case of PNF
  - for each LTL-operator, a dual operator is needed
  - e.g., $\neg(\varphi \,\mathsf{U}\, \psi) \equiv \big((\varphi \wedge \neg\psi) \,\mathsf{U}\, (\neg\varphi \wedge \neg\psi)\big) \vee \Box(\varphi \wedge \neg\psi)$
  - that is: $\neg(\varphi \,\mathsf{U}\, \psi) \equiv (\varphi \wedge \neg\psi) \,\mathsf{W}\, (\neg\varphi \wedge \neg\psi)$
- For $a \in AP$, the set of LTL formulas in PNF is given by:

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

  - $\Box$ and $\Diamond$ are also permitted: $\Box\varphi \equiv \varphi \,\mathsf{W}\, \text{false}$ and $\Diamond\varphi = \text{true} \,\mathsf{U}\, \varphi$

(Weak until) PNF is always possible

For each LTL-formula there exists an equivalent LTL-formula in PNF

Transformations:

$$\neg \text{true} \rightsquigarrow \text{false}$$
$$\neg \text{false} \rightsquigarrow \text{true}$$
$$\neg\neg\varphi \rightsquigarrow \varphi$$
$$\neg(\varphi \wedge \psi) \rightsquigarrow \neg\varphi \vee \neg\psi$$
$$\neg(\varphi \vee \psi) \rightsquigarrow \neg\varphi \wedge \neg\psi$$
$$\neg \bigcirc \varphi \rightsquigarrow \bigcirc \neg\varphi$$
$$\neg(\varphi \,\mathsf{U}\, \psi) \rightsquigarrow (\varphi \wedge \neg\psi) \,\mathsf{W}\, (\neg\varphi \wedge \neg\psi)$$
$$\neg(\varphi \,\mathsf{W}\, \psi) \rightsquigarrow (\phi \wedge \neg\psi) \,\mathsf{U}\, (\neg\phi \wedge \neg\psi)$$
$$\neg \Diamond \varphi \rightsquigarrow \Box \neg\varphi$$
$$\neg \Box \varphi \rightsquigarrow \Diamond \neg\varphi$$

but an exponential growth in size is possible

Example

Consider the LTL-formula $\neg \Box \big((a \,\mathsf{U}\, b) \vee \bigcirc c \big)$
This formula is not in PNF, but can be transformed into PNF as follows:

$$
\begin{aligned}
& \neg \Box \big((a \,\mathsf{U}\, b) \vee \bigcirc c \big) \\
\equiv\ & \Diamond \neg \big((a \,\mathsf{U}\, b) \vee \bigcirc c \big) \\
\equiv\ & \Diamond \big(\neg (a \,\mathsf{U}\, b) \wedge \neg \bigcirc c \big) \\
\equiv\ & \Diamond \big((a \wedge \neg b) \,\mathsf{W}\, (\neg a \wedge \neg b) \wedge \bigcirc \neg c \big)
\end{aligned}
$$

can the exponential growth in size be avoided?

The release operator

- The release operator: $\varphi \, \mathsf{R} \, \psi \overset{\text{def}}{=} \neg(\neg\varphi \, \mathsf{U} \, \neg\psi)$
  - ψ always holds, a requirement that is released as soon as φ holds
- Until U and release R are dual:

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

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

- Until and release are equally expressive:
  - $\Box\psi \equiv \text{false} \, \mathsf{R} \, \psi$ and $\varphi \, \mathsf{U} \, \psi \equiv \neg(\neg\varphi \, \mathsf{R} \, \neg\psi)$
- Release satisfies the expansion law:
  $\varphi \, \mathsf{R} \, \psi \equiv \psi \wedge (\varphi \vee \bigcirc(\varphi \, \mathsf{R} \, \psi))$

Semantics of release

$$\sigma \vDash \varphi \,\mathsf{R}\, \psi$$

iff (* definition of R *)

$$\neg\exists j \geq 0.\left(\sigma[j..] \vDash \neg\psi \wedge \forall i < j.\, \sigma[i..] \vDash \neg\varphi\right)$$

iff (* semantics of negation *)

$$\neg\exists j \geq 0.\left(\sigma[j..] \nvDash \psi \;\wedge\; \forall i < j.\, \sigma[i..] \nvDash \varphi\right)$$

iff (* duality of ∃ and ∀ *)

$$\forall j \geq 0.\, \neg\left(\sigma[j..] \nvDash \psi \;\wedge\; \forall i < j.\, \sigma[i..] \nvDash \varphi\right)$$

iff (* de Morgan's law *)

$$\forall j \geq 0.\left(\neg(\sigma[j..] \nvDash \psi) \;\vee\; \neg\forall i < j.\, \sigma[i..] \nvDash \varphi\right)$$

iff (* semantics of negation *)

$$\forall j \geq 0.\left(\sigma[j..] \vDash \psi \;\vee\; \exists i < j.\, \sigma[i..] \vDash \varphi\right)$$

iff

$$\forall j \geq 0.\, \sigma[j..] \vDash \psi \quad \text{or} \quad \exists i \geq 0.\left(\sigma[i..] \vDash \varphi \wedge \forall k \leq i.\, \sigma[k..] \vDash \psi\right)$$

Positive normal form (revisited)

For $a \in AP$, LTL formulas in PNF are given by:

$$\varphi \ ::= \ \text{true} \ \Big| \ \text{false} \ \Big| \ a \ \Big| \ \neg a \ \Big| \ \varphi_1 \wedge \varphi_2 \ \Big| \ \varphi_1 \vee \varphi_2 \ \Big| \ \bigcirc \varphi \ \Big| \ \varphi_1 \, \mathsf{U} \, \varphi_2 \ \Big| \ \varphi_1 \, \mathsf{R} \, \varphi_2$$

PNF in linear size

For any LTL-formula φ there exists
an equivalent LTL-formula ψ in PNF with $|\psi| = \mathcal{O}(|\varphi|)$

Transformations:

$$
\begin{array}{lcl}
\neg \mathsf{true} & \rightsquigarrow & \mathsf{false} \\
\neg \mathsf{false} & \rightsquigarrow & \mathsf{true} \\
\neg\neg\varphi & \rightsquigarrow & \varphi \\
\neg(\varphi \wedge \psi) & \rightsquigarrow & \neg\varphi \vee \neg\psi \\
\neg(\varphi \vee \psi) & \rightsquigarrow & \neg\varphi \wedge \neg\psi \\
\neg \bigcirc \varphi & \rightsquigarrow & \bigcirc \neg\varphi \\
\neg(\varphi \, \mathsf{U} \, \psi) & \rightsquigarrow & \neg\varphi \, \mathsf{R} \, \neg\psi \\
\neg(\varphi \, \mathsf{R} \, \psi) & \rightsquigarrow & \neg\varphi \, \mathsf{U} \, \neg\psi \\
\neg \Diamond \varphi & \rightsquigarrow & \Box \neg\varphi \\
\neg \Box \varphi & \rightsquigarrow & \Diamond \neg\varphi
\end{array}
$$