Tutorial 5: Linear Temporal Logic

Logan Murphy

CSC 410

Fall 2020
Contents

- Formalizing specifications
- Checking satisfaction
- Proving equivalences
In our proofs, we will be analyzing the semantics of LTL formulae

\[ \sigma \models \Phi \lor \Psi \]

\[ \sigma \models \Phi \quad \text{or} \quad \sigma \models \Psi \]

“By the definition of satisfiability with respect to \( \lor \)…”

\[ \sigma \models \Phi \lor \Psi \]

iff \( \sigma \models \Phi \quad \text{or} \quad \sigma \models \Psi \) (Def. \( \models \lor \))
Example.
Suppose we are reasoning about a system which can receive requests and send out answers.

\[ AP = \{ req, ans \} \]
Consider the transition system $M_1$ over $AP$:
Formalizing Specifications

Specifically, define the labelling function \( L : S \rightarrow \mathcal{P}(AP) \) as

\[
L(wait) = \emptyset \\
L(s) = \{s\} \quad (s \neq wait)
\]
Formalizing Specifications

Formalize the property

“No request is left unanswered”

One approach:
- Notice that the property describes an invariant.
- Define the behaviour we want, and then “quantify” it over the entire path.

\[ req \implies \Diamond ans \]

\[ \Box (req \implies \Diamond ans) \]

Recall:

\[ P \implies Q \iff \lnot P \lor Q \]
Another approach:

Sometimes, breaking down and rephrasing a property in a natural language can help us write appropriate formulae.

E.g.

“No request is left unanswered.”

“It is never the case that a request is made and an answer will never be issued.”

“It is ALWAYS NOT the case that (a request is made AND there is ALWAYS NOT an answer)”

\[ \square \neg (req \land \square \neg ans) \]

Warning: Natural languages can be ambiguous or misleading!
Let’s go with the first formulation,

\[ \Phi := \Box (req \implies \Diamond ans) \]

Question: Does \( M_1 \models \Phi \)?

\[
M_1 \models \Phi \iff \forall \pi \in \text{Paths}(M_1), \pi \models \Phi \\
\quad \iff \forall \pi \in \text{Paths}(M_1), \text{trace}(\pi) \models \Phi
\]
Checking Satisfaction

\[ \pi_1 = req \ wait \ ans \ wait^\omega \]
\[ \pi_2 = req \ wait \ ans \ (req \ ans)^\omega \]
Checking Satisfaction

\[ \sigma_1 = trace(\pi_1) = \{\text{req}\} \emptyset \{\text{ans}\} \emptyset^\omega \]
\[ \sigma_2 = trace(\pi_2) = \{\text{req}\} \emptyset \{\text{ans}\} (\{\text{req}\} \{\text{ans}\})^\omega \]
Checking Satisfaction

Does $\sigma_1 = \{ req \} \emptyset \{ ans \} \emptyset^\omega$ satisfy $\Phi$?

$\sigma_1 \models \Phi \iff \sigma_1 \models \Box (req \implies \Diamond ans)$

iff $\forall i \geq 0$, $\sigma_1[i..] \models req \implies \Diamond ans$ (Def. $\models \Box$)

iff $\forall i \geq 0$, $\sigma_1[i..] \models (\neg req) \lor \Diamond ans$ (Def. impl)

iff $\forall i \geq 0$, $\sigma_1[i..] \models \neg req$ or $\sigma_1[i..] \models \Diamond ans$ (Def. $\models \lor$)

iff $\forall i \geq 0$, $\sigma_1[i..] \not\models req$ or $\sigma_1[i..] \models \Diamond ans$ (Def. $\models \neg$)

iff $\forall i \geq 0$, $\sigma_1[i..] \not\models req$ or $\exists j \geq i$, $\sigma_1[j..] \models ans$ (Def. $\Diamond$)

Logan Murphy

Tutorial 5: Linear Temporal Logic
Does \( \sigma_1 = \{ req \} \emptyset \{ ans \} \emptyset^\omega \) satisfy \( \Phi \)?

Prove

\[
\forall i \geq 0, \ \sigma_1[i..] \not\models req \ \text{or} \ \exists j \geq i, \ \sigma_1[j..] \models ans
\]

Proof by cases:

Note: for all \( i > 0 \), the first case holds.

When \( i = 0 \), the second case holds with \( j = 2 \). QED.
Checking Satisfaction

Does $\sigma_2 = \{\text{req}\} \emptyset \{\text{ans}\} (\{\text{req}\} \{\text{ans}\})^\omega$ satisfy $\Phi$?

Prove

$$\forall i \geq 0, \sigma_2[i..] \not\models \text{req} \quad \text{or} \quad \exists j \geq i, \sigma_2[i..] \models \text{ans}$$

Proof by (more) cases:

When $i = 0$, second case holds with $j = 2$.

When $i = 1$ or $i = 2$, the first case holds.

For all $i \geq 3$,

- If $i$ is odd, the second case holds with $j = i + 1$.
- If $i$ is even, the first case holds.

QED.
Consider a new model, $M_2$

Does $M_2$ satisfy $\Phi$?
Checking Satisfaction

Notice that from $M_2$ we can form the word

$$\sigma_F = \{req\}\{ans\}\{req\}\emptyset^\omega$$

Try to prove

$$\forall i \geq 0, \sigma_F[i..] \not\models req \text{ or } \exists j \geq i, \sigma_F[i..] \models ans$$

Fails for $i = 2$, neither cases are met!

So

$$M_2 \not\models \Phi$$
Equivalence in LTL

Given two LTL formulae $\Phi, \Psi$, we say that $\Phi$ and $\Psi$ are equivalent if every model which satisfies $\Phi$ also satisfies $\Psi$, and vice versa.

\[
\Phi \equiv \Psi \iff \{ \sigma \mid \sigma \models \Phi \} = \{ \sigma \mid \sigma \models \Psi \}
\]

iff \[
\{ \sigma \mid \sigma \models \Phi \} \subseteq \{ \sigma \mid \sigma \models \Psi \} \quad \text{and} \quad \{ \sigma \mid \sigma \models \Psi \} \subseteq \{ \sigma \mid \sigma \models \Phi \}
\]

iff \[
\forall \sigma, \ \sigma \models \Phi \iff \sigma \models \Psi
\]
**Example.** Prove the duality law for the “next” operator: For any LTL formula $\Phi$,

$$\neg \bigcirc \Phi \equiv \bigcirc \neg \Phi$$

**Proof.** Suppose $\sigma \in (2^{AP})^\omega$.

$$\sigma \models \neg \bigcirc \Phi \iff \sigma \not\models \bigcirc \Phi \quad \text{(Def } \models \neg)$$
$$\quad \iff \sigma[1...] \not\models \Phi \quad \text{(Def } \models \bigcirc)$$
$$\quad \iff \sigma[1...] \models \neg \Phi \quad \text{(Def } \models \neg)$$
$$\quad \iff \sigma \models \bigcirc \neg \Phi \quad \text{(Def } \models \bigcirc)$$

QED.
Example. Prove the expansion law for the “eventually” operator: For any $\Phi$,

$$\Diamond \Phi \equiv (\Phi \lor \Box \Diamond \Phi)$$

Forward direction: if $\sigma \models \Diamond \Phi$, then $\sigma \models (\Phi \lor \Box \Diamond \Phi)$
Equivalence in LTL

Forward direction: if $\sigma \models \Diamond \Phi$, then $\sigma \models \Phi \lor \Box \Diamond \Phi$.

Suppose $\sigma \models \Diamond \Phi$.

Need to show that either $\sigma \models \Phi$ or $\sigma \models \Box \Diamond \Phi$.

Then (by the definition of $\models \Diamond$)

$$\exists i \geq 0, \sigma[i..] \models \Phi$$

Proof by case analysis on $i$

- if $i = 0$, then $\sigma[0..] \models \Phi$. Hence $\sigma \models \Phi$, and we are done.
- $i = j + 1$ for some $j$. Then $\exists j, \sigma[1 + j..] \models \Phi$

$$\exists j, \sigma[1..][j..] \models \Phi$$

iff $\sigma[1..] \models \Diamond \Phi$ (Def. $\models \Diamond$)

$$\sigma \models \Box \Diamond \Phi$$ (Def. $\models \Box$)
Equivalence in LTL

Reverse direction: if $\sigma \models \Phi \lor \Diamond \Diamond \Phi$, then $\sigma \models \Diamond \Phi$.

To show $P \lor Q$ implies $R$, show that both $P$ implies $R$ and $Q$ implies $R$.

By recalling the definition of $\models \Diamond$, we see that we need to prove

$$\exists j \geq 0, \sigma[j..] \models \Phi$$

By assumption, either $\sigma \models \Phi$, or $\sigma \models \Diamond \Diamond \Phi$.

- If $\sigma \models \Phi$, use $j = 0$. Done.
- If $\sigma \models \Diamond \Diamond \Phi$,

  $$\sigma \models \Diamond \Diamond \Phi \quad \text{iff} \quad \sigma[1..] \models \Diamond \Phi \quad \text{(Def. $\models \Diamond$)}$$

  $$\text{iff} \quad \exists k, \sigma[1..][k..] \models \Phi \quad \text{(Def. $\models \Diamond$)}$$

  I.e. $\sigma[k + 1..] \models \Phi$, so use $j = k + 1$. QED.
Equivalence in LTL

**Example.** Prove the expansion law for the “always” operator: For any LTL formula $\Phi$,

$$\square \Phi \equiv \Phi \land \bigcirc \square \Phi$$
Equivalence in LTL

Forward direction: if $\sigma \vDash \Box \Phi$ then $\sigma \vDash \Phi \land \Diamond \Box \Phi$

We need to prove both conjuncts:
$P$ implies $Q \land R$ iff $P$ implies $Q$ and $P$ implies $R$.

By the definition of $\vDash \Box$, we have $\forall i \geq 0, \sigma[i..] \vDash \Phi$ and in particular
$$\sigma[0..] = \sigma \vDash \Phi$$

so that conjunct is proved.
For the other, note that

$$\sigma \vDash \Diamond \Box \Phi$$

iff $\sigma[1..] \vDash \Box \Phi$ \hspace{1cm} (Def. $\vDash \Diamond$)

iff $\forall j, \sigma[1..][j..] \vDash \Phi$ \hspace{1cm} (Def. $\vDash \Box$)

By assumption, $\forall (j + 1), \sigma[j + 1..] \vDash \Phi$. 
Reverse direction: if $\sigma \models \Phi \land \Box \Box \Phi$ then $\sigma \models \Box \Phi$

Now, we need to prove $\forall i \geq 0, \sigma[i..] \models \Phi$

By assumption, we have $\sigma \models \Phi$ and $\sigma \models \Box \Box \Phi$.

Take any $i$, and we will show that $\sigma[i..] \models \Phi$.

Either $i = 0$ or $i = k + 1$ for some $k$.
- In the first case, we just need to show $\sigma[0..] \models \Phi$, which is our assumption.
- In the second case, we need to show $\sigma[k + 1..]$ for any $k$.
  But by assumption

  \[
  \sigma \models \Box \Box \Phi
  \]
  \[
  \text{iff } \sigma[1..] \models \Box \Phi \quad \quad \text{(Def. } \models \Box)\]
  \[
  \text{iff } \forall k, \sigma[1..][k..] \models \Phi \quad \quad \text{(Def. } \models \Box)\]
  \[
  \text{iff } \forall k, \sigma[k + 1..] \models \Phi
  \]

QED
Equivalence in LTL

**Example.** Prove the expansion law for the “until” operator:
For any LTL formulae $\Phi$ and $\Psi$,

$$\Phi U \Psi \equiv \Psi \lor (\Phi \land \Box(\Phi U \Psi))$$
Equivalence in LTL

Forward Direction: if $\sigma \models \Phi U \Psi$ then $\sigma \models \Psi \lor (\Phi \land \Diamond(\Phi U \Psi))$

First, recall that

\[
\sigma \models \Phi U \Psi \iff \exists j \geq 0. \sigma[j...] \models \Psi \quad \text{and} \quad \forall i < j \sigma[i..] \models \Phi
\]

Suppose $\sigma \models \Phi U \Psi$. Then $\exists j$ such that

1) $\sigma[j..] \models \Psi$

2) $\forall i < j, \sigma[i..] \models \Phi$

What do we know about $j$?
Equivalence in LTL

Proof by case analysis on $j$: either $j = 0$ or $j = k + 1$ for some $k$. Want to prove

$$\sigma \models \Psi \lor (\Phi \land \Diamond(\Phi U \Psi))$$

I.e. show either $\sigma \models \Psi$ or $\sigma \models \Phi \land \Diamond(\Phi U \Psi)$

If $j = 0$, then by premise 1) becomes $\sigma[0..] \models \Psi$. This is enough to prove the goal (left disjunct).

If $j = k + 1$, then premise 2) becomes $\forall i < (k + 1), \sigma[i..] \models \Phi$

We have nothing that says that $\Psi$ at the current time step, so we should work to prove the right disjunct holds.
Equivalence in LTL

Need to prove:

$$\sigma \models \Phi \land \Diamond (\Phi \cup \Psi)$$

Our premises are:

1) \(\sigma[k + 1..] \models \Psi\)

2) \(\forall i < k + 1, \sigma[i..] \models \Phi\)

To prove the left conjunct, note that premise 2) says that in particular \(\sigma[0..] \models \Phi\)
To prove $\sigma \models \Box(\Phi U \Psi)$, note that

$$\sigma \models \Box(\Phi U \Psi) \iff \sigma[1..] \models \Phi U \Psi$$

$$\iff \exists n, \sigma[1..][n..] \models \Psi \quad \text{and} \quad \forall m < n, \sigma[1..][m..] \models \Phi$$

We’re actually just going to use $k$.

The left clause is our premise 1) from before:

$$\sigma[k + 1] \models \Psi$$

To get the right clause, take any $m < k$.

Next, note that $m + 1 < k + 1$ since $m < k$.

Thus by premise 2), we have $\sigma[m + 1..] = \sigma[1..][m..] \models \Phi$. 
Reverse direction: if $\sigma \models \psi \lor (\phi \land \circ (\phi \cup \psi))$ then $\sigma \models \phi \cup \psi$

Suppose $\sigma \models \psi \lor (\phi \land \circ (\phi \cup \psi))$.

We need to show

$$\exists j \geq 0, \sigma[j..] \models \psi \text{ and } \forall i < j, \sigma[i..] \models \phi$$

Perform case analysis on our premise.

Case 1: $\sigma \models \psi$.

$$\exists 0, \sigma[0..] \models \psi \text{ and } \forall i < 0, \sigma[i..] \models \phi$$

LHS holds, RHS is vacuously true

Case 2: Left as an excercise to check your comprehension :)