Model Checking

Linear Temporal Logic

[Baier & Katoen, Chapter 5.1]

Joost-Pieter Katoen and Tim Quatmann

Software Modeling and Verification Group

RWTH Aachen, SoSe 2022

Overview

Overview

Specifying LT Properties

- An LT property is a set of infinite traces over AP
- Specifying such sets explicitly is often inconvenient
- Mutual exclusion is specified over $AP = \{ c_1, c_2 \}$ by

  E_{mutex} = set of infinite words $A_0 A_1 \ldots$ with $\{ c_1, c_2 \} \not\subseteq A_i$ for all $0 \leq i$

- Starvation freedom is specified over $AP = \{ c_1, w_1, c_2, w_2 \}$ by

$E_{nostarve}$ = set of infinite words $A_0 A_1 \ldots$ such that:

there are ∞ many j s.t. ...

Proc. 2

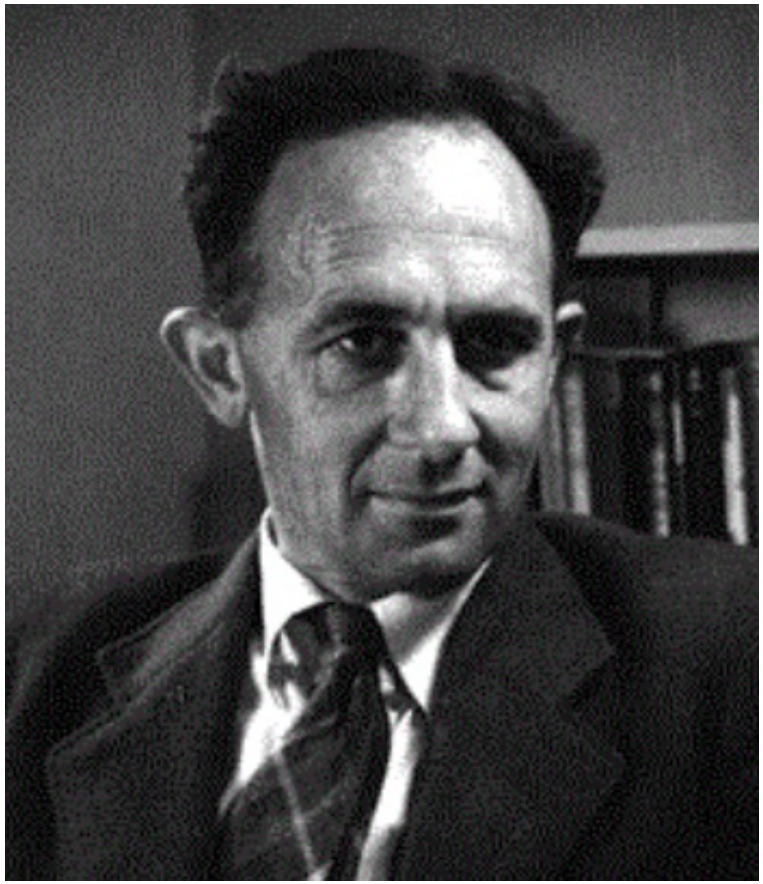
$$\left(\left(\overset{\infty}{\exists} j.\ w_1 \in A_j \right) \Rightarrow \left(\overset{\infty}{\exists} j.\ c_1 \in A_j \right) \right) \wedge \left(\left(\overset{\infty}{\exists} j.\ w_2 \in A_j \right) \Rightarrow \left(\overset{\infty}{\exists} j.\ c_2 \in A_j \right) \right)$$

∞ often Proc. 1 waits

∞ often Proc 1 is in crit.

Such properties can be specified much more succinctly using logic
(or using ω-regular expressions)

Linear Temporal Logic



Arthur Norman Prior
(1914–†1969)

Amir Pnueli
(1941–†2009)

LTL Syntax

Definition: LTL syntax

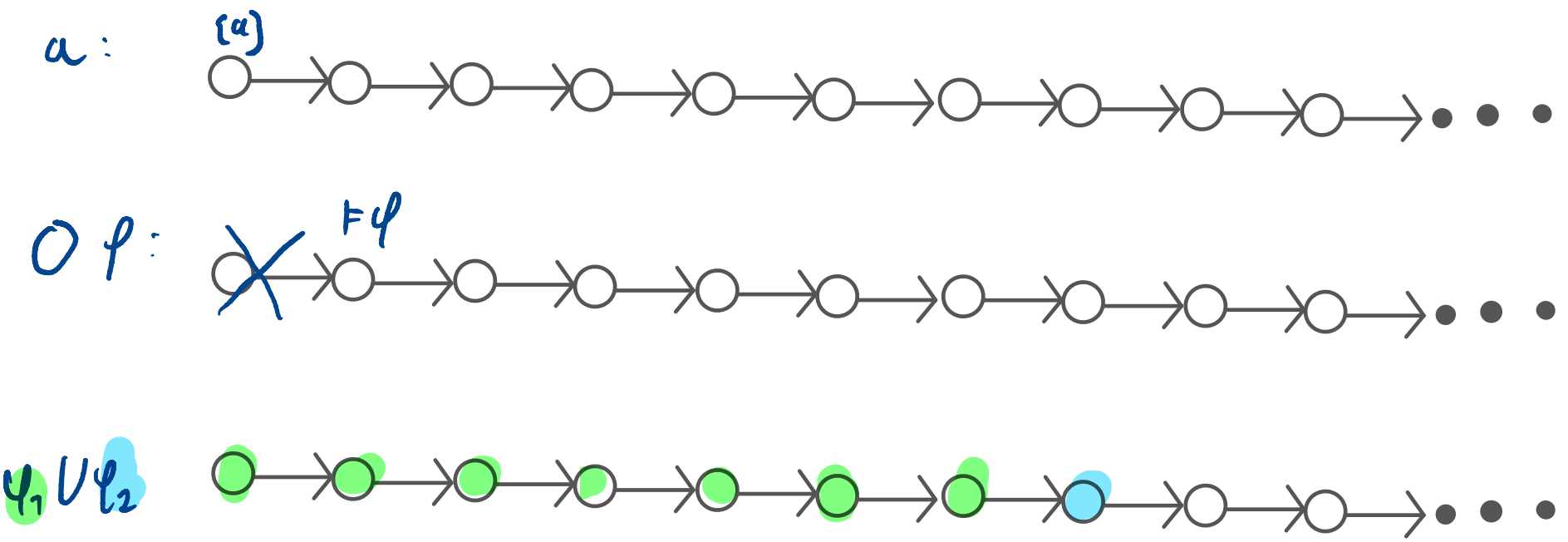
BNF grammar for LTL formulas with proposition $a \in AP$:

Backus Naur Form

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

"next φ" — "φ_1 until φ_2"

Prop. Logic — Modal operators



LTL Syntax

Definition: LTL syntax

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

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

- 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

LTL Syntax

Definition: 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

Derived Operators

"syntactic sugar"

$$\varphi \vee \psi \equiv \neg(\neg\varphi \wedge \neg\psi)$$

$$\varphi \Rightarrow \psi \equiv \neg\varphi \vee \psi$$ "implies"

$$\varphi \Leftrightarrow \psi \equiv (\varphi \Rightarrow \psi) \wedge (\psi \Rightarrow \varphi)$$

$$\varphi \oplus \psi \equiv (\varphi \wedge \neg\psi) \vee (\neg\varphi \wedge \psi)$$ "exclusive Or"

$$\text{true} \equiv \varphi \vee \neg\varphi$$

$$\text{false} \equiv \neg\,\text{true}$$

Derived Operators

$$\varphi \vee \psi \equiv \neg(\neg\varphi \wedge \neg\psi)$$

$$\varphi \Rightarrow \psi \equiv \neg\varphi \vee \psi$$

$$\varphi \Leftrightarrow \psi \equiv (\varphi \Rightarrow \psi) \wedge (\psi \Rightarrow \varphi)$$

$$\varphi \oplus \psi \equiv (\varphi \wedge \neg\psi) \vee (\neg\varphi \wedge \psi)$$

$$\text{true} \equiv \varphi \vee \neg\varphi$$

$$\text{false} \equiv \neg\,\text{true}$$

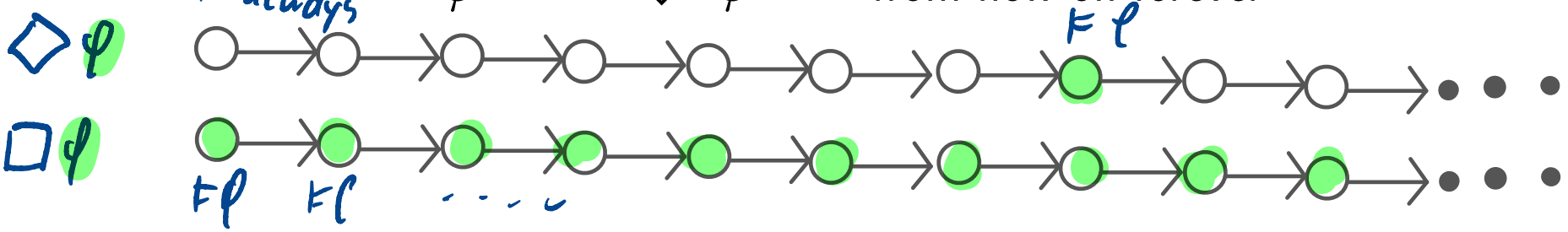
"eventually"

german: "irgendwann"

$$\Diamond\varphi \equiv \text{true}\,\mathsf{U}\,\varphi$$ "some time in the future"

"globally" / "always"

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



Derived Operators

$$\varphi \vee \psi \equiv \neg(\neg\varphi \wedge \neg\psi)$$

$$\varphi \Rightarrow \psi \equiv \neg\varphi \vee \psi$$

$$\varphi \Leftrightarrow \psi \equiv (\varphi \Rightarrow \psi) \wedge (\psi \Rightarrow \varphi)$$

$$\varphi \oplus \psi \equiv (\varphi \wedge \neg\psi) \vee (\neg\varphi \wedge \psi)$$

$\neg a \wedge b$
$\equiv (\neg a) \wedge b$

$$\text{true} \equiv \varphi \vee \neg\varphi$$

$$\text{false} \equiv \neg\,\text{true}$$

$a \wedge b \mathrel{U} c$
$\equiv a \wedge (b \mathrel{U} c)$

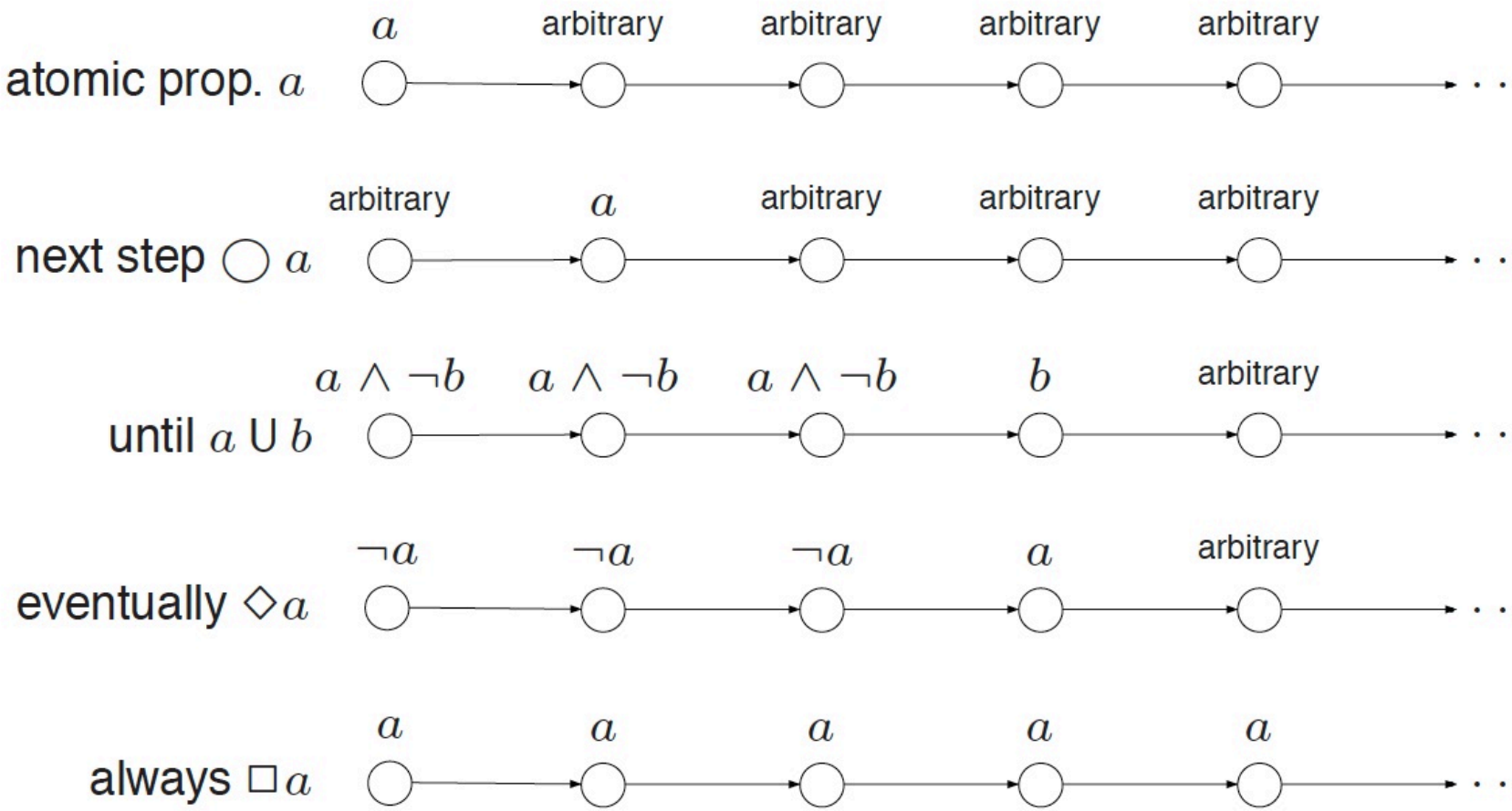
$$\Diamond\varphi \equiv \text{true}\,\mathsf{U}\,\varphi$$ "some time in the future"

$$\Box\varphi \equiv \neg\Diamond\neg\varphi$$ "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 $\wedge$, $\vee$, and $\Rightarrow$

Intuitive Semantics



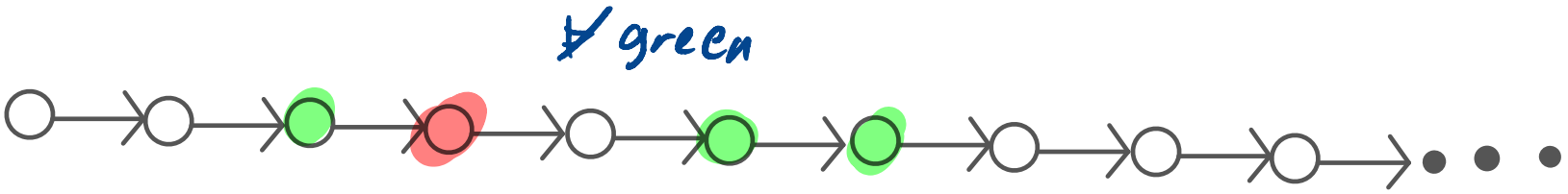
Example:Traffic Light Properties

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

Example:Traffic Light Properties

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

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

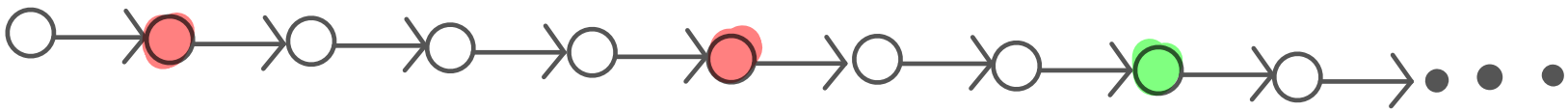


Example:Traffic Light Properties

- 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: $\Box\,(red \Rightarrow \Diamond\, green)$



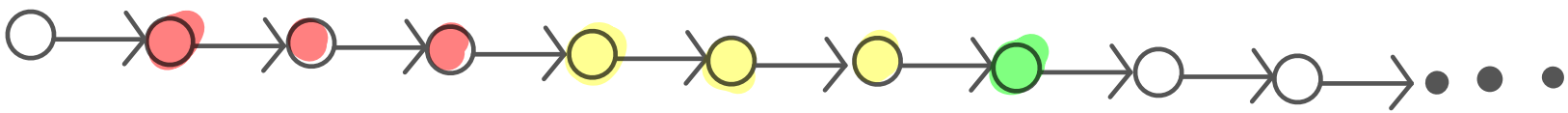
Example:Traffic Light Properties

- 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:

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



Example Properties in LTL

- Reachability
  - negated reachability $\Diamond \neg \psi$
  - conditional reachability $\varphi \, \mathsf{U} \, \psi$
  - reachability from any state not expressible

Example Properties in LTL

- Reachability
  - negated reachability $\Diamond \neg \psi$
  - conditional reachability $\varphi \, \mathsf{U} \, \psi$
  - reachability from any state not expressible
- Safety
  - simple safety $\Box \neg \varphi$
  - conditional safety $(\varphi \, \mathsf{U} \, \psi) \vee \Box \varphi$

Example Properties in LTL

- Reachability
  - negated reachability — $\Diamond \neg \psi$
  - conditional reachability — $\varphi \, \mathsf{U} \, \psi$
  - reachability from any state — not expressible
- Safety
  - simple safety — $\Box \neg \varphi$
  - conditional safety — "weak until" (Later today) $(\varphi \, \mathsf{U} \, \psi) \vee \Box \varphi$
- Liveness — $\Box (\varphi \Rightarrow \Diamond \psi)$ and others

Overview

Semantics Over Words

Definition: LTL semantics over infinite words

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

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

$\sigma = A_0 A_1 A_2 \cdots \qquad A_i \subseteq AP$

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

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

Semantics of □, ◇, □◇ and ◇□

$\sigma \models \Diamond \varphi$

iff $\sigma \models true \, U \, \varphi$

iff $\exists j \geq 0 \quad \sigma[j \ldots] \models \varphi$

$true \rightarrow \wedge \forall i < j \quad \sigma[i \ldots] \models true$

iff $\exists j \geq 0 \quad \sigma[j \ldots] \models \varphi$

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

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

$$\sigma \models \Box \varphi$$

iff $\sigma \models \neg \Diamond \neg \varphi$

iff $\sigma \not\models \Diamond \neg \varphi$

iff not $(\exists j \geq 0.\ \sigma[j..] \models \neg \varphi)$

iff $\forall j \geq 0.\ \sigma[j..] \not\models \neg \varphi$

$\not\models \neg \varphi \equiv \models \varphi$

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

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

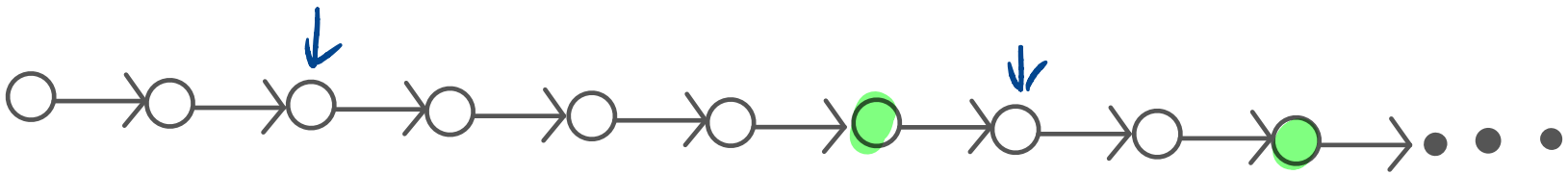
$$\sigma \models \Box\varphi \quad \text{iff} \quad \forall j \geq 0.\ \sigma[j..] \models \varphi$$

$$\sigma \models \Box\Diamond\varphi$$

"infinetly often φ"

iff $\forall j \geq 0\ \sigma[j\cdots] \models \Diamond\varphi$

iff $\forall j \geq 0\ \exists i \geq j\ \sigma[i\cdots] \models \varphi$



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

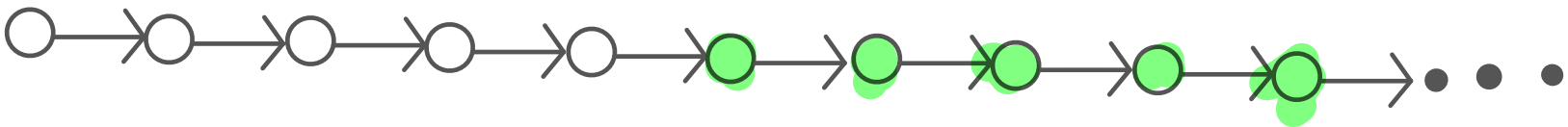
$$\sigma \models \Diamond \varphi \quad \text{iff} \quad \exists j \geq 0.\ \sigma[j..] \models \varphi$$

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

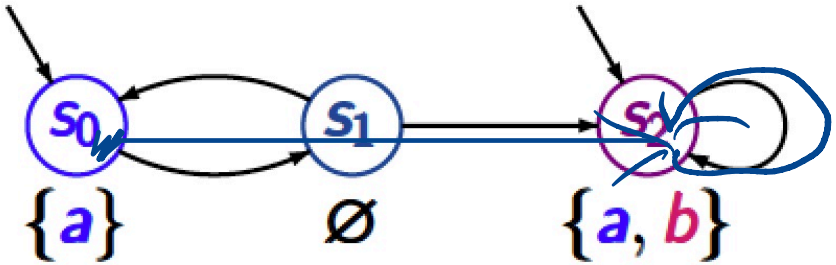
$$\sigma \models \Box\Diamond \varphi \quad \text{iff} \quad \forall j \geq 0.\ \exists i \geq j.\ \sigma[i \ldots] \models \varphi$$

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

Persistence Property



Example



$AP = \{a, b\}$

path $\pi = s_0\, s_1\, s_2\, s_2\, s_2\, s_2 \ldots$ $\quad$ $trace(\pi) = \{a\}\,\varnothing\,\{a, b\}^\omega$

$\pi \models a$, but $\pi \not\models b$	as $L(s_0) = \{a\}$
$\pi \models \bigcirc(\neg a \wedge \neg b)$	as $L(s_1) = \varnothing$
$\pi \models \bigcirc\bigcirc(a \wedge b)$	as $L(s_2) = \{a, b\}$
$\pi \models (\neg b)\ \mathsf{U}\ (a \wedge b)$	as $s_0, s_1 \models \neg b$
$\pi \models (\neg b)\ \mathsf{U}\ \Box(a \wedge b)$	and $s_2 \models a \wedge b$

Semantics over Paths and States

Let $TS = (S, Act, \rightarrow, I, AP, L)$ be a transition system and φ be an LTL-formula over AP.

- For infinite path fragment π of TS:

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

- For state $s \in S$:

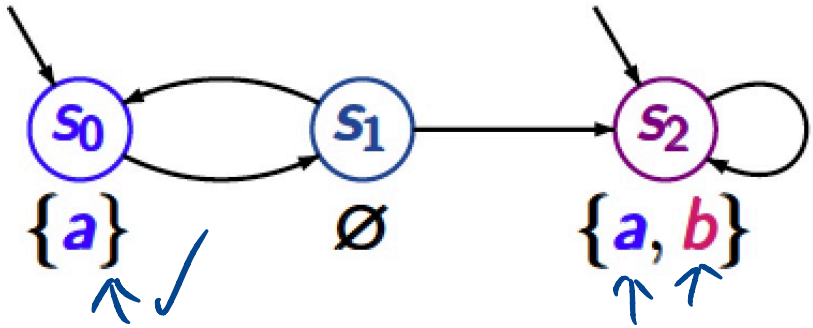
$$s \models \varphi \quad \text{iff} \quad \forall \pi \in Paths(s).\ \pi \models \varphi$$

- For transition system TS:

$$TS \models \varphi \quad \text{iff} \quad Traces(TS) \subseteq Words(\varphi) \quad \text{iff} \quad \forall s \in I.\ s \models \varphi$$

iff $\forall \sigma \in Traces(TS) : \sigma \models \varphi$

Example



$AP = \{a, b\}$

$\mathcal{T} \models a$ as $s_0 \models a$ and $s_2 \models a$

$\mathcal{T} \not\models \Diamond\Box a$ as $s_0\, s_1\, s_0\, s_1 \ldots \not\models \Diamond\Box a$

$\mathcal{T} \models \Diamond\Box b \vee \Box\Diamond(\neg a \wedge \neg b)$ as $s_2 \models b$, $s_1 \not\models a, b$

$\mathcal{T} \models \Box(a \rightarrow ((\bigcirc\neg a) \vee b))$ as $s_2 \models b$, $s_0 \models \bigcirc\neg a$

refer to same position

On The Semantics of Negation

For paths, it holds $\pi \models \varphi$ if and only if $\pi \not\models \neg\varphi$ since:

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

But $TS \models \varphi$ and $TS \not\models \neg\varphi$ are not equivalent

$TS \models \varphi$ iff $\forall \sigma \in Traces(TS) : \sigma \in \varphi$

$TS \not\models \neg\varphi$ iff $\neg(\forall \sigma \in Traces(TS) : \sigma \models \neg\varphi)$

iff $\exists \sigma \in Traces(TS) : \sigma \not\models \neg\varphi$

iff $\exists \sigma \in Traces(TS) : \sigma \models \varphi$

On The Semantics of Negation

For paths, it holds $\pi \models \varphi$ if and only if $\pi \not\models \neg\varphi$ since:

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

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

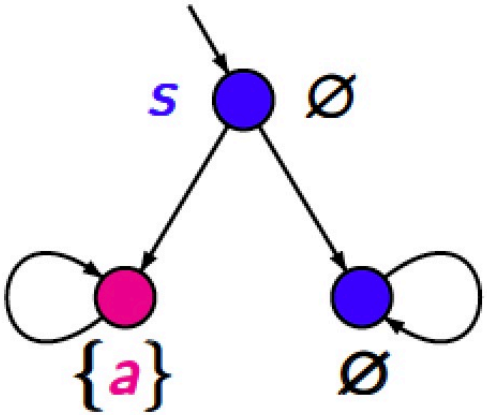
It holds: $TS \models \neg\varphi$ implies $TS \not\models \varphi$. Not always the reverse!

Note that:

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

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

Example



$s \not\models \Diamond a$ and $s \not\models \neg\Diamond a$

iff $\exists \sigma \in Traces(s)$:

$\sigma \not\models \Diamond a$

LTL Formulas for LT Properties

Provide LTL formulas over $AP = \{ a, b \}$ for the LT properties:

- set of all words $A_0 A_1 \ldots$ over $\left(2^{AP}\right)^\omega$ such that:

"whenever a holds, then b was true before"

$$\forall i \geq 0.\ (a \in A_i \ \Rightarrow\ i > 0 \ \wedge\ b \in A_{i-1})$$

$$\equiv\ \forall j \geq 0.\ \left(b \in A_j \ \vee\ a \notin A_{j+1}\right)$$

$$\equiv\ \mathit{Words}(\ \Box\,(b \ \vee\ \neg \bigcirc a)\ )$$

LTL Formulas for LT Properties

Provide LTL formulas over $AP = \{ a, b \}$ for the LT properties:

- set of all words $A_0 A_1 \ldots$ over $\left(2^{AP}\right)^\omega$ such that:

$$\begin{aligned} & \forall i \geq 0.\ (a \in A_i \ \Rightarrow\ i > 0 \ \wedge\ b \in A_{i-1}) \\ \equiv\ & \forall j \geq 0.\ \left(b \in A_j \ \vee\ a \notin A_{j+1}\right) \\ \equiv\ & \mathit{Words}(\ \Box\,(b \ \vee\ \neg \bigcirc a)\ ) \end{aligned}$$

- set of all words of the form

$$\{ b \}^{n_1} \{ a \} \{ b \}^{n_2} \{ a \} \{ b \}^{n_3} \{ a \} \ldots$$

where $n_i \geq 0$. This is captured by

$$\mathit{Words}(\ \Box\,((b \wedge \neg a)\,\mathsf{U}\,(a \wedge \neg b))\ )$$

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:

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

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

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

$\equiv \neg(\neg \bigcirc \neg \varphi)$

$\sigma \models \neg \bigcirc \varphi$

iff $\sigma \not\models \bigcirc \varphi$

iff $\sigma[1..] \not\models \varphi$

iff $\sigma[1..] \models \neg \varphi$

iff $\sigma \models \bigcirc \neg \varphi$

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

Absorption:

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

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

Distributive:

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

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

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

Absorption and Distributive

Absorption:

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

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

Distributive:

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

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

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

but .....:

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

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

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

Let $\varphi = a$ $\psi = b$

$\sigma = (\{a\}\{b\})^\omega$

$\sigma \models \varphi_1$ but $\sigma \not\models \varphi_2$

Expansion Law

Expansion: $\varphi \mathsf{U} \psi \equiv \psi \vee (\varphi \wedge \bigcirc(\varphi \mathsf{U} \psi))$

$\Diamond \varphi \equiv \varphi \vee \bigcirc \Diamond \varphi$

$\Box \varphi \equiv \varphi \wedge \bigcirc \Box \varphi$

Proof for : $\varphi \mathrel{U} \psi \quad \equiv \quad \psi \vee (\varphi \wedge \bigcirc(\varphi \mathrel{U} \psi))$

$\sigma \models \varphi \mathrel{U} \psi$

iff $\exists\, j \geq 0 : \sigma[j..] \models \psi \wedge \forall\, i < j \;\; \sigma[i..] \models \varphi$

"$j = 0$" iff $\sigma \models \psi \vee \big(\exists\, j \geq 1 : \sigma[j..] \models \psi \wedge$

"$i = 0$" $\sigma \models \varphi \wedge \forall\, 1 \leq i < j \;\; \sigma[i..] \models \varphi\big)$

iff $\sigma \models \psi \vee \big(\sigma \models \varphi \wedge \exists\, j \geq 1 : \sigma[j..] \models \psi$

$\wedge \forall\, 1 \leq i \leq j : \sigma[i..] \models \varphi\big)$

iff $\sigma \models \psi \vee \big(\sigma \models \varphi \wedge \sigma \models \bigcirc(\varphi \mathrel{U} \psi)\big)$

iff $\sigma \models \psi \vee \big(\varphi \wedge \bigcirc(\varphi \mathrel{U} \psi)\big)$

Proof for

$\Diamond \varphi \equiv \varphi \vee \bigcirc \Diamond \varphi$

$\Diamond \varphi \equiv true \, U \, \varphi$

// Expansion for U

$\equiv \varphi \vee (true \wedge \bigcirc (true \, U \, \varphi))$

$\equiv \varphi \vee \bigcirc \Diamond \varphi$

Proof for $\Box\varphi \equiv \varphi \wedge \bigcirc\Box\varphi$

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

// Expansion for $\Diamond$

$\equiv \neg(\neg\varphi \vee \bigcirc\Diamond\neg\varphi)$

$\equiv \neg\neg\varphi \wedge \neg\bigcirc\Diamond\neg\varphi$

$\equiv \varphi \wedge \bigcirc\neg\Diamond\neg\varphi$

$\equiv \varphi \wedge \bigcirc\Box\varphi$

Expansion for Until

$\mathit{Words}(\varphi \,\mathsf{U}\, \psi)$ is the smallest LT-property P such that:

1. $\mathit{Words}(\psi) \subseteq P$, and
2. $\{A_0 A_1 A_2 \ldots \in \mathit{Words}(\varphi) \mid A_1 A_2 \ldots \in P\} \subseteq P$

where smallest is w.r.t. the $\subseteq$-ordering on sets (of infinite words).

In fact, $\mathit{Words}(\varphi \,\mathsf{U}\, \psi)$ equals

$$\mathit{Words}(\psi) \cup \{A_0 A_1 A_2 \ldots \in \mathit{Words}(\varphi) \mid A_1 A_2 \ldots \in \mathit{Words}(\varphi \,\mathsf{U}\, \psi)\}.$$

Proof for :

Words(φ U ψ) is the smallest LT-property P such that:

1. *Words*(ψ) $\subseteq$ P, and
2. $\{A_0A_1A_2\ldots \in \mathit{Words}(\varphi) \mid A_1A_2\ldots \in P\} \subseteq P$

where smallest is w.r.t. the $\subseteq$-ordering on sets (of infinite words).

equivalent

Consider

$$\mathit{Words}(\psi) \cup \{\sigma \in \mathit{Words}(\varphi) \mid \sigma[1\ldots] \in P\} \subseteq P \quad (*)$$

To show:

(a) $P = \mathit{Words}(\varphi \,U\, \psi)$ implies $(*)$

(b) $\forall P \subseteq (2^{AP})^\omega$. P satisfies $(*)$ implies $\mathit{Words}(\varphi \,U\, \psi) \subseteq P$

We only show (b). Assume P satisfies $(*)$. Then

(i) $\mathit{words}(\psi) \subseteq P$

(ii) $\sigma \in \mathit{words}(\varphi)$ and $\sigma[1\ldots] \in P$ implies $\sigma \in P$

To show: $\mathit{words}(\varphi \,U\, \psi) \subseteq P$

Consider $\sigma \in \mathit{words}(\varphi \,U\, \psi)$. Then there is $k \geq 0$ s.t.

(iii) $\sigma[i\ldots] \in \mathit{words}(\varphi)$ for all $i < k$ and

(iv) $\sigma[k\ldots] \in \mathit{words}(\psi)$

(i), (iv) $\rightsquigarrow$ we get $\sigma[k\ldots] \in P$

(iii) $\rightsquigarrow$ we get $\sigma[k-1\ldots] \in \mathit{words}(\varphi)$

} (v)

(ii), (v) $\rightsquigarrow$ $\sigma[k-1\ldots] \in P$

Thus $\sigma[k\ldots] \in P$ implies $\sigma[k-1\ldots] \in P$

Repeating this for k steps yields $\sigma \in P$ $\square$

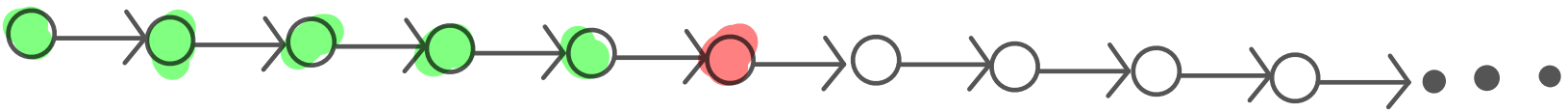
Weak Until

Definition: the weak-until-operator

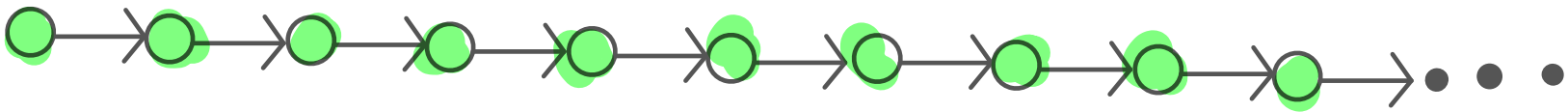
The weak-until (or: unless) operator is defined by

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

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



or



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

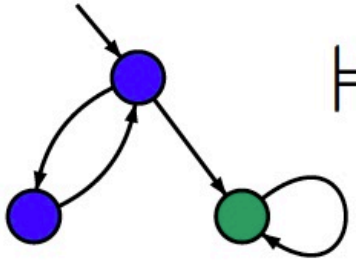
Until U and weak until W are dual:

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

$\Box\varphi \equiv \varphi \,\mathsf{W}\, \mathit{false}$

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

Example

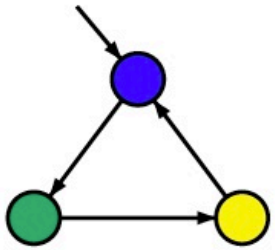


$\models a \mathbf{W} b$

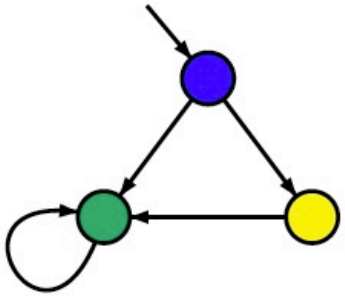
$\bigcirc \mathrel{\widehat{=}} \{a\}$

$\bigcirc \mathrel{\widehat{=}} \{b\}$

$\bigcirc \mathrel{\widehat{=}} \varnothing$



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



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

Expansion for Weak Until

Recall: $\mathit{Words}(\varphi \,\mathsf{U}\, \psi)$ is the smallest LT property P such that

$$\mathit{Words}(\psi) \cup \{A_0 A_1 A_2 \ldots \in \mathit{Words}(\varphi) \mid A_1 A_2 \ldots \in P\} \subseteq P.$$

$\mathit{Words}(\varphi \,\mathsf{W}\, \psi)$ is the largest LT-property P such that:

$$\mathit{Words}(\psi) \cup \{A_0 A_1 A_2 \ldots \in \mathit{Words}(\varphi) \mid A_1 A_2 \ldots \in P\} \supseteq P$$

where largest is w.r.t. the $\subseteq$ ordering on sets (of infinite words).

Overview

The Release Operator

Definition: release operator

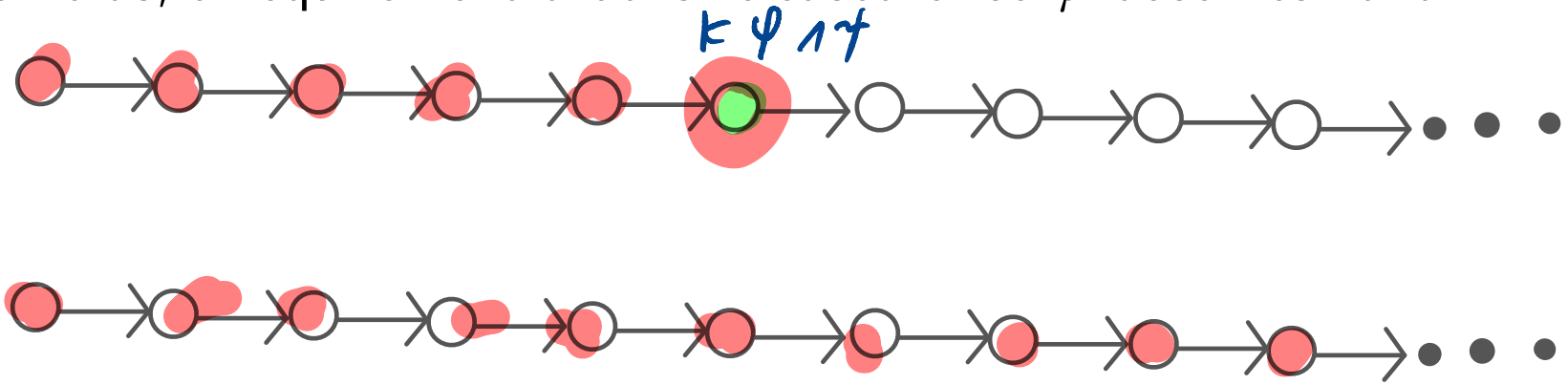
The release operator is defined by

$$\varphi \,\mathsf{R}\, \psi \;=\; \neg\,(\neg\varphi \,\mathsf{U}\, \neg\psi)\,.$$

Semantics:

$$\sigma \vDash \varphi \,\mathsf{R}\, \psi \quad \text{iff} \quad \sigma \vDash \Box\psi \vee \big(\exists i.\ (\sigma[i..] \vDash \varphi \wedge \forall k \leq i.\sigma[k..] \vDash \psi)\big)$$

ψ always holds, a requirement that is released once φ becomes valid



The Release Operator

Definition: release operator

The release operator is defined by

$$\varphi \,\mathsf{R}\, \psi \;=\; \neg\left(\neg\varphi \,\mathsf{U}\, \neg\psi\right).$$

Semantics:

$$\sigma \vDash \varphi \,\mathsf{R}\, \psi \quad \text{iff} \quad \sigma \vDash \Box\psi \vee \exists i.\ (\sigma[i..] \vDash \varphi \wedge \forall k \leq i . \sigma[k..] \vDash \psi)$$

ψ always holds, a requirement that is released once φ becomes valid
It follows:

$$\begin{aligned} \Box\varphi &\equiv \mathsf{false}\,\mathsf{R}\,\varphi \\ \varphi \,\mathsf{W}\, \psi &\equiv \psi \,\mathsf{R}\, (\varphi \vee \psi)) \\ \varphi \,\mathsf{R}\, \psi &\equiv \psi \wedge \left(\varphi \vee \bigcirc(\varphi \,\mathsf{R}\, \psi)\right) \end{aligned}$$

✓ l'exp Lamir

The Semantics of Release

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

iff **(* definition of R *)**

$$\sigma \vDash \neg\,(\neg\varphi \,\mathsf{U}\, \neg\psi)$$

iff **(* definition of U *)**

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

iff **(* semantics of negation *)**

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

iff **(* duality of $\exists$ and $\forall$ *)**

$$\forall j \geq 0.\ \neg\Big(\sigma[j..] \nvDash \psi \ \ \wedge\ \ \forall i < j.\ \sigma[i..] \nvDash \varphi\Big)$$

iff **(* de Morgan's law *)**

$$\forall j \geq 0.\ \Big(\neg(\sigma[j..] \nvDash \psi) \ \ \vee\ \ \neg\forall i < j.\ \sigma[i..] \nvDash \varphi\Big)$$

iff **(* semantics of negation *)**

$$\forall j \geq 0.\ \Big(\sigma[j..] \vDash \psi \ \ \vee\ \ \exists i < j.\ \sigma[i..] \vDash \varphi\Big)$$

iff

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

Positive Normal Form

Definition: positive normal form

The LTL-formula φ is in positive normal form (PNF) if it is of the form:

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

As $\Box\varphi \equiv \text{false}\,\mathsf{R}\,\varphi$, $\Box\varphi$ is in PNF; $\Diamond\varphi \equiv \text{true}\,\mathsf{U}\,\varphi$ is in PNF too.

negations $\neg\varphi$ are only allowed if $\varphi = a$ for some $a \in AP$

Positive Normal Form

Definition: positive normal form

The LTL-formula φ is in positive normal form (PNF) if it is of the form:

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

As $\Box\varphi \equiv \mathsf{false}\,\mathsf{R}\,\varphi$, $\Box\varphi$ is in PNF; $\Diamond\varphi \equiv \mathsf{true}\,\mathsf{U}\,\varphi$ is in PNF too.

For each LTL-formula φ, there exists an equivalent LTL-formula ψ in PNF such that $|\psi| \in O(|\varphi|)$.

Proof.

Transformation rules to push negations into the LTL-formula φ, in particular $\neg\bigcirc\varphi \equiv \bigcirc\neg\varphi$ and $\neg(\varphi\,\mathsf{U}\,\psi) \equiv \neg\varphi\,\mathsf{R}\,\neg\psi$. □

Overview

Summary

- Linear temporal logic (LTL) is a logic to succinctly describe LT properties
- LTL-formulas are equivalent iff they describe the same LT properties
- The until-operator is the smallest solution of an expansion law
- The weak until-operator is the largest solution of that expansion law
- An LTL-formula is in positive normal form if negations only occur adjacent to propositions
- Each LTL-formula can be transformed into an equivalent LTL-formula in PNF

Next Lecture

Monday May 9, 10:30