FORMAL METHODS

LECTURE III: LINEAR TEMPORAL LOGIC

Alessandro Artale

Faculty of Computer Science – Free University of Bolzano

artale@inf.unibz.it http://www.inf.unibz.it/~artale/

Some material (text, figures) displayed in these slides is courtesy of:
Introducing Temporal Logics.

Intuitions beyond Linear Temporal Logic.

LTL: Syntax and Semantics.

LTL in Computer Science.

LTL Interpreted over Kripke Models.

LTL and Model Checking: Intuitions.
In classical logic, formulae are evaluated within a single fixed world.

For example, a proposition such as “it is Monday” must be either *true* or *false*.

Propositions are then combined using constructs such as ‘∧’, ‘¬’, etc.

But, most (not just computational) systems are *dynamic*.

In temporal logics, evaluation takes place within a set of worlds. Thus, “it is Monday” may be satisfied in some worlds, but not in others.
The set of worlds correspond to moments in time.

How we navigate between these worlds depends on our particular view of time.

The particular model of time is captured by a temporal accessibility relation between worlds.

Essentially, temporal logic extends classical propositional logic with a set of temporal operators that navigate between worlds using this accessibility relation.
Introducing Temporal Logics.

Intuitions beyond Linear Temporal Logic.

LTL: Syntax and Semantics.

LTL in Computer Science.

LTL Interpreted over Kripke Models.

LTL and Model Checking: Intuitions.
Consider a simple temporal logic (LTL) where the accessibility relation characterises a discrete, linear model isomorphic to the Natural Numbers.

Typical temporal operators used are

- $\bigcirc \phi$: $\phi$ is true in the *next* moment in time
- $\square \phi$: $\phi$ is true in *all* future moments
- $\Diamond \phi$: $\phi$ is true in *some* future moment
- $\phi \mathcal{U} \psi$: $\phi$ is true *until* $\psi$ is true

Examples:

$$\square((\neg\text{passport} \lor \neg\text{ticket}) \Rightarrow \bigcirc \neg\text{board_flight})$$
From the above we should be able to infer that it is not the case that the system continually re-sends a request, but never sees it completed (□¬done); i.e. the statement

□requested ∧ □¬done

should be inconsistent.
Summary

- Introducing Temporal Logics.
- Intuitions beyond Linear Temporal Logic.
- LTL: Syntax and Semantics.
- LTL in Computer Science.
- LTL Interpreted over Kripke Models.
- LTL and Model Checking: Intuitions.
LTL: Syntax

Countable set $\Sigma$ of atomic propositions: $p, q, \ldots$ the set $\text{FORM}$ of formulas is:

$\varphi, \psi \rightarrow p \mid \text{(atomic proposition)}$

$\top \mid \text{(true)}$

$\bot \mid \text{(false)}$

$\neg \varphi \mid \text{(complement)}$

$\varphi \land \psi \mid \text{(conjunction)}$

$\varphi \lor \psi \mid \text{(disjunction)}$

$\bigcirc \varphi \mid \text{(next time)}$

$\blacksquare \varphi \mid \text{(always)}$

$\lozenge \varphi \mid \text{(sometime)}$

$\varphi \mathcal{U} \psi \mid \text{(until)}$
We interpret our temporal formulae in a discrete, linear model of time. Formally, this structure is represented by

\[ M = \langle \mathbb{N}, I \rangle \]

where

- \( I : \mathbb{N} \mapsto 2^{\Sigma} \)

maps each Natural number (representing a moment in time) to a set of propositions.

The semantics of a temporal formula is provided by the satisfaction relation:

\[ \models : (M \times \mathbb{N} \times \text{FORM}) \rightarrow \{\text{true, false}\} \]
We start by defining when an atomic proposition is true at a time point “i”

\[ \langle M, i \rangle \models p \iff p \in I(i) \quad (\text{for } p \in \Sigma) \]

The semantics for the classical operators is as expected:

\[ \langle M, i \rangle \models \neg \phi \iff \langle M, i \rangle \not\models \phi \]
\[ \langle M, i \rangle \models \phi \land \psi \iff \langle M, i \rangle \models \phi \text{ and } \langle M, i \rangle \models \psi \]
\[ \langle M, i \rangle \models \phi \lor \psi \iff \langle M, i \rangle \models \phi \text{ or } \langle M, i \rangle \models \psi \]
\[ \langle M, i \rangle \models \phi \Rightarrow \psi \iff \text{if } \langle M, i \rangle \models \phi \text{ then } \langle M, i \rangle \models \psi \]
\[ M, i \models \top \]
\[ M, i \not\models \bot \]
Temporal Operators: ‘next’

\[ \langle M, i \rangle \models \Diamond \varphi \iff \langle M, i + 1 \rangle \models \varphi \]

This operator provides a constraint on the next moment in time.

Examples:

\( (sad \land \neg rich) \Rightarrow \Diamond sad \)
\( ((x = 0) \land add3) \Rightarrow \Diamond (x = 3) \)
Temporal Operators: ‘sometime’

\[ \langle M, i \rangle \models \Diamond \varphi \quad \text{iff} \quad \text{there exists } j. (j \geq i) \land \langle M, j \rangle \models \varphi \]

**N.B.** while we can be sure that \( \varphi \) will be true either now or in the future, we can not be sure exactly *when* it will be true.

Examples:

\[
(\neg \text{resigned} \wedge \text{sad}) \Rightarrow \Diamond \text{famous}
\]

\[
\text{sad} \Rightarrow \Diamond \text{happy}
\]

\[
\text{send} \Rightarrow \Diamond \text{receive}
\]
\[ \langle M, i \rangle \models \Box \varphi \iff \text{for all } j. \text{if } (j \geq i) \text{ then } \langle M, j \rangle \models \varphi \]

This can represent invariant properties.

Examples:

\[ \text{lottery-win} \Rightarrow \Box \text{rich} \]
Temporal Operators: ‘until’

\[ \langle M, i \rangle \models \phi \mathbin{U} \psi \iff \text{there exists } j. \ (j \geq i) \land \langle M, j \rangle \models \psi \land \text{for all } k. \ (i \leq k < j) \Rightarrow \langle M, k \rangle \models \phi \]

Examples:

- \textit{start\_lecture} \Rightarrow \textit{talk} \mathbin{U} \textit{end\_lecture}
- \textit{born} \Rightarrow \textit{alive} \mathbin{U} \textit{dead}
- \textit{request} \Rightarrow \textit{reply} \mathbin{U} \textit{acknowledgement}
A structure $\mathcal{M} = \langle \mathbb{N}, I \rangle$ is a model of $\phi$, if

$$\langle \mathcal{M}, i \rangle \models \phi, \text{ for some } i \in \mathbb{N}.$$  

Similarly as in classical logic, an LTL formula $\phi$ can be satisfiable, unsatisfiable or valid. A formula $\phi$ is:

- **Satisfiable**, if there is model for $\phi$.
- **Unsatisfiable**, if $\phi$ is not satisfiable.
- **Valid** (i.e., a Tautology):
  $$\models \phi \text{ iff } \forall \mathcal{M}, \forall i \in \mathbb{N}. \langle \mathcal{M}, i \rangle \models \phi.$$
Similarly as in classical logic we can define the notions of **entailment** and **equivalence** between two LTL formulas

- **Entailment.**
  \[ \phi \models \psi \text{ iff } \forall M, \forall i \in \mathbb{N}. \langle M, i \rangle \models \phi \Rightarrow \langle M, i \rangle \models \psi \]

- **Equivalence.**
  \[ \phi \equiv \psi \text{ iff } \forall M, \forall i \in \mathbb{N}. \langle M, i \rangle \models \phi \iff \langle M, i \rangle \models \psi \]
The temporal operators $\Box$ and $\Diamond$ are duals

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

$\Diamond$ (and then $\Box$) can be rewritten in terms of $\mathcal{U}$

$$\Diamond \varphi \equiv \top \mathcal{U} \varphi$$

All the temporal operators can be rewritten using the “Until” and “Next” operators
◊ distributes over ∨ while □ distributes over ∧

◊(ϕ ∨ ψ) ≡ ◊ϕ ∨ ◊ψ

□(ϕ ∧ ψ) ≡ □ϕ ∧ □ψ

The following equivalences are useful for generating formulas in Negated Normal Form.

¬□ϕ ≡ □¬ϕ

¬(ϕ U ψ) ≡ (¬ψ U (¬ϕ ∧ ¬ψ)) ∨ □¬ψ
Linear Temporal Logic can be thought of as

a specific decidable (PSPACE-complete) fragment of classical first-order logic

We just map each proposition to a unary predicate in FOL. In general, the following satisfiability preserving mapping ($\mapsto$) holds:

\[
\begin{align*}
p & \mapsto p(t) \\
\Box p & \mapsto p(t + 1) \\
\Diamond p & \mapsto \exists t'. (t' \geq t) \land p(t') \\
\square p & \mapsto \forall t'. (t' \geq t) \Rightarrow p(t')
\end{align*}
\]
Summary

- Introducing Temporal Logics.
- Intuitions beyond Linear Temporal Logic.
- LTL: Syntax and Semantics.
- LTL in Computer Science.
- LTL Interpreted over Kripke Models.
- LTL and Model Checking: Intuitions.
Temporal logic was originally developed in order to represent tense in natural language.

Within Computer Science, it has achieved a significant role in the formal specification and verification of concurrent reactive systems.

Much of this popularity has been achieved as a number of useful concepts can be formally, and concisely, specified using temporal logics, e.g.

- safety properties
- liveness properties
- fairness properties
Safety Properties

Safety:

“something bad will not happen”

Typical examples:

\[ \neg (\text{reactor}_\text{temp} > 1000) \]
\[ \neg (\text{one}_\text{way} \land \bigcirc \text{other}_\text{way}) \]
\[ \neg ((x = 0) \land \bigcirc \bigcirc \bigcirc \bigcirc (y = z/x)) \]

and so on.....

Usually: \[ \square \neg \text{....} \]
Liveness:

“something good will happen”

Typical examples:

◊ \textit{rich}

◊ \((x > 5)\)

□ \((\text{start} \Rightarrow \Diamond \text{terminate})\)

and so on.....

Usually: ◊ ....
Fairness Properties

Often only really useful when scheduling processes, responding to messages, etc.

Strong Fairness:

“if something is attempted/requested infinitely often, then it will be successful/allocated infinitely often”

Typical example:

$\blacksquare \Diamond \text{ready} \Rightarrow \blacksquare \Diamond \text{run}$
Introducing Temporal Logics.
Intuitions beyond Linear Temporal Logic.
LTL: Syntax and Semantics.
LTL in Computer Science.
LTL Interpreted over Kripke Models.
LTL and Model Checking: Intuitions.
Consider the following Kripke structure:

Its paths/computations can be seen as a set of linear structures (computation tree):
Path-Semantics for LTL

- LTL formulae are evaluated over the set $\mathbb{N}$ of Natural Numbers.

- Paths in Kripke structures are infinite and linear sequences of states. Thus, they are isomorphic to the Natural Numbers:

$$\pi = s_0 \rightarrow s_1 \rightarrow \cdots \rightarrow s_i \rightarrow s_{i+1} \rightarrow \cdots$$

- We want to interpret LTL formulas over Kripke structures.

- Given a Kripke structure, $\mathcal{K}M = (S, I, R, AP, L)$, a path $\pi$ in $\mathcal{K}M$, a state $s \in S$, and an LTL formula $\phi$, we define:

  1. $\langle \mathcal{K}M , \pi \rangle \models \phi$, and then

  2. $\langle \mathcal{K}M , s \rangle \models \phi$

Based on the LTL semantics over the Natural Numbers.
We first extract an LTL model, $\mathcal{M}_\pi = (\pi, I_\pi)$, from the Kripke structure $\mathcal{K}M$. $\mathcal{M}_\pi = (\pi, I_\pi)$ is such that:

- $\pi$ is a path in $\mathcal{K}M$.
- $I_\pi$ is the restriction of $L$ to states in $\pi$:

$$\forall s \in \pi \text{ and } \forall p \in AP, \ p \in I_\pi(s) \iff p \in L(s)$$

Given a Kripke structure, $\mathcal{K}M = (S, I, R, AP, L)$, a path $\pi$ in $\mathcal{K}M$, a state $s \in S$, and an LTL formula $\phi$:

1. $\langle \mathcal{K}M, \pi \rangle \models \phi$ iff $\langle \mathcal{M}_\pi, s_0 \rangle \models \phi$
   with $s_0$ initial state of $\pi$

2. $\langle \mathcal{K}M, s \rangle \models \phi$ iff $\langle \mathcal{K}M, \pi \rangle \models \phi$
   for all paths $\pi$ starting at $s$. 
Given a Kripke structure, $\mathcal{KM} = (S, I, R, AP, L)$, the LTL model checking problem $\mathcal{KM} \models \phi$:

Check if $\langle \mathcal{KM}, s_0 \rangle \models \phi$, for every $s_0 \in I$ initial state of the Kripke structure $\mathcal{KM}$. 
Summary

- Introducing Temporal Logics.
- Intuitions beyond Linear Temporal Logic.
- LTL: Syntax and Semantics.
- LTL in Computer Science.
- LTL Interpreted over Kripke Models.
- LTL and Model Checking: Intuitions.
Example 1: mutual exclusion (safety)

\[ \mathcal{KM} \models \square \neg (C_1 \land C_2) \]
Example 1: mutual exclusion (safety)

N = noncritical,  T = trying,  C = critical

\( K \mathcal{M} \models \Box \neg (C_1 \land C_2) \) ?

**YES:** There is no reachable state in which \((C_1 \land C_2)\) holds!
Example 2: mutual exclusion (liveness)

$\mathcal{KM} \models \Diamond C_1 ?$

$N = \text{noncritical}, \ T = \text{trying}, \ C = \text{critical}$

N1, N2

T1, N2

C1, N2

T1, T2

C1, T2

T1, C2

N1, T2

T1, C2

N1, C2

User 1

User 2
Example 2: mutual exclusion (liveness)

N = noncritical, T = trying, C = critical

N1, N2

T1, N2

C1, T2

T2, N1

T1, C2

N1, C2

KM = ♦ C1?

NO: the blue cyclic path is a counterexample!
Example 3: mutual exclusion (liveness)

\[
\mathcal{KM} \models \Box(T_1 \Rightarrow \Diamond C_1) ?
\]

N = noncritical, T = trying, C = critical
Example 3: mutual exclusion (liveness)

\[ \mathcal{KM} \models \Box (T_1 \Rightarrow \Diamond C_1) \ ? \]

\textbf{YES}: in every path if \( T_1 \) holds afterwards \( C_1 \) holds!
Example 4: mutual exclusion (fairness)

N = noncritical, T = trying, C = critical

\( \mathcal{KM} \models \lozenge C_1 ? \)
Example 4: mutual exclusion (fairness)

\[ \mathcal{KM} \models \Box \Diamond C_1 \]

**NO:** the blue cyclic path is a counterexample!
Example 4: mutual exclusion (strong fairness)

N = noncritical,  T = trying,  C = critical

\[ \mathcal{K}M \models \square \Diamond T_1 \Rightarrow \square \Diamond C_1 ? \]
Example 4: mutual exclusion (strong fairness)

\[ \mathcal{KM} \models \square \Diamond T_1 \Rightarrow \square \Diamond C_1 \]

**YES**: every path which visits \( T_1 \) infinitely often also visits \( C_1 \) infinitely often!
Alternative notations are used for temporal operators.

\[ \Diamond \leadsto F \text{ sometime in the Future} \]

\[ \square \leadsto G \text{ Globally in the future} \]

\[ \bigcirc \leadsto X \text{ neXtime} \]
Summary of Lecture III

- Introducing Temporal Logics.
- Intuitions beyond Linear Temporal Logic.
- LTL: Syntax and Semantics.
- LTL in Computer Science.
- LTL Interpreted over Kripke Models.
- LTL and Model Checking: Intuitions.