Modeling and verifying reactive systems

Temporal logics

Nicolas Markey

Lab. Specification et Verification
ENS Cachan & CNRS, France

Why verification?

- Computers (in a broad sense) are ubiquitous and ever more complex:

Why verification?

- Computers (in a broad sense) are ubiquitous and ever more complex:



- they are (more or less) notoriously buggy:

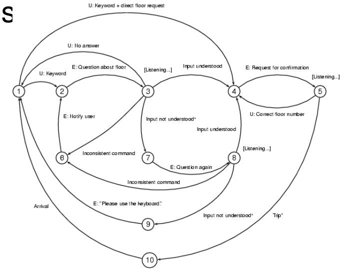

How to verify those systems?

- “naive” approach: build it and try it!

How to verify those systems?

- “naive” approach: build it and try it!

- more “mathematical” approaches
  - (formal) testing;
  - static analysis;
  - model-checking;
  - ...



Principles of model checking

system:

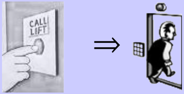
property:

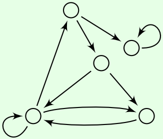
$\Rightarrow$

Principles of model checking

system:

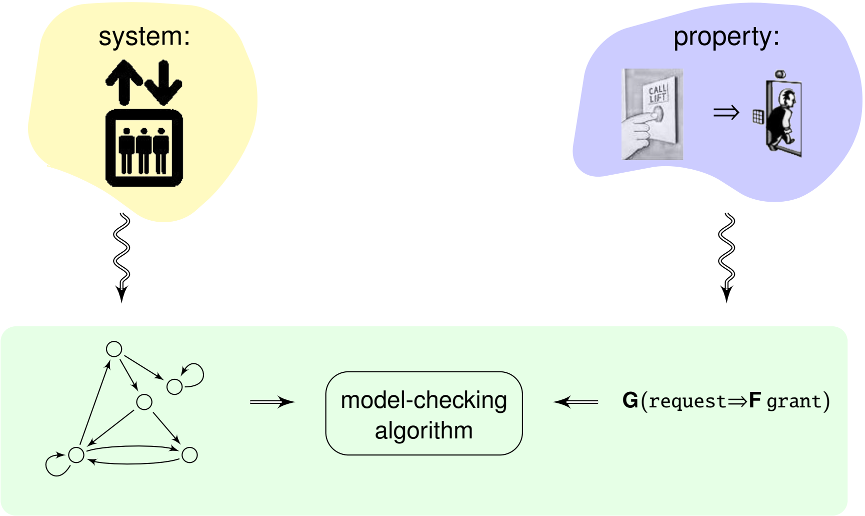
property:



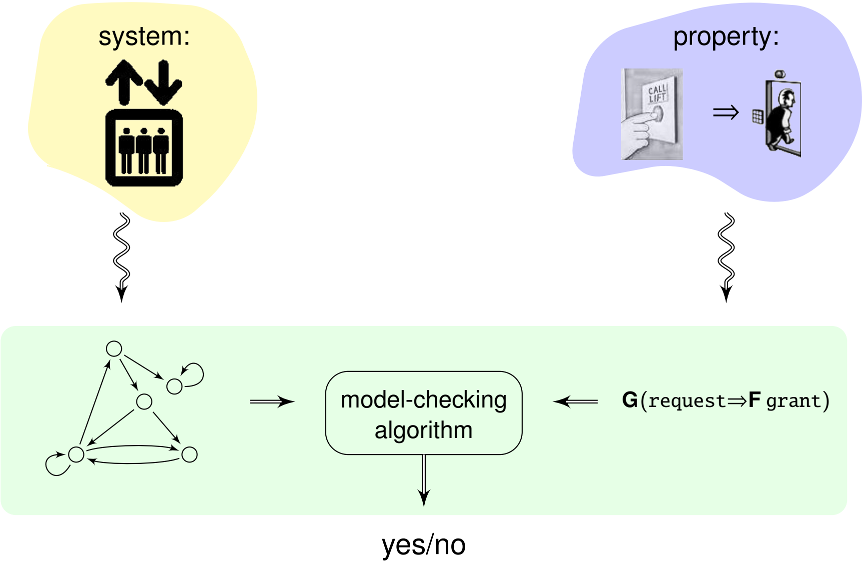


$\mathbf{G}(\mathtt{request} \Rightarrow \mathbf{F}\,\mathtt{grant})$

Principles of model checking



Principles of model checking



Two related problems

Definition

The model-checking problem is defined as follows:

input:	a model and a formula
output:	`true` iff the formula holds in the model.

Two related problems

Definition

The model-checking problem is defined as follows:

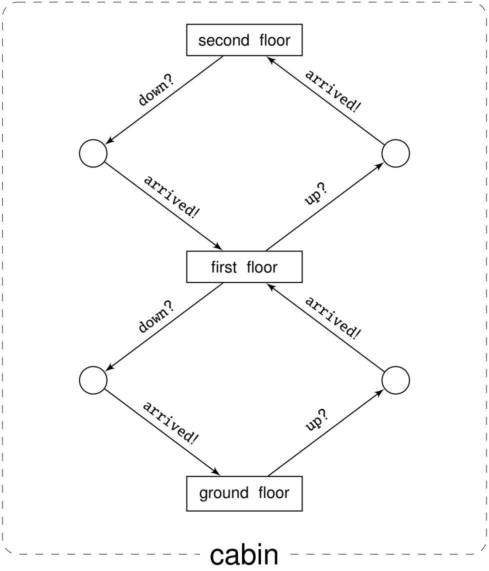
input: a model and a formula
output: `true` iff the formula holds in the model.

Definition

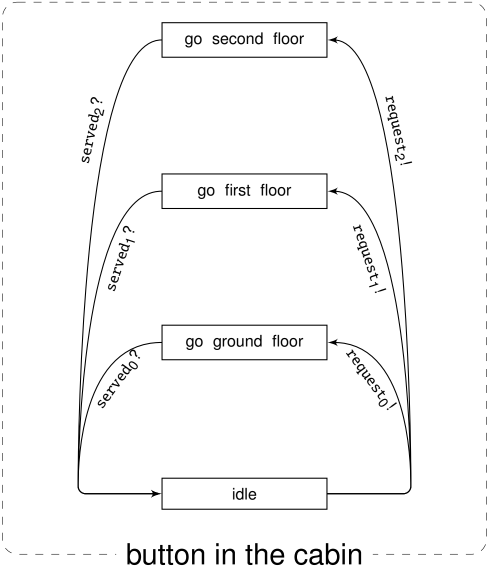
The satisfiability problem is defined as follows:

input: a formula
output: `true` iff there exists a model in which the formula holds.

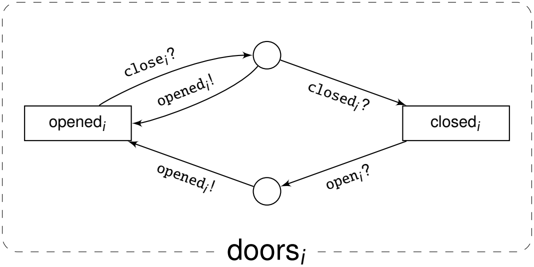
Example: a lift



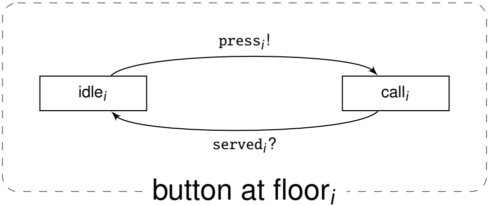
Example: a lift



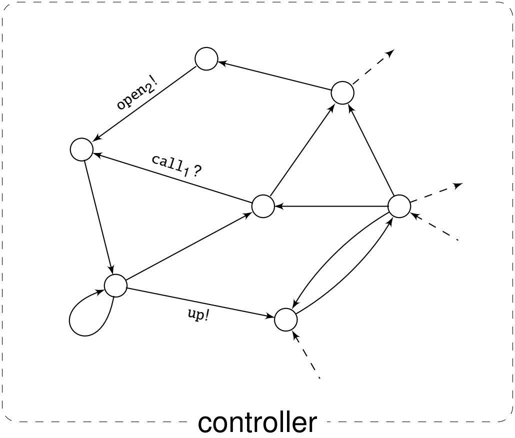
Example: a lift



Example: a lift

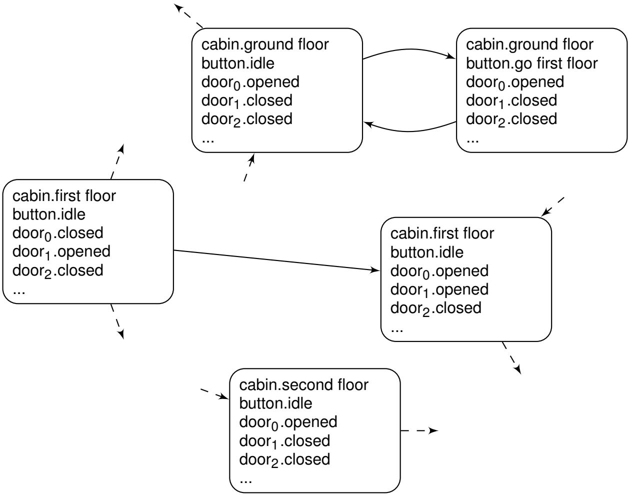


Example: a lift



Example: a lift

Complete model = product of those small modules



Expressing properties: propositional logic

Definition

The syntax of *propositional logics* is defined as

$$\varphi \ ::= \ p \mid \neg\varphi \mid \varphi \vee \varphi \mid \varphi \wedge \varphi$$

where p ranges over a (finite) set of atomic propositions AP.

The semantics is given by truth tables, e.g., for $p \wedge q$:

$\wedge$	$\top$	$\bot$
$\top$	$\top$	$\bot$
$\bot$	$\bot$	$\bot$

Expressing properties: propositional logic

Definition

The syntax of *propositional logics* is defined as

$$\varphi \;::=\; p \mid \neg\varphi \mid \varphi \vee \varphi \mid \varphi \wedge \varphi$$

where p ranges over a (finite) set of atomic propositions AP.

The semantics is given by truth tables, e.g., for $p \wedge q$:

$\wedge$	$\top$	$\bot$
$\top$	$\top$	$\bot$
$\bot$	$\bot$	$\bot$

Examples

$$\text{door}_0.\text{closed} \vee \text{cabin.ground floor}$$

Expressing properties: propositional logic

Definition

The syntax of *propositional logics* is defined as

$$\varphi \ ::= \ p \mid \neg\varphi \mid \varphi \vee \varphi \mid \varphi \wedge \varphi$$

where p ranges over a (finite) set of atomic propositions AP.

The semantics is given by truth tables, e.g., for $p \wedge q$:

$\wedge$	$\top$	$\bot$
$\top$	$\top$	$\bot$
$\bot$	$\bot$	$\bot$

Examples

$\neg(\text{door}_0.\text{open} \wedge \text{door}_1.\text{open})$

Expressing properties: propositional logic

Definition

The syntax of *propositional logics* is defined as

$$\varphi \ ::= \ p \mid \neg\varphi \mid \varphi \vee \varphi \mid \varphi \wedge \varphi$$

where p ranges over a (finite) set of atomic propositions AP.

The semantics is given by truth tables, e.g., for $p \wedge q$:

$\wedge$	$\top$	$\bot$
$\top$	$\top$	$\bot$
$\bot$	$\bot$	$\bot$

Examples

$$\neg(\mathrm{door}_0.\mathrm{open} \wedge \mathrm{door}_1.\mathrm{open}) \equiv \neg\mathrm{door}_0.\mathrm{open} \vee \neg\mathrm{door}_1.\mathrm{open}$$

Verifying properties: propositional logic

Theorem (Jones, 1975)

Checking if a state q' is reachable from a state q in a finite state system S is NLOGSPACE-complete.

Proof.

- algorithm in NLOGSPACE:
  - "guess" the path step by step. We only have to remember the current position (stored as a binary-encoded integer).
- hardness in NLOGSPACE:
  - build the *configuration graph* of a non-deterministic logarithmic-space Turing machine,
  - check whether an accepting state is reachable.

$\square$

Verifying properties: propositional logic

Theorem (Cook, 1973)

Deciding the satisfiability of a propositional logic formula is NP-complete.

Proof.

- algorithm in NP:
  - guess the values of atomic propositions, and check if they make the formula true.
- hardness in NP:
  - we can consider a non-deterministic Turing machine having exactly two choices at each step;
  - encode each cell, at each step, with m boolean variables;
  - build a circuit encoding the executions of the Turing machine. This can be done with only logarithmic space because the transitions only depend on a small amount of "local" information;
  - sat. of a formula is equivalent to sat. of a circuit.

Expressing properties: first-order logic

Definition

First-order logic is an extension of propositional logic with (first-order) quantification:

$$\varphi \ ::= \ p(x) \mid x < y \mid \neg\varphi \mid \varphi \wedge \varphi \mid \exists x \in X.\, \varphi \mid \forall x \in X.\, \varphi$$

where p ranges over a finite set of predicates, X is an ordered set, and x and y range over this set.

Expressing properties: first-order logic

Definition

First-order logic is an extension of propositional logic with (first-order) quantification:

$$\varphi \ ::= \ p(x) \mid x < y \mid \neg\varphi \mid \varphi \wedge \varphi \mid \exists x \in X.\, \varphi \mid \forall x \in X.\, \varphi$$

where p ranges over a finite set of predicates, X is an ordered set, and x and y range over this set.

In our case, the order is given by the transition system:

Examples

$$\neg(\exists x.\ \mathrm{door_1open}(x) \wedge \neg\,\mathrm{cabin.first\ floor}(x))$$

Expressing properties: first-order logic

Definition

First-order logic is an extension of propositional logic with (first-order) quantification:

$$\varphi \ ::= \ p(x) \mid x < y \mid \neg\varphi \mid \varphi \wedge \varphi \mid \exists x \in X.\, \varphi \mid \forall x \in X.\, \varphi$$

where p ranges over a finite set of predicates, X is an ordered set, and x and y range over this set.

In our case, the order is given by the transition system:

Examples

$$\forall x.\, \mathrm{call}_2(x) \Rightarrow (\exists y.\, y > x \wedge \mathrm{door}_2.\mathrm{open}(y))$$

Expressing properties: first-order logic

Definition

First-order logic is an extension of propositional logic with (first-order) quantification:

$$\varphi \ ::= \ p(x) \mid x < y \mid \neg\varphi \mid \varphi \wedge \varphi \mid \exists x \in X.\, \varphi \mid \forall x \in X.\, \varphi$$

where p ranges over a finite set of predicates, X is an ordered set, and x and y range over this set.

In our case, the order is given by the transition system:

Examples

$$\forall x.\, \mathrm{call}_2(x) \Rightarrow (\exists y.\, y > x \wedge \mathrm{door}_2.\mathrm{open}(y))$$

Unfortunately, verifying first-order properties is very hard.

Expressing properties: temporal logics

Definition

Modal logic is an extension of propositional logic with "modalities" for expressing that something is possible or necessary:

$$\varphi \ ::= \ p \mid \neg\varphi \mid \varphi \vee \varphi \mid \varphi \wedge \varphi \mid \Diamond\varphi \mid \Box\varphi$$

where p ranges over AP.

Expressing properties: temporal logics

Definition

Modal logic is an extension of propositional logic with "modalities" for expressing that something is possible or necessary:

$$\varphi \ ::= \ p \mid \neg\varphi \mid \varphi \vee \varphi \mid \varphi \wedge \varphi \mid \Diamond\varphi \mid \Box\varphi$$

where p ranges over AP.

Temporal logics are a special kind of modal logics where

- $\Diamond$ is read "eventually in the future",
- $\Box$ is read "always in the future".

Expressing properties: temporal logics

Definition

Modal logic is an extension of propositional logic with "modalities" for expressing that something is possible or necessary:

$$\varphi \ ::= \ p \mid \neg\varphi \mid \varphi \vee \varphi \mid \varphi \wedge \varphi \mid \Diamond\varphi \mid \Box\varphi$$

where p ranges over AP.

Temporal logics are a special kind of modal logics where

- $\Diamond$ is read "eventually in the future",
- $\Box$ is read "always in the future".

Example

$$\Box(\text{call}_2 \Rightarrow \Diamond\text{door}_2.\text{open})$$

Expressing properties: temporal logics

Definition

Modal logic is an extension of propositional logic with "modalities" for expressing that something is possible or necessary:

$$\varphi \ ::= \ p \mid \neg\varphi \mid \varphi \vee \varphi \mid \varphi \wedge \varphi \mid \Diamond\varphi \mid \Box\varphi$$

where p ranges over AP.

Temporal logics are a special kind of modal logics where

- $\Diamond$ is read "eventually in the future",
- $\Box$ is read "always in the future".

Temporal logics are an acceptable compromise between expressiveness and complexity.

Two notions of time

- linear-time framework: properties deal with one execution at a time:

Example

$$\Box(\mathsf{call}_2 \Rightarrow \Diamond \mathsf{door}_2.\mathsf{open})$$

This formula states that a request (at the second floor) is eventually granted.

Two notions of time

- linear-time framework: properties deal with one execution at a time:

Example

$$\Box(\mathrm{call}_2 \Rightarrow \Diamond \mathrm{door}_2.\mathrm{open})$$

This formula states that a request (at the second floor) is eventually granted.

- branching-time framework: properties deal with the execution tree of the system:

Example

$$\Box(\Diamond \mathrm{door}_0.\mathrm{open})$$

This formula states that it is always possible to reach the ground floor.

Outline of the course

1. Introduction
2. Definitions and examples
   - Linear-time temporal logics
   - Branching-time temporal logics
3. Linear-time temporal logics
   - Expressiveness of LTL and LTL+Past
   - How hard is LTL verification?
   - Algorithms for verifying LTL formulas
   - Back to expressiveness
4. Branching-time temporal logics
   - Expressiveness of branchig-time logics
   - Complexity
   - Alternating-time Temporal Logic

Outline of the course

The linear-time framework

Definition

A *(labelled) linear structure* over a (finite) set AP of atomic propositions is a triple $\mathcal{S} = \langle T, <, \ell \rangle$ where

- T is an infinite set,
- $<$ is a linear order on T s.t. T has a minimal element, and
- $\ell \colon T \to 2^{\mathrm{AP}}$ is a labelling function.

The linear-time framework

Definition

A *(labelled) linear structure* over a (finite) set AP of atomic propositions is a triple $\mathcal{S} = \langle T, <, \ell \rangle$ where

- T is an infinite set,
- $<$ is a linear order on T s.t. T has a minimal element, and
- $\ell \colon T \to 2^{\mathrm{AP}}$ is a labelling function.

Example

An execution of a Kripke structure is a linear structure $\langle \mathbb{Z}^+, <, \ell \rangle$ as follows:

0. cabin.ground floor
button.idle
$door_0$.opened
$door_1$.closed
$door_2$.closed
...

$\rightarrow$

1. cabin.ground floor
button.go first floor
$door_0$.opened
$door_1$.closed
$door_2$.closed
...

$\rightarrow$

2. cabin.ground floor
button.go first floor
$door_0$.closed
$door_1$.closed
$door_2$.closed
...

$\dashrightarrow$

Semantics of LTL modalities

$\widetilde{\mathbf{F}}\,\varphi$ (or $\Diamond\varphi$) : $\langle \mathcal{S}, t\rangle \models \widetilde{\mathbf{F}}\,\varphi \quad \Leftrightarrow \quad \exists u > t.\ \langle \mathcal{S}, u\rangle \models \varphi$
(“eventually” φ)

$\widetilde{\mathbf{G}}\,\varphi$ (or $\Box\varphi$) : $\langle \mathcal{S}, t\rangle \models \widetilde{\mathbf{G}}\,\varphi \quad \Leftrightarrow \quad \forall u > t.\ \langle \mathcal{S}, u\rangle \models \varphi$
(“always” φ)

Semantics of LTL modalities

$\widetilde{\mathbf{F}}\,\varphi$ (or $\Diamond\varphi$) : $\langle \mathcal{S}, t\rangle \models \widetilde{\mathbf{F}}\,\varphi \quad \Leftrightarrow \quad \exists u > t.\ \langle \mathcal{S}, u\rangle \models \varphi$
("eventually" φ)

$\widetilde{\mathbf{G}}\,\varphi$ (or $\Box\varphi$) : $\langle \mathcal{S}, t\rangle \models \widetilde{\mathbf{G}}\,\varphi \quad \Leftrightarrow \quad \forall u > t.\ \langle \mathcal{S}, u\rangle \models \varphi$
("always" φ)

Examples

Liveness properties: $\widetilde{\mathbf{F}}\,\mathrm{open}_i$

Semantics of LTL modalities

$\widetilde{\mathbf{F}}\,\varphi$ (or $\Diamond\varphi$) : $\langle \mathcal{S}, t\rangle \models \widetilde{\mathbf{F}}\,\varphi \quad \Leftrightarrow \quad \exists u > t.\, \langle \mathcal{S}, u\rangle \models \varphi$
("eventually" φ)

$\widetilde{\mathbf{G}}\,\varphi$ (or $\Box\varphi$) : $\langle \mathcal{S}, t\rangle \models \widetilde{\mathbf{G}}\,\varphi \quad \Leftrightarrow \quad \forall u > t.\, \langle \mathcal{S}, u\rangle \models \varphi$
("always" φ)

Examples

Liveness properties: $\widetilde{\mathbf{F}}\,\mathrm{open}_i$

Safety properties: $\widetilde{\mathbf{G}}(\mathrm{open}_i \Rightarrow i\text{-th floor})$

Semantics of LTL modalities

$\widetilde{\mathbf{F}}\,\varphi$ (or $\Diamond\varphi$) : $\langle \mathcal{S}, t\rangle \models \widetilde{\mathbf{F}}\,\varphi \quad \Leftrightarrow \quad \exists u > t.\ \langle \mathcal{S}, u\rangle \models \varphi$
("eventually" φ)

$\widetilde{\mathbf{G}}\,\varphi$ (or $\Box\varphi$) : $\langle \mathcal{S}, t\rangle \models \widetilde{\mathbf{G}}\,\varphi \quad \Leftrightarrow \quad \forall u > t.\ \langle \mathcal{S}, u\rangle \models \varphi$
("always" φ)

Examples

Duality: $\widetilde{\mathbf{F}}\,\varphi \equiv \neg\,\widetilde{\mathbf{G}}\,\neg\varphi$

Semantics of LTL modalities

$\widetilde{\mathbf{F}}\,\varphi$ (or $\Diamond\varphi$) : $\langle \mathcal{S}, t\rangle \models \widetilde{\mathbf{F}}\,\varphi \quad \Leftrightarrow \quad \exists u > t.\ \langle \mathcal{S}, u\rangle \models \varphi$
("eventually" φ)

$\widetilde{\mathbf{G}}\,\varphi$ (or $\Box\varphi$) : $\langle \mathcal{S}, t\rangle \models \widetilde{\mathbf{G}}\,\varphi \quad \Leftrightarrow \quad \forall u > t.\ \langle \mathcal{S}, u\rangle \models \varphi$
("always" φ)

Examples

Distributivity:

$$\widetilde{\mathbf{F}}\,\varphi \lor \widetilde{\mathbf{F}}\,\psi \equiv \widetilde{\mathbf{F}}(\varphi \lor \psi)$$

$$\widetilde{\mathbf{F}}\,\varphi \land \widetilde{\mathbf{F}}\,\psi \not\equiv \widetilde{\mathbf{F}}(\varphi \land \psi)$$

Semantics of LTL modalities

$\widetilde{\mathbf{F}}\,\varphi$ (or $\Diamond\varphi$) : $\langle \mathcal{S}, t\rangle \models \widetilde{\mathbf{F}}\,\varphi \quad \Leftrightarrow \quad \exists u > t.\, \langle \mathcal{S}, u\rangle \models \varphi$
("eventually" φ)

$\widetilde{\mathbf{G}}\,\varphi$ (or $\Box\varphi$) : $\langle \mathcal{S}, t\rangle \models \widetilde{\mathbf{G}}\,\varphi \quad \Leftrightarrow \quad \forall u > t.\, \langle \mathcal{S}, u\rangle \models \varphi$
("always" φ)

Examples

Distributivity:

$$\widetilde{\mathbf{G}}\,\varphi \vee \widetilde{\mathbf{G}}\,\psi \not\equiv \widetilde{\mathbf{G}}(\varphi \vee \psi)$$

$$\widetilde{\mathbf{G}}\,\varphi \wedge \widetilde{\mathbf{G}}\,\psi \equiv \widetilde{\mathbf{G}}(\varphi \wedge \psi)$$

Semantics of LTL modalities

$\widetilde{\mathbf{F}}\,\varphi$ (or $\Diamond\varphi$) : $\langle\mathcal{S},t\rangle \models \widetilde{\mathbf{F}}\,\varphi \quad\Leftrightarrow\quad \exists u > t.\ \langle\mathcal{S},u\rangle \models \varphi$
("eventually" φ)

$\widetilde{\mathbf{G}}\,\varphi$ (or $\Box\varphi$) : $\langle\mathcal{S},t\rangle \models \widetilde{\mathbf{G}}\,\varphi \quad\Leftrightarrow\quad \forall u > t.\ \langle\mathcal{S},u\rangle \models \varphi$
("always" φ)

Examples

Fairness properties: $\widetilde{\mathbf{G}}\,\widetilde{\mathbf{F}}\,\varphi$

("infinitely often" φ)

Semantics of LTL modalities

$\widetilde{\mathbf{F}}\,\varphi$ (or $\Diamond\varphi$) : $\langle \mathcal{S}, t\rangle \models \widetilde{\mathbf{F}}\,\varphi \quad \Leftrightarrow \quad \exists u > t.\, \langle \mathcal{S}, u\rangle \models \varphi$
("eventually" φ)

$\widetilde{\mathbf{G}}\,\varphi$ (or $\Box\varphi$) : $\langle \mathcal{S}, t\rangle \models \widetilde{\mathbf{G}}\,\varphi \quad \Leftrightarrow \quad \forall u > t.\, \langle \mathcal{S}, u\rangle \models \varphi$
("always" φ)

Examples

Fairness properties: $\widetilde{\mathbf{G}}\,\widetilde{\mathbf{F}}\,\varphi \stackrel{\text{def}}{\equiv} \stackrel{\infty}{\mathbf{F}}\,\varphi$

("infinitely often" φ)

Semantics of LTL modalities

$\widetilde{\mathbf{F}}\,\varphi$ (or $\Diamond\varphi$) : $\langle \mathcal{S}, t\rangle \models \widetilde{\mathbf{F}}\,\varphi \quad \Leftrightarrow \quad \exists u > t.\ \langle \mathcal{S}, u\rangle \models \varphi$
("eventually" φ)

$\widetilde{\mathbf{G}}\,\varphi$ (or $\Box\varphi$) : $\langle \mathcal{S}, t\rangle \models \widetilde{\mathbf{G}}\,\varphi \quad \Leftrightarrow \quad \forall u > t.\ \langle \mathcal{S}, u\rangle \models \varphi$
("always" φ)

Examples

Non-strict modalities:

$$\mathbf{F}\,\varphi \overset{\text{def}}{\equiv} \varphi \vee \widetilde{\mathbf{F}}\,\varphi$$

$$\mathbf{G}\,\varphi \overset{\text{def}}{\equiv} \varphi \wedge \widetilde{\mathbf{G}}\,\varphi$$

Semantics of LTL modalities

Past-time counterparts:

$\widetilde{\mathbf{F}}^{-1}\,\varphi$ (or $\blacklozenge\varphi$) : $\langle \mathcal{S}, t\rangle \models \widetilde{\mathbf{F}}^{-1}\,\varphi \quad \Leftrightarrow \quad \exists u < t.\ \langle \mathcal{S}, u\rangle \models \varphi$

("sometimes in the past" φ)

$\widetilde{\mathbf{G}}^{-1}\,\varphi$ (or $\blacksquare\varphi$) : $\langle \mathcal{S}, t\rangle \models \widetilde{\mathbf{G}}^{-1}\,\varphi \quad \Leftrightarrow \quad \forall u < t.\ \langle \mathcal{S}, u\rangle \models \varphi$

("always in the past" φ)

Semantics of LTL modalities

Past-time counterparts:

$\widetilde{\mathbf{F}}^{-1}\,\varphi$ (or $\blacklozenge\varphi$) : $\langle \mathcal{S}, t\rangle \models \widetilde{\mathbf{F}}^{-1}\,\varphi \quad \Leftrightarrow \quad \exists u < t.\, \langle \mathcal{S}, u\rangle \models \varphi$
("sometimes in the past" φ)

$\widetilde{\mathbf{G}}^{-1}\,\varphi$ (or $\blacksquare\varphi$) : $\langle \mathcal{S}, t\rangle \models \widetilde{\mathbf{G}}^{-1}\,\varphi \quad \Leftrightarrow \quad \forall u < t.\, \langle \mathcal{S}, u\rangle \models \varphi$
("always in the past" φ)

Examples

Duality: $\widetilde{\mathbf{F}}^{-1}\,\varphi \equiv \neg\, \widetilde{\mathbf{G}}^{-1}\, \neg\,\varphi$

Semantics of LTL modalities

Past-time counterparts:

$\widetilde{\mathbf{F}}^{-1}\,\varphi$ (or $\blacklozenge\varphi$) : $\langle \mathcal{S}, t\rangle \models \widetilde{\mathbf{F}}^{-1}\,\varphi \quad \Leftrightarrow \quad \exists u < t.\ \langle \mathcal{S}, u\rangle \models \varphi$
("sometimes in the past" φ)

$\widetilde{\mathbf{G}}^{-1}\,\varphi$ (or $\blacksquare\varphi$) : $\langle \mathcal{S}, t\rangle \models \widetilde{\mathbf{G}}^{-1}\,\varphi \quad \Leftrightarrow \quad \forall u < t.\ \langle \mathcal{S}, u\rangle \models \varphi$
("always in the past" φ)

Examples

Duality: $\widetilde{\mathbf{F}}^{-1}\,\varphi \equiv \neg\,\widetilde{\mathbf{G}}^{-1}\,\neg\,\varphi$

Precedence properties: $\widetilde{\mathbf{G}}(\varphi \Rightarrow \widetilde{\mathbf{F}}^{-1}\,\psi)$

Semantics of LTL modalities

Past-time counterparts:

$\widetilde{\mathbf{F}}^{-1}\varphi$ (or $\blacklozenge\varphi$) : $\langle \mathcal{S}, t\rangle \models \widetilde{\mathbf{F}}^{-1}\varphi \quad \Leftrightarrow \quad \exists u < t.\ \langle \mathcal{S}, u\rangle \models \varphi$
("sometimes in the past" φ)

$\widetilde{\mathbf{G}}^{-1}\varphi$ (or $\blacksquare\varphi$) : $\langle \mathcal{S}, t\rangle \models \widetilde{\mathbf{G}}^{-1}\varphi \quad \Leftrightarrow \quad \forall u < t.\ \langle \mathcal{S}, u\rangle \models \varphi$
("always in the past" φ)

Examples

Non-strict versions:

$$\mathbf{F}^{-1}\varphi \stackrel{\text{def}}{\equiv} \varphi \vee \widetilde{\mathbf{F}}^{-1}\varphi$$

$$\mathbf{G}^{-1}\varphi \stackrel{\text{def}}{\equiv} \varphi \wedge \widetilde{\mathbf{G}}^{-1}\varphi$$

Semantics of LTL modalities

Past-time counterparts:

$\widetilde{\mathbf{F}}^{-1}\varphi$ (or $\blacklozenge\varphi$) : $\langle \mathcal{S}, t\rangle \models \widetilde{\mathbf{F}}^{-1}\varphi \quad \Leftrightarrow \quad \exists u < t.\ \langle \mathcal{S}, u\rangle \models \varphi$
("sometimes in the past" φ)

$\widetilde{\mathbf{G}}^{-1}\varphi$ (or $\blacksquare\varphi$) : $\langle \mathcal{S}, t\rangle \models \widetilde{\mathbf{G}}^{-1}\varphi \quad \Leftrightarrow \quad \forall u < t.\ \langle \mathcal{S}, u\rangle \models \varphi$
("always in the past" φ)

Examples

$\widetilde{\mathbf{G}}^{-1}\widetilde{\mathbf{F}}^{-1}\varphi \equiv \bot$ except at origin

$\widetilde{\mathbf{F}}^{-1}\widetilde{\mathbf{G}}^{-1}\varphi \equiv \top$ except at origin

Semantics of LTL modalities

Past-time counterparts:

$\widetilde{\mathbf{F}}^{-1}\,\varphi$ (or $\blacklozenge\varphi$) : $\langle \mathcal{S}, t\rangle \models \widetilde{\mathbf{F}}^{-1}\,\varphi \quad\Leftrightarrow\quad \exists u < t.\ \langle \mathcal{S}, u\rangle \models \varphi$
(“sometimes in the past” φ)

$\widetilde{\mathbf{G}}^{-1}\,\varphi$ (or $\blacksquare\varphi$) : $\langle \mathcal{S}, t\rangle \models \widetilde{\mathbf{G}}^{-1}\,\varphi \quad\Leftrightarrow\quad \forall u < t.\ \langle \mathcal{S}, u\rangle \models \varphi$
(“always in the past” φ)

Examples

“Initially”: $\mathbf{G}^{-1}\,\mathbf{F}^{-1}\,\varphi \equiv \mathbf{F}^{-1}\,\mathbf{G}^{-1}\,\varphi$

Semantics of LTL modalities

Past-time counterparts:

$\widetilde{\mathbf{F}}^{-1}\,\varphi$ (or $\blacklozenge\varphi$) : $\langle \mathcal{S}, t\rangle \models \widetilde{\mathbf{F}}^{-1}\,\varphi \quad \Leftrightarrow \quad \exists u < t.\ \langle \mathcal{S}, u\rangle \models \varphi$
("sometimes in the past" φ)

$\widetilde{\mathbf{G}}^{-1}\,\varphi$ (or $\blacksquare\varphi$) : $\langle \mathcal{S}, t\rangle \models \widetilde{\mathbf{G}}^{-1}\,\varphi \quad \Leftrightarrow \quad \forall u < t.\ \langle \mathcal{S}, u\rangle \models \varphi$
("always in the past" φ)

Examples

"Initially": $\mathbf{G}^{-1}\,\mathbf{F}^{-1}\,\varphi \equiv \mathbf{F}^{-1}\,\mathbf{G}^{-1}\,\varphi \stackrel{\text{def}}{\equiv} \mathbf{I}\,\varphi$

Semantics of LTL modalities

Past-time counterparts:

$\widetilde{\mathbf{F}}^{-1}\,\varphi$ (or $\blacklozenge\varphi$) : $\langle \mathcal{S}, t\rangle \models \widetilde{\mathbf{F}}^{-1}\,\varphi \quad \Leftrightarrow \quad \exists u < t.\ \langle \mathcal{S}, u\rangle \models \varphi$
("sometimes in the past" φ)

$\widetilde{\mathbf{G}}^{-1}\,\varphi$ (or $\blacksquare\varphi$) : $\langle \mathcal{S}, t\rangle \models \widetilde{\mathbf{G}}^{-1}\,\varphi \quad \Leftrightarrow \quad \forall u < t.\ \langle \mathcal{S}, u\rangle \models \varphi$
("always in the past" φ)

Examples

"Initially": $\mathbf{G}^{-1}\,\mathbf{F}^{-1}\,\varphi \equiv \mathbf{F}^{-1}\,\mathbf{G}^{-1}\,\varphi \overset{\text{def}}{\equiv} \mathbf{I}\,\varphi$

"Until": $\widetilde{\mathbf{F}}(\psi \wedge \widetilde{\mathbf{G}}^{-1}\,\varphi)$

"Until"?

Example

$$\texttt{green}\ \text{“until”}\ \texttt{red} \equiv \widetilde{\mathbf{F}}(\texttt{red} \wedge \widetilde{\mathbf{G}}^{-1}\,\texttt{green})$$

“Until”?

Example

$$\widetilde{\mathbf{F}}(\texttt{red} \wedge \texttt{red} \text{ “until” } \texttt{blue}) \not\equiv \widetilde{\mathbf{F}}(\texttt{red} \wedge \widetilde{\mathbf{F}}(\texttt{blue} \wedge \widetilde{\mathbf{G}}^{-1}\, \texttt{red}))$$

“Until”?

Example

$$\widetilde{\mathbf{F}}(\texttt{red} \wedge \texttt{red} \text{ “until” } \texttt{blue}) \not\equiv \widetilde{\mathbf{F}}(\texttt{red} \wedge \widetilde{\mathbf{F}}(\texttt{blue} \wedge \widetilde{\mathbf{G}}^{-1} \texttt{red}))$$

Theorem (Kamp, 1968)

“Until” cannot be expressed using only $\widetilde{\mathbf{F}}$, $\widetilde{\mathbf{G}}$, $\widetilde{\mathbf{F}}^{-1}$, *and* $\widetilde{\mathbf{G}}^{-1}$.

skip proof

“Until”?

Theorem (Kamp, 1968)

“Until” cannot be expressed using only $\widetilde{\mathbf{F}}$, $\widetilde{\mathbf{G}}$, $\widetilde{\mathbf{F}}^{-1}$, *and* $\widetilde{\mathbf{G}}^{-1}$.

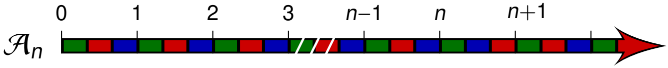
“Until”?

Theorem (Kamp, 1968)

“Until” cannot be expressed using only $\widetilde{\mathbf{F}}$, $\widetilde{\mathbf{G}}$, $\widetilde{\mathbf{F}}^{-1}$, and $\widetilde{\mathbf{G}}^{-1}$.

Proof (sketch).

Consider the following linear structure:



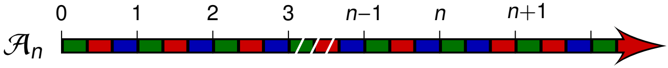
“Until”?

Theorem (Kamp, 1968)

“Until” cannot be expressed using only $\widetilde{\mathbf{F}}$, $\widetilde{\mathbf{G}}$, $\widetilde{\mathbf{F}}^{-1}$, *and* $\widetilde{\mathbf{G}}^{-1}$.

Proof (sketch).

Consider the following linear structure:



Lemma

For any $n \in \mathbb{Z}^+$, *formula*

$$\widetilde{\mathbf{F}}(\mathtt{blue} \wedge \mathtt{blue} \text{ “until” } \mathtt{red})$$

holds along $\mathcal{A}_n$ *on a bounded subset of* $\mathbb{R}^+$ *containing* n.

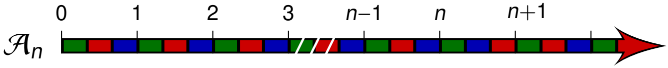
“Until”?

Theorem (Kamp, 1968)

“Until” cannot be expressed using only $\widetilde{\mathbf{F}}$, $\widetilde{\mathbf{G}}$, $\widetilde{\mathbf{F}}^{-1}$, *and* $\widetilde{\mathbf{G}}^{-1}$.

Proof (sketch).

Consider the following linear structure:

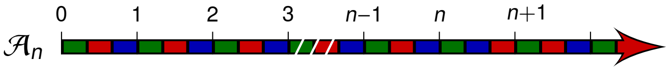


Lemma

Let $n \in \mathbb{Z}^+$, *and* φ *be a formula built on* $\widetilde{\mathbf{F}}$, $\widetilde{\mathbf{G}}$, $\widetilde{\mathbf{F}}^{-1}$, *and* $\widetilde{\mathbf{G}}^{-1}$. *Let* $t \geq |\varphi|$ *and* $u \geq |\varphi|$ *labelled with the same atomic propositions. Then*

$$\langle \mathcal{A}_n, t\rangle \models \varphi \quad\Longleftrightarrow\quad \langle \mathcal{A}_n, u\rangle \models \varphi$$

"Until"?



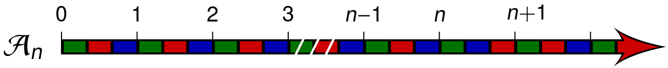
Lemma

Let $n \in \mathbb{Z}^+$, and φ be a formula built on $\widetilde{\mathbf{F}}$, $\widetilde{\mathbf{G}}$, $\widetilde{\mathbf{F}}^{-1}$, and $\widetilde{\mathbf{G}}^{-1}$. Let $t \geq |\varphi|$ and $u \geq |\varphi|$ labelled with the same atomic propositions. Then

$$\langle \mathcal{A}_n, t \rangle \models \varphi \qquad \iff \qquad \langle \mathcal{A}_n, u \rangle \models \varphi$$

Proof. By induction on the structure of the formula:

“Until”?



Lemma

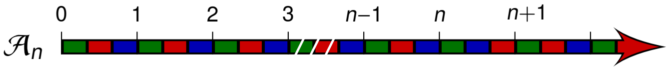
Let $n \in \mathbb{Z}^+$, and φ be a formula built on $\widetilde{\mathbf{F}}$, $\widetilde{\mathbf{G}}$, $\widetilde{\mathbf{F}}^{-1}$, and $\widetilde{\mathbf{G}}^{-1}$. Let $t \geq |\varphi|$ and $u \geq |\varphi|$ labelled with the same atomic propositions. Then

$$\langle \mathcal{A}_n, t \rangle \models \varphi \quad \iff \quad \langle \mathcal{A}_n, u \rangle \models \varphi$$

Proof. By induction on the structure of the formula:

- obvious for atomic propositions,
- straightforward for boolean combinators,

“Until”?



Lemma

Let $n \in \mathbb{Z}^+$, and φ be a formula built on $\widetilde{\mathbf{F}}$, $\widetilde{\mathbf{G}}$, $\widetilde{\mathbf{F}}^{-1}$, and $\widetilde{\mathbf{G}}^{-1}$. Let $t \geq |\varphi|$ and $u \geq |\varphi|$ labelled with the same atomic propositions. Then

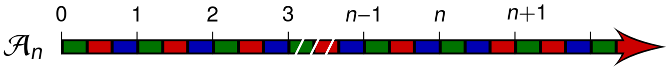
$$\langle \mathcal{A}_n, t\rangle \models \varphi \quad \iff \quad \langle \mathcal{A}_n, u\rangle \models \varphi$$

Proof. By induction on the structure of the formula:

- if $\varphi = \widetilde{\mathbf{F}}\,\psi$, then

$$\begin{aligned} \langle \mathcal{A}_n, t\rangle \models \varphi &\Rightarrow \langle \mathcal{A}_n, t'\rangle \models \psi \quad \text{for some } t' \geq t \geq |\psi| \\ &\Rightarrow \langle \mathcal{A}_n, u'\rangle \models \psi \quad \text{for any } u' \geq |\psi| \text{ labeled as } t' \\ &\Rightarrow \langle \mathcal{A}_n, u\rangle \models \varphi. \end{aligned}$$

“Until”?



Now, if $\widetilde{\mathbf{F}}(\texttt{blue} \wedge \texttt{blue}$“until”$\texttt{red})$ can be expressed as a formula φ built on $\widetilde{\mathbf{F}}$, $\widetilde{\mathbf{G}}$, $\widetilde{\mathbf{F}}^{-1}$, and $\widetilde{\mathbf{G}}^{-1}$, let $n = |\varphi|$. Then

- the set of positions along $\mathcal{A}_n$ where φ holds is bounded and contains n;
- since φ holds at position n along $\mathcal{A}_n$, it also holds at any future position that is labeled by the same atomic propositions.

This is a contradiction.

Semantics of LTL modalities

$$\varphi \; \widetilde{\mathbf{U}} \; \psi : \;\; \langle \mathcal{S}, t \rangle \models \varphi \; \widetilde{\mathbf{U}} \; \psi \;\; \Leftrightarrow \;\; \exists u > t. \, (\langle \mathcal{S}, u \rangle \models \psi \; \text{ and } \; \forall v > t. \, (v < u \; \Rightarrow \; \langle \mathcal{S}, v \rangle \models \varphi))$$

(φ “until” ψ)

$$\varphi \; \widetilde{\mathbf{S}} \; \psi : \;\; \langle \mathcal{S}, t \rangle \models \varphi \; \widetilde{\mathbf{S}} \; \psi \;\; \Leftrightarrow \;\; \exists u < t. \, (\langle \mathcal{S}, u \rangle \models \psi \; \text{ and } \; \forall v < t. \, (v > u \; \Rightarrow \; \langle \mathcal{S}, v \rangle \models \varphi))$$

(φ “since” ψ)

Semantics of LTL modalities

$\varphi \, \widetilde{\mathbf{U}} \, \psi$: $\langle \mathcal{S}, t \rangle \models \varphi \, \widetilde{\mathbf{U}} \, \psi \quad \Leftrightarrow \quad \exists u > t. \, (\langle \mathcal{S}, u \rangle \models \psi$ and
(φ "until" ψ) $\qquad \forall v > t. \, (v < u \Rightarrow \langle \mathcal{S}, v \rangle \models \varphi))$

$\varphi \, \widetilde{\mathbf{S}} \, \psi$: $\langle \mathcal{S}, t \rangle \models \varphi \, \widetilde{\mathbf{S}} \, \psi \quad \Leftrightarrow \quad \exists u < t. \, (\langle \mathcal{S}, u \rangle \models \psi$ and
(φ "since" ψ) $\qquad \forall v < t. \, (v > u \Rightarrow \langle \mathcal{S}, v \rangle \models \varphi))$

Examples

Equivalences:

$$\widetilde{\mathbf{F}} \, \varphi \equiv \top \, \widetilde{\mathbf{U}} \, \varphi$$

$$\widetilde{\mathbf{F}}^{-1} \, \varphi \equiv \top \, \widetilde{\mathbf{S}} \, \varphi$$

Semantics of LTL modalities

$\varphi\ \widetilde{\mathbf{U}}\ \psi$: $\langle \mathcal{S}, t\rangle \models \varphi\ \widetilde{\mathbf{U}}\ \psi \;\Leftrightarrow\; \exists u > t.\ (\langle \mathcal{S}, u\rangle \models \psi$ and
(φ "until" ψ) $\forall v > t.\ (v < u \Rightarrow \langle \mathcal{S}, v\rangle \models \varphi))$

$\varphi\ \widetilde{\mathbf{S}}\ \psi$: $\langle \mathcal{S}, t\rangle \models \varphi\ \widetilde{\mathbf{S}}\ \psi \;\Leftrightarrow\; \exists u < t.\ (\langle \mathcal{S}, u\rangle \models \psi$ and
(φ "since" ψ) $\forall v < t.\ (v > u \Rightarrow \langle \mathcal{S}, v\rangle \models \varphi))$

Examples

Non-strict modalities:

$$\varphi\ \mathbf{U}\ \psi \stackrel{\text{def}}{\equiv} \psi \lor (\varphi \land \varphi\ \widetilde{\mathbf{U}}\ \psi)$$

$$\varphi\ \mathbf{S}\ \psi \stackrel{\text{def}}{\equiv} \psi \lor (\varphi \land \varphi\ \widetilde{\mathbf{S}}\ \psi)$$

Semantics of LTL modalities

$\varphi \ \widetilde{\mathbf{U}} \ \psi$: $\langle \mathcal{S}, t \rangle \models \varphi \ \widetilde{\mathbf{U}} \ \psi \quad \Leftrightarrow \quad \exists u > t. \, (\langle \mathcal{S}, u \rangle \models \psi$ and
(φ "until" ψ) $\qquad \forall v > t. \, (v < u \Rightarrow \langle \mathcal{S}, v \rangle \models \varphi))$

$\varphi \ \widetilde{\mathbf{S}} \ \psi$: $\langle \mathcal{S}, t \rangle \models \varphi \ \widetilde{\mathbf{S}} \ \psi \quad \Leftrightarrow \quad \exists u < t. \, (\langle \mathcal{S}, u \rangle \models \psi$ and
(φ "since" ψ) $\qquad \forall v < t. \, (v > u \Rightarrow \langle \mathcal{S}, v \rangle \models \varphi))$

Examples

"Next" modality: $\quad \bot \ \widetilde{\mathbf{U}} \ \varphi \stackrel{\text{def}}{\equiv} \mathbf{X} \, \varphi \quad$ in discrete time

Semantics of LTL modalities

$$\varphi \; \widetilde{\mathbf{U}} \; \psi : \quad \langle \mathcal{S}, t \rangle \models \varphi \; \widetilde{\mathbf{U}} \; \psi \quad \Leftrightarrow \quad \exists u > t.\, (\langle \mathcal{S}, u \rangle \models \psi \text{ and } \forall v > t.\, (v < u \Rightarrow \langle \mathcal{S}, v \rangle \models \varphi))$$

(φ "until" ψ)

$$\varphi \; \widetilde{\mathbf{S}} \; \psi : \quad \langle \mathcal{S}, t \rangle \models \varphi \; \widetilde{\mathbf{S}} \; \psi \quad \Leftrightarrow \quad \exists u < t.\, (\langle \mathcal{S}, u \rangle \models \psi \text{ and } \forall v < t.\, (v > u \Rightarrow \langle \mathcal{S}, v \rangle \models \varphi))$$

(φ "since" ψ)

Examples

"Next" modality: $\bot \; \widetilde{\mathbf{U}} \; \varphi \stackrel{\text{def}}{\equiv} \mathbf{X}\, \varphi$ in discrete time

$\bot \; \widetilde{\mathbf{U}} \; \varphi \equiv \bot$ in dense time

Semantics of LTL modalities

$$\varphi\ \widetilde{\mathbf{U}}\ \psi : \quad \langle \mathcal{S}, t\rangle \models \varphi\ \widetilde{\mathbf{U}}\ \psi \quad \Leftrightarrow \quad \exists u > t.\ (\langle \mathcal{S}, u\rangle \models \psi \ \text{ and}$$

$(\varphi$ "until" $\psi)$

$$\forall v > t.\ (v < u \ \Rightarrow\ \langle \mathcal{S}, v\rangle \models \varphi))$$

$$\varphi\ \widetilde{\mathbf{S}}\ \psi : \quad \langle \mathcal{S}, t\rangle \models \varphi\ \widetilde{\mathbf{S}}\ \psi \quad \Leftrightarrow \quad \exists u < t.\ (\langle \mathcal{S}, u\rangle \models \psi \ \text{ and}$$

$(\varphi$ "since" $\psi)$

$$\forall v < t.\ (v > u \ \Rightarrow\ \langle \mathcal{S}, v\rangle \models \varphi))$$

Examples

"Next" modality: $\bot\ \widetilde{\mathbf{U}}\ \varphi \stackrel{\text{def}}{\equiv} \mathbf{X}\,\varphi$ in discrete time

"Previous" modality: $\bot\ \widetilde{\mathbf{S}}\ \varphi \stackrel{\text{def}}{\equiv} \mathbf{X}^{-1}\,\varphi$ in discrete time

Duality

Examples

Duality is an important notion in logic:

$$\neg(\neg p \wedge \neg q) \equiv p \vee q$$
$$\neg(\neg p \vee \neg q) \equiv p \wedge q$$

$$\neg\,\mathbf{F}\,\neg p \equiv \mathbf{G}\,p$$
$$\neg\,\mathbf{G}\,\neg p \equiv \mathbf{F}\,p$$

$$\neg\,\mathbf{X}\,\neg p \equiv \mathbf{X}\,p$$

What is the dual of $\widetilde{\mathbf{U}}$?

Duality

Examples

Duality is an important notion in logic:

$$\neg(\neg p \wedge \neg q) \equiv p \vee q$$
$$\neg(\neg p \vee \neg q) \equiv p \wedge q$$

$$\neg\, \mathbf{F} \neg p \equiv \mathbf{G}\, p$$
$$\neg\, \mathbf{G} \neg p \equiv \mathbf{F}\, p$$

$$\neg\, \mathbf{X} \neg p \equiv \mathbf{X}\, p$$

What is the dual of $\widetilde{\mathbf{U}}$?

$$\varphi \;\widetilde{\mathbf{R}}\; \psi : \;\langle \mathcal{S}, t\rangle \models \varphi \;\widetilde{\mathbf{R}}\; \psi \;\Leftrightarrow\; \forall u > t.\, (\langle \mathcal{S}, u\rangle \not\models \psi \Rightarrow \exists v > t.\, (v < u \wedge \langle \mathcal{S}, v\rangle \models \varphi))$$

(φ “releases” ψ)

Duality

What is the dual of $\widetilde{\mathbf{U}}$?

$$\varphi \; \widetilde{\mathbf{R}} \; \psi : \; \langle \mathcal{S}, t \rangle \models \varphi \; \widetilde{\mathbf{R}} \; \psi \quad \Leftrightarrow \quad \forall u > t. \, (\langle \mathcal{S}, u \rangle \not\models \psi \; \Rightarrow \; \exists v > t. \, (v < u \; \wedge \; \langle \mathcal{S}, v \rangle \models \varphi))$$

(φ "releases" ψ)

Proposition

On $\langle \mathbb{Z}^+, <, \ell \rangle$,

$$\varphi \; \widetilde{\mathbf{R}} \; \psi \equiv \widetilde{\mathbf{G}} \, \psi \; \vee \; \psi \; \widetilde{\mathbf{U}} \, (\varphi \; \wedge \; \psi).$$

This equivalence fails to hold on $\langle \mathbb{R}^+, <, \ell \rangle$.

LTL and LTL+Past

Definition

Given modalities M_1 to M_n and a set AP of atomic propositions, the logic $\mathcal{L}_{\mathrm{AP}}(M_1, ..., M_n)$ is defined by the following grammar:

$$\mathcal{L}_{\mathrm{AP}}(M_1, ..., M_n) \ni \varphi, \psi, ... ::= \top \mid p \mid \neg \varphi \mid \varphi \vee \psi \mid M_i(\varphi, \psi, ...)$$

where p ranges over AP, and i over $\{1, ..., n\}$.

LTL and LTL+Past

Definition

Given modalities M_1 to M_n and a set AP of atomic propositions, the logic $\mathcal{L}_{\mathrm{AP}}(M_1, \ldots, M_n)$ is defined by the following grammar:

$$\mathcal{L}_{\mathrm{AP}}(M_1, \ldots, M_n) \ni \varphi, \psi, \ldots ::= \top \mid p \mid \neg\varphi \mid \varphi \vee \psi \mid M_i(\varphi, \psi, \ldots)$$

where p ranges over AP, and i over $\{1, \ldots, n\}$.

Definition

- LTL+Past = $\mathcal{L}(\widetilde{\mathbf{U}}, \widetilde{\mathbf{S}})$
- LTL = $\mathcal{L}(\widetilde{\mathbf{U}})$

LTL and LTL+Past

Definition

Given modalities M_1 to M_n and a set AP of atomic propositions, the logic $\mathcal{L}_{\mathrm{AP}}(M_1, \ldots, M_n)$ is defined by the following grammar:

$$\mathcal{L}_{\mathrm{AP}}(M_1, \ldots, M_n) \ni \varphi, \psi, \ldots ::= \top \mid p \mid \neg\varphi \mid \varphi \vee \psi \mid M_i(\varphi, \psi, \ldots)$$

where p ranges over AP, and i over $\{1, \ldots, n\}$.

Definition

- LTL+Past = $\mathcal{L}(\widetilde{\mathbf{U}}, \widetilde{\mathbf{S}})$
- LTL = $\mathcal{L}(\widetilde{\mathbf{U}})$
- LTL = $\mathcal{L}(\mathbf{U}, \mathbf{X})$ often prefered in discrete-time.

⚠ Both definitions of LTL are not exactly equivalent.

Examples of properties

Examples

- any request is eventually granted:

$$\mathbf{G}(\text{button}_2.\text{call} \Rightarrow \mathbf{F}(\text{door}_2.\text{open}))$$

Examples of properties

Examples

- any request is eventually granted:

$$\mathbf{G}(\text{button}_2.\text{call} \Rightarrow \mathbf{F}(\text{door}_2.\text{open}))$$

- the doors open only on request:

$$\mathbf{G}\,[\text{door}_2.\text{closed} \Rightarrow (\text{button}_2.\text{call} \vee \text{button.go second floor})\ \mathbf{R}\ \text{door}_2.\text{closed}]$$

Examples of properties

Examples

- any request is eventually granted:

$$\mathbf{G}(\text{button}_2.\text{call} \Rightarrow \mathbf{F}(\text{door}_2.\text{open}))$$

- the doors open only on request:

$$\mathbf{G}\,[\text{door}_2.\text{closed} \Rightarrow (\text{button}_2.\text{call} \vee \text{button.go second floor})\ \mathbf{R}\ \text{door}_2.\text{closed}]$$

- the cabin will serve a request as early as possible:

$$\mathbf{G}\,[(\text{cabin.first floor} \wedge \text{button}_1.\text{call}) \Rightarrow (\text{cabin.first floor}\ \mathbf{U}\ \text{door}_1.\text{open})]$$

Outline of the course

The branching-time framework

Definition

A *(labelled) branching structure* over a (finite) set AP of atomic propositions is a triple $\mathcal{S} = \langle T, <, \ell \rangle$ where

- T is an infinite set,
- $<$ is a tree order on T s.t. T has a minimal element, and
- $\ell \colon T \to 2^{\mathrm{AP}}$ is a labelling function.

Definition

An order $<$ on a set T is a tree order if for any $t \in T$, the set $\{u \in T \mid u < t\}$ is totally ordered and has a minimal element.

The branching-time framework

Definition

A *(labelled) branching structure* over a (finite) set AP of atomic propositions is a triple $\mathcal{S} = \langle T, <, \ell \rangle$ where

- T is an infinite set,
- $<$ is a tree order on T s.t. T has a minimal element, and
- $\ell \colon T \to 2^{\mathsf{AP}}$ is a labelling function.

Definition

A branch of a tree $\mathcal{S} = \langle T, <, \ell \rangle$ is a maximal totally ordered subset of T. We write $\mathrm{Br}_{\mathcal{S}}(t)$ for the set of branches of $\mathcal{S}$ containing t.

The branching-time framework

Definition

A *(labelled) branching structure* over a (finite) set AP of atomic propositions is a triple $\mathcal{S} = \langle T, <, \ell \rangle$ where

- T is an infinite set,
- $<$ is a tree order on T s.t. T has a minimal element, and
- $\ell \colon T \to 2^{\mathsf{AP}}$ is a labelling function.

Definition

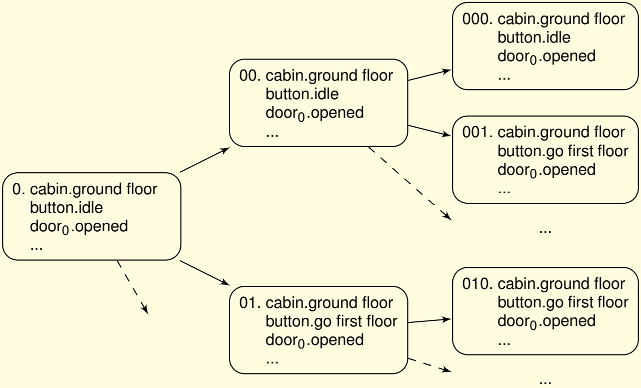
A branch of a tree $\mathcal{S} = \langle T, <, \ell \rangle$ is a maximal totally ordered subset of T. We write $\mathrm{Br}_{\mathcal{S}}(t)$ for the set of branches of $\mathcal{S}$ containing t.

In the sequel, we require that all branches be infinite, and we only deal with discrete-time (where all the branches are isomorphic to $\mathbb{Z}^+$).

The branching-time framework

Example

The execution tree of a Kripke structure is a tree structure $\langle T, \prec, \ell \rangle$, where $T \subseteq (\mathbb{Z}^+)^*$:



Path quantifiers

$$\mathbf{E}\varphi: \quad \langle \mathcal{S}, t\rangle \models \mathbf{E}\varphi \quad \Leftrightarrow \quad \exists b \in \mathrm{Br}_{\mathcal{S}}(t).\ \langle \mathcal{S}, b, t\rangle \models \varphi$$

("there exists a path satisfying" φ)

$$\mathbf{A}\varphi: \quad \langle \mathcal{S}, t\rangle \models \mathbf{A}\varphi \quad \Leftrightarrow \quad \forall b \in \mathrm{Br}_{\mathcal{S}}(t).\ \langle \mathcal{S}, b, t\rangle \models \varphi$$

("for all paths," φ)

Path quantifiers

$$\mathbf{E}\varphi: \quad \langle \mathcal{S}, t\rangle \models \mathbf{E}\varphi \quad \Leftrightarrow \quad \exists b \in \mathrm{Br}_{\mathcal{S}}(t).\, \langle \mathcal{S}, b, t\rangle \models \varphi$$

(“there exists a path satisfying” φ)

$$\mathbf{A}\varphi: \quad \langle \mathcal{S}, t\rangle \models \mathbf{A}\varphi \quad \Leftrightarrow \quad \forall b \in \mathrm{Br}_{\mathcal{S}}(t).\, \langle \mathcal{S}, b, t\rangle \models \varphi$$

(“for all paths,” φ)

Examples

- A request is always served:

$$\mathbf{A}\,\mathbf{G}(\mathsf{button_2.call} \Rightarrow \mathbf{A}\,\mathbf{F}\,\mathsf{door_2.open})$$

Path quantifiers

$$\mathbf{E}\varphi : \quad \langle \mathcal{S}, t \rangle \models \mathbf{E}\varphi \qquad \Leftrightarrow \qquad \exists b \in \mathrm{Br}_{\mathcal{S}}(t).\ \langle \mathcal{S}, b, t \rangle \models \varphi$$

("there exists a path satisfying" φ)

$$\mathbf{A}\varphi : \quad \langle \mathcal{S}, t \rangle \models \mathbf{A}\varphi \qquad \Leftrightarrow \qquad \forall b \in \mathrm{Br}_{\mathcal{S}}(t).\ \langle \mathcal{S}, b, t \rangle \models \varphi$$

("for all paths," φ)

Examples

- The ground floor is always reachable:

$$\mathbf{A}\,\mathbf{G}(\mathbf{E}\,\mathbf{F}(\mathrm{door}_0.\mathrm{open}))$$

Several branching-time logics

Definition

Given a set $\{M_1, ..., M_n\}$ of n modalities, we define the three logics:

$$\mathcal{B}(M_1, ..., M_n) \ni \varphi_b ::= p \mid \neg \varphi_b \mid \varphi_b \vee \varphi_b \mid \mathbf{E}\varphi_l \mid \mathbf{A}\varphi_l$$
$$\varphi_l ::= M_1(\varphi_b, ..., \varphi_b) \mid \cdots \mid M_n(\varphi_b, ..., \varphi_b)$$

Several branching-time logics

Definition

Given a set $\{M_1, ..., M_n\}$ of n modalities, we define the three logics:

$$\mathcal{B}(M_1, ..., M_n) \ni \varphi_b ::= p \mid \neg \varphi_b \mid \varphi_b \vee \varphi_b \mid \mathbf{E}\varphi_l \mid \mathbf{A}\varphi_l$$
$$\varphi_l ::= M_1(\varphi_b, ..., \varphi_b) \mid \cdots \mid M_n(\varphi_b, ..., \varphi_b)$$

Examples

$$\mathbf{A}\,\mathbf{G}(\text{door}_0.\text{open} \Rightarrow \text{cabin.ground floor})$$

Several branching-time logics

Definition

Given a set $\{M_1, ..., M_n\}$ of n modalities, we define the three logics:

$$\mathcal{B}(M_1, ..., M_n) \ni \varphi_b ::= p \mid \neg \varphi_b \mid \varphi_b \vee \varphi_b \mid \mathbf{E}\varphi_l \mid \mathbf{A}\varphi_l$$
$$\varphi_l ::= M_1(\varphi_b, ..., \varphi_b) \mid \cdots \mid M_n(\varphi_b, ..., \varphi_b)$$

Examples

$$\mathbf{A}\,\mathbf{G}(\mathbf{E}\,\mathbf{F}\,\mathrm{door}_0.\mathrm{open})$$

Several branching-time logics

Definition

Given a set $\{M_1, ..., M_n\}$ of n modalities, we define the three logics:

$$\begin{aligned} \mathcal{B}(M_1, ..., M_n) \ni \varphi_b &::= p \mid \neg \varphi_b \mid \varphi_b \vee \varphi_b \mid \mathbf{E}\varphi_l \mid \mathbf{A}\varphi_l \\ \varphi_l &::= M_1(\varphi_b, ..., \varphi_b) \mid \cdots \mid M_n(\varphi_b, ..., \varphi_b) \end{aligned}$$

Examples

$$\mathbf{A}\,\mathbf{G}(\mathbf{E}\,\mathbf{F}\,\mathrm{door}_0.\mathrm{open})$$

Definition

$$\mathrm{CTL} = \mathcal{B}(\mathbf{X}, \mathbf{U})$$

Several branching-time logics

Definition

Given a set $\{M_1, ..., M_n\}$ of n modalities, we define the three logics:

$$\begin{aligned}\mathcal{B}^+(M_1, ..., M_n) \ni \varphi_b &::= p \mid \neg\varphi_b \mid \varphi_b \vee \varphi_b \mid \mathbf{E}\varphi_l \mid \mathbf{A}\varphi_l \\ \varphi_l &::= \neg\varphi_l \mid \varphi_l \vee \varphi_l \mid \\ &\qquad M_1(\varphi_b, ..., \varphi_b) \mid \cdots \mid M_n(\varphi_b, ..., \varphi_b)\end{aligned}$$

Several branching-time logics

Definition

Given a set $\{M_1, ..., M_n\}$ of n modalities, we define the three logics:

$$\begin{aligned}\mathcal{B}^+(M_1, ..., M_n) \ni \varphi_b &::= p \mid \neg \varphi_b \mid \varphi_b \vee \varphi_b \mid \mathbf{E}\varphi_l \mid \mathbf{A}\varphi_l \\ \varphi_l &::= \neg \varphi_l \mid \varphi_l \vee \varphi_l \mid \\ &\qquad M_1(\varphi_b, ..., \varphi_b) \mid \cdots \mid M_n(\varphi_b, ..., \varphi_b)\end{aligned}$$

Examples

$$\mathbf{E}(\mathbf{F}\,\mathrm{door}_1.\mathrm{open} \wedge \neg\, \mathbf{F}\,\mathrm{button}_1.\mathrm{call})$$

Several branching-time logics

Definition

Given a set $\{M_1, ..., M_n\}$ of n modalities, we define the three logics:

$$\mathcal{B}^+(M_1, ..., M_n) \ni \varphi_b ::= p \mid \neg \varphi_b \mid \varphi_b \vee \varphi_b \mid \mathbf{E}\varphi_l \mid \mathbf{A}\varphi_l$$
$$\varphi_l ::= \neg \varphi_l \mid \varphi_l \vee \varphi_l \mid M_1(\varphi_b, ..., \varphi_b) \mid \cdots \mid M_n(\varphi_b, ..., \varphi_b)$$

Examples

$$\mathbf{E}(\mathbf{F}\,\text{door}_1\text{.open} \wedge \neg\,\mathbf{F}\,\text{button}_1\text{.call})$$

Definition

$$\text{CTL}^+ = \mathcal{B}^+(\mathbf{X}, \mathbf{U})$$

Several branching-time logics

Definition

Given a set $\{M_1, ..., M_n\}$ of n modalities, we define the three logics:

$$\begin{aligned}\mathcal{B}^*(M_1, ..., M_n) \ni \varphi_b &::= p \mid \neg\varphi_b \mid \varphi_b \vee \varphi_b \mid \mathbf{E}\varphi_l \mid \mathbf{A}\varphi_l \\ \varphi_l &::= \varphi_b \mid \neg\varphi_l \mid \varphi_l \vee \varphi_l \mid \\ &\qquad M_1(\varphi_l, ..., \varphi_l) \mid \cdots \mid M_n(\varphi_l, ..., \varphi_l)\end{aligned}$$

Several branching-time logics

Definition

Given a set $\{M_1, ..., M_n\}$ of n modalities, we define the three logics:

$$\begin{aligned}\mathcal{B}^*(M_1, ..., M_n) \ni \varphi_b &::= p \mid \neg \varphi_b \mid \varphi_b \vee \varphi_b \mid \mathbf{E}\varphi_l \mid \mathbf{A}\varphi_l \\ \varphi_l &::= \varphi_b \mid \neg \varphi_l \mid \varphi_l \vee \varphi_l \mid \\ &\qquad M_1(\varphi_l, ..., \varphi_l) \mid \cdots \mid M_n(\varphi_l, ..., \varphi_l)\end{aligned}$$

Examples

$$\mathbf{E}\,\mathbf{F}\,\mathbf{G}\ \mathrm{door}_0.\mathrm{closed}$$

Several branching-time logics

Definition

Given a set $\{M_1, ..., M_n\}$ of n modalities, we define the three logics:

$$\begin{aligned}\mathcal{B}^*(M_1, ..., M_n) \ni \varphi_b &::= p \mid \neg \varphi_b \mid \varphi_b \vee \varphi_b \mid \mathbf{E}\varphi_l \mid \mathbf{A}\varphi_l \\ \varphi_l &::= \varphi_b \mid \neg \varphi_l \mid \varphi_l \vee \varphi_l \mid \\ &\qquad M_1(\varphi_l, ..., \varphi_l) \mid \cdots \mid M_n(\varphi_l, ..., \varphi_l)\end{aligned}$$

Examples

$$\mathbf{E}\,\mathbf{F}\,\mathbf{G}\ \mathrm{door}_0.\mathrm{closed}$$

Definition

$$\mathrm{CTL}^* = \mathcal{B}^*(\mathbf{X}, \mathbf{U})$$