

Chapter 4

LTL model checking

Course “Specification and Verification of Parallel Systems”

Juliane Päßler, Tobias John

Spring 2024



Section

LTL formulas

Spring 2024

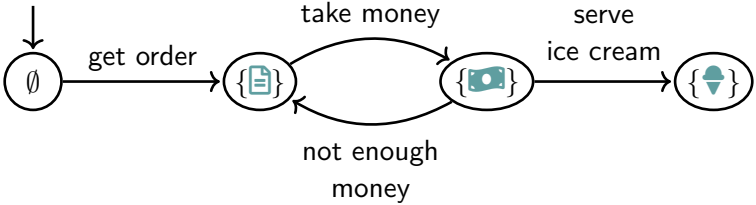
Overview

- repeat: labeled transition systems
- LTL
  - Syntax and semantic
  - Example properties
  - Dual operators + complete sets of operators



Example: Infinite

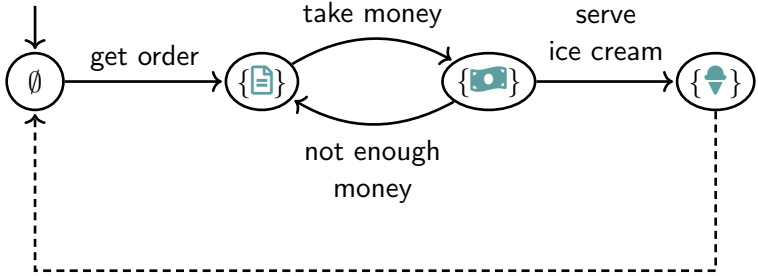
- model: the customers always return to ice cream shop



How is a labeled transition system defined?

Example: Infinite

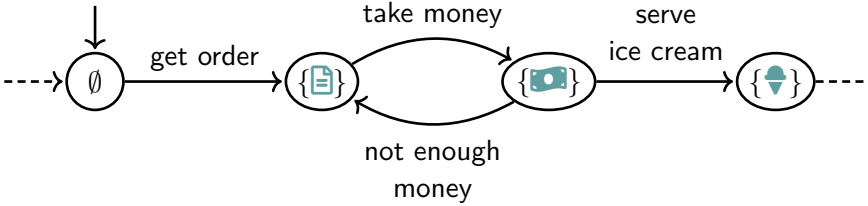
- model: the customers always return to ice cream shop



What new paths are now possible?

Example: Infinite

- model: the customers always return to ice cream shop



What new paths are now possible?

LTL: speaking about "time"

- **linear** time temporal logic
- first proposed by Pnueli in 1977
- one central temporal logic in CS
- supported by Spin and other model checkers
- we assume time is a *sequence* of discrete points in time
- we can express occurrence and order of events
- E.g.:
  - p holds in i and every following point (the future)
  - p holds in i and every preceding point (the past)



Amir Pnueli
(1941–2009)

$$\ldots \longrightarrow \bullet^{p}_{i-2} \longrightarrow \bullet^{p}_{i-1} \longrightarrow \bullet^{p}_{i} \longrightarrow \bullet^{p}_{i+1} \longrightarrow \bullet^{p}_{i+2} \longrightarrow \ldots$$

Syntax

ψ			propositional/first-order formula
φ	$::=$	ψ	formulas of the "core" logics
	$\mid$	$\neg\varphi \mid \varphi \wedge \varphi \mid \varphi \rightarrow \varphi \mid \ldots$	boolean combinations
	$\mid$	$\bigcirc\varphi$	next φ
	$\mid$	$\Box\varphi$	always φ
	$\mid$	$\Diamond\varphi$	eventually φ
	$\mid$	$\varphi \; U \; \varphi$	"until"
	$\mid$	$\varphi \; R \; \varphi$	"release"
	$\mid$	$\varphi \; W \; \varphi$	"waiting for", "weak until"



Illustrations

$\pi \models \Box p$



$\pi \models \Diamond p$



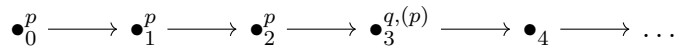
$\pi \models \bigcirc p$



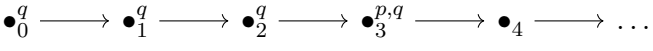


Some more illustrations

$\pi \models p\ U\ q$ (sequence of p's is *finite*)

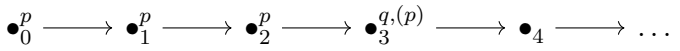


$\pi \models p\ R\ q$ (sequence of qs may be infinite)



$\pi \models p\ W\ q$

The sequence of ps may be infinite. ($p\ W\ q \sim p\ U\ q \vee \Box p$).



Semantics: Paths and computations



Definition (Path)

- A **path** is an infinite sequence

$$\pi = s_0, s_1, s_2, \ldots$$

  of states.
- π^k denotes the *path* $s_k, s_{k+1}, s_{k+2}, \ldots$
- π_k denotes the *state* s_k.

Semantics

$$
\begin{array}{lll}
\pi \models \psi & \text{iff} & \pi_0 \models_{\text{ul}} \psi \text{ with } \psi \text{ from the underlying core language} \\
\pi \models \neg\varphi & \text{iff} & \pi \not\models \varphi \\
\pi \models \varphi_1 \wedge \varphi_2 & \text{iff} & \pi \models \varphi_1 \text{ and } \pi \models \varphi_2 \\
\pi \models \bigcirc\varphi & \text{iff} & \pi^1 \models \varphi \\
\pi \models \varphi_1 \; U \; \varphi_2 & \text{iff} & \pi^k \models \varphi_2 \text{ for some } k \geq 0, \text{ and} \\
 & & \pi^i \models \varphi_1 \text{ for every } i \text{ such that } 0 \leq i < k
\end{array}
$$



Semantics: derived operators

$\pi \models \Box\varphi$ iff $\pi^k \models \varphi$ for all $k \geq 0$

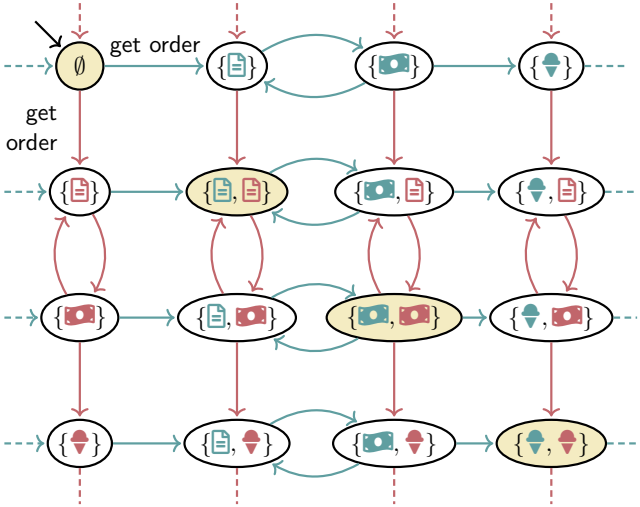
$\pi \models \Diamond\varphi$ iff $\pi^k \models \varphi$ for some $k \geq 0$

$\pi \models \varphi_1 \; R \; \varphi_2$ iff for every $j \geq 0$,
if $\pi^i \not\models \varphi_1$ for every $i < j$ then $\pi^j \models \varphi_2$

$\pi \models \varphi_1 \; W \; \varphi_2$ iff $\pi \models \varphi_1 \; U \; \varphi_2$ or $\pi \models \Box\varphi_1$



Example: Infinite



$\Diamond\Box$ 

$\Box(\Diamond$ $\wedge \Diamond$ $)$

$\Box($  $\rightarrow \Diamond$  $)$

$\bigcirc($  $\rightarrow (\neg$  $)\ W$  $)$

Validity and semantic equivalence

Definition (Validity and equivalence)

- φ is **(temporally) valid** , written $\models \varphi$, if
  $\pi \models \varphi$ for all paths π.



Validity and semantic equivalence

Definition (Validity and equivalence)

- φ is **(temporally) valid** , written $\models \varphi$, if
$$\pi \models \varphi \text{ for all paths } \pi.$$
- φ_1 and φ_2 are **equivalent** , written $\varphi_1 \sim \varphi_2$, if
$$\models \varphi_1 \leftrightarrow \varphi_2 \text{ (i.e. } \pi \models \varphi_1 \text{ iff } \pi \models \varphi_2, \text{ for all } \pi).$$



Validity and semantic equivalence

Definition (Validity and equivalence)

- φ is **(temporally) valid** , written $\models \varphi$, if
$$\pi \models \varphi \text{ for all paths } \pi.$$
- φ_1 and φ_2 are **equivalent** , written $\varphi_1 \sim \varphi_2$, if
$$\models \varphi_1 \leftrightarrow \varphi_2 \text{ (i.e. } \pi \models \varphi_1 \text{ iff } \pi \models \varphi_2, \text{ for all } \pi).$$

Example

$\Box$ distributes over $\wedge$, while $\Diamond$ distributes over $\vee$.

$$\Box(\varphi \wedge \psi) \sim (\Box\varphi \wedge \Box\psi)$$
$$\Diamond(\varphi \vee \psi) \sim (\Diamond\varphi \vee \Diamond\psi)$$





Section

Example Properties

Spring 2024

Formalization of “informal” properties

Example (Informal statement: “when φ then ψ”)

- $\varphi \rightarrow \psi$?
- $\Box(\varphi \rightarrow \psi)$?
- $\varphi \rightarrow \Diamond\psi$?
- $\Box(\varphi \rightarrow \Diamond\psi)$?



Formalization of “informal” properties

Example (Informal statement: “when φ then ψ”)

- $\varphi \to \psi$? $\varphi \to \psi$ holds in the initial state.
- $\Box(\varphi \to \psi)$? $\varphi \to \psi$ holds in every state.
- $\varphi \to \Diamond\psi$? if φ holds in the initial state, ψ will hold in some state.
- $\Box(\varphi \to \Diamond\psi)$? “response”



Some examples

Example (Temporal properties)

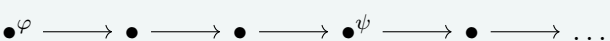
1. If φ holds initially, then ψ holds eventually.
2. Every φ-position is responded by a later ψ-position (**response**)
3. There are **infinitely** many ψ-positions.
4. Sooner or later, φ will hold *permanently* (**permanence** , **stabilization**).
5. The first φ-position must coincide or be preceded by a ψ-position.
6. Every φ-position initiates a sequence of ψ-positions, and if terminated, by a χ-position.



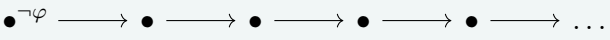
Example

Example

$\varphi \to \Diamond\psi$: If φ holds initially, then ψ holds eventually.



This formula will also hold in every path where φ does not hold initially.



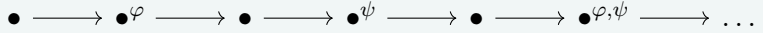


Response

Example (Response)

$\Box(\varphi \rightarrow \Diamond\psi)$

Every φ-position coincides with or is followed by a ψ-position.



This formula will also hold in every path where φ never holds.





Example: ∞

Example (∞)

$\Box\Diamond\psi$

There are infinitely many ψ-positions.



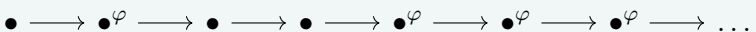


Permanence

Example (Permanence)

$\Diamond\Box\varphi$

Eventually φ will hold **permanently.**



Equivalently: there are *finitely* many $\neg\varphi$-positions.

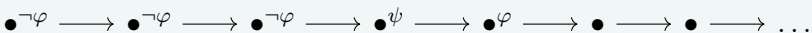


And another one

Example

$(\neg\varphi)\ W\ \psi$

The first φ-position must coincide or be preceded by a ψ-position.



φ may never hold



LTL example

Example

$\square(\varphi \rightarrow \psi \ W \ \chi)$

Every φ-position initiates a sequence of ψ-positions, and if terminated, by a χ-position.

$$\bullet \longrightarrow \bullet^{\varphi,\psi} \longrightarrow \bullet^{\psi} \longrightarrow \bullet^{\psi} \longrightarrow \bullet^{\chi} \longrightarrow \bullet \longrightarrow \bullet^{\varphi,\psi} \longrightarrow \ldots$$

The sequence of ψ-positions need not terminate.

$$\bullet \longrightarrow \bullet^{\varphi,\psi} \longrightarrow \bullet^{\psi} \longrightarrow \bullet^{\psi} \longrightarrow \bullet^{\psi} \longrightarrow \bullet^{\psi} \longrightarrow \bullet^{\psi} \longrightarrow \ldots$$





Section

Dual Operators

Spring 2024

Duality

Definition (Duals)

For binary boolean connectives $\circ$ and $\bullet$, we say that $\bullet$ is the **dual** of $\circ$ if

$$\neg(\varphi \circ \psi) \sim (\neg\varphi \bullet \neg\psi).$$

Similarly for unary connectives: $\bullet$ is the dual of $\circ$ if $\neg \circ \varphi \sim \bullet\neg\varphi$.

Duality is *symmetric*:

- If $\bullet$ is the dual of $\circ$ then
- $\circ$ is the dual of $\bullet$, thus
- we may refer to two connectives as dual (of each other).



Dual connectives

- $\wedge$ and $\vee$ are duals:

$$\neg(\varphi \wedge \psi) \sim (\neg\varphi \vee \neg\psi).$$



Dual connectives

- $\wedge$ and $\vee$ are duals:

$$\neg(\varphi \wedge \psi) \sim (\neg\varphi \vee \neg\psi).$$

- $\neg$ is its own dual:

$$\neg\neg\varphi \sim \neg\neg\varphi.$$



Dual connectives

- $\wedge$ and $\vee$ are duals:
$$\neg(\varphi \wedge \psi) \sim (\neg\varphi \vee \neg\psi).$$
- $\neg$ is its own dual:
$$\neg\neg\varphi \sim \neg\neg\varphi.$$
- What is the dual of $\rightarrow$?



Dual connectives

- $\wedge$ and $\vee$ are duals:
$$\neg(\varphi \wedge \psi) \sim (\neg\varphi \vee \neg\psi).$$
- $\neg$ is its own dual:
$$\neg\neg\varphi \sim \neg\neg\varphi.$$
- What is the dual of $\rightarrow$? It's $\not\leftarrow$:
$$\neg(\varphi \not\leftarrow \psi)$$



Dual connectives

- $\wedge$ and $\vee$ are duals:
$$\neg(\varphi \wedge \psi) \sim (\neg\varphi \vee \neg\psi).$$
- $\neg$ is its own dual:
$$\neg\neg\varphi \sim \neg\neg\varphi.$$
- What is the dual of $\rightarrow$? It's $\not\leftarrow$:
$$\begin{aligned}\neg(\varphi \not\leftarrow \psi) &\sim \varphi \leftarrow \psi \\ &\sim \psi \rightarrow \varphi \\ &\sim \neg\varphi \rightarrow \neg\psi\end{aligned}$$



Complete sets of connectives

- A set of connectives is *complete* (for boolean formulae) if every other connective can be defined in terms of them.
- Our set of connectives ($\{\wedge, \neg, \rightarrow\}$) is complete (e.g., $\not\leftarrow$ can be defined), but also subsets of it, so we don't actually need all the connectives.



Complete sets of connectives

- A set of connectives is *complete* (for boolean formulae) if every other connective can be defined in terms of them.
- Our set of connectives ($\{\wedge, \neg, \rightarrow\}$) is complete (e.g., $\not\leftarrow$ can be defined), but also subsets of it, so we don't actually need all the connectives.

Example

$\{\vee, \neg\}$ is complete.



Complete sets of connectives

- A set of connectives is *complete* (for boolean formulae) if every other connective can be defined in terms of them.
- Our set of connectives ($\{\wedge, \neg, \rightarrow\}$) is complete (e.g., $\not\leftarrow$ can be defined), but also subsets of it, so we don't actually need all the connectives.

Example

$\{\vee, \neg\}$ is complete.

- $\wedge$ is the dual of $\vee$.
- $\varphi \rightarrow \psi$ is equivalent to $\neg\varphi \vee \psi$.
- $\varphi \leftrightarrow \psi$ is equivalent to $(\varphi \rightarrow \psi) \wedge (\psi \rightarrow \varphi)$.
- $\top$ is equivalent to $p \vee \neg p$
- $\bot$ is equivalent to $p \wedge \neg p$



Duals in LTL

- What are the duals of $\bigcirc$, $\Box$, $\Diamond$?



Duals in LTL

- What are the duals of $\bigcirc$, $\Box$, $\Diamond$?
- $\bigcirc$ is its own dual:

$$\neg \bigcirc \varphi \sim \bigcirc \neg \varphi.$$

- $\Box$ and $\Diamond$ are duals.

$$\neg \Box \varphi \sim \Diamond \neg \varphi$$
$$\neg \Diamond \varphi \sim \Box \neg \varphi$$

- Any other?



Duals in LTL

- What are the duals of $\bigcirc$, $\Box$, $\Diamond$?
- $\bigcirc$ is its own dual:

$$\neg \bigcirc \varphi \sim \bigcirc \neg \varphi.$$

- $\Box$ and $\Diamond$ are duals.

$$\neg \Box \varphi \sim \Diamond \neg \varphi$$
$$\neg \Diamond \varphi \sim \Box \neg \varphi$$

- Any other?
- U and R are duals.

$$\neg(\varphi \ U \ \psi) \sim (\neg\varphi) \ R \ (\neg\psi)$$
$$\neg(\varphi \ R \ \psi) \sim (\neg\varphi) \ U \ (\neg\psi)$$



Complete set of LTL operators

Proposition

The set of operators $\vee, \neg, U, \bigcirc$ *is complete for LTL.*

Show that this set is complete!



Summary

- LTL is a fragment of CTL*
- LTL is a set of *path formulas*
- There is a set of several temporal operators
- Complete set: $\{\vee, \neg, U, \bigcirc\}$
- Next lecture:
  - Classification of LTL properties
  - Modeling program executions
  - Publication of exercise sheet



References I



Bibliography