Temporal Logic

[Syntax and Semantics]

Michael Fisher

Department of Computer Science, University of Liverpool, UK

MFisher@liverpool.ac.uk

An Introduction to Practical Formal Methods Using Temporal Logic

PTL Syntax

Formulae in PTL are constructed from the following.

- A finite set of propositional symbols, \( \text{PROP} \), such as \( p, q, r, \text{trigger}, \text{terminate\_condition2}, \text{lunch}, \ldots \)
- Propositional connectives: \( \text{true}, \text{false}, \neg, \lor, \land, \Rightarrow \).
- Temporal connectives: \( \Box, \Diamond, \text{start}, U, \text{and} W \).
- Parentheses, ‘(‘ and ‘)’, used to avoid ambiguity.

The set of well-formed formulae of PTL, denoted by \( \text{WFF} \), is now inductively defined as follows.

- \( \text{PROP} \subseteq \text{WFF} \), and \( \text{true}, \text{false} \) and \( \text{start} \) are in \( \text{WFF} \).
- If \( \varphi \) and \( \psi \) are in \( \text{WFF} \), then so are
  - \( \neg\varphi \quad \varphi \lor \psi \quad \varphi \land \psi \quad \varphi \Rightarrow \psi \quad (\varphi) \)
  - \( \Diamond \varphi \quad \Box \varphi \quad \varphi U \psi \quad \varphi W \psi \quad \Diamond\varphi \).

Examples of Syntax

The following are all legal \( \text{WFF} \) of PTL

\[
p U (q \land \Diamond r) \quad a \Rightarrow \Box \Diamond (bWc) \quad (f \land \Diamond g) U \Box \neg h
\]

But the following are not

\[
p \Diamond q \quad (U r) \quad a \Rightarrow \Box b \Box c
\]

Semantic Structures (1)

Models of PTL are formally

\[
\text{Model} = \langle S, R, \pi \rangle
\]

where

- \( S \) is the set of \textit{moments} in time (accessible worlds),
- \( R \) is the \textit{temporal accessibility relation} (linear, discrete, finite past), and
- \( \pi : S \mapsto \mathcal{P} \text{PROP} \), a \textit{propositional valuation}, mapping each moment/world to a set of propositions (i.e. those that are true in that moment/world).
**Semantic Structures (2)**

A linear, discrete relation, such as \( R \), is isomorphic to \( \mathbb{N} \). So, this is often reduced to

\[
\text{Model} = \langle \mathbb{N}, \pi \rangle
\]

where

\[
\pi : \mathbb{N} \rightarrow \mathcal{P}\text{PROP}
\]

maps each moment in time to a set of propositions.

And, still further to

\[
\text{Model} = s_0, s_1, s_2, s_3, \ldots
\]

where each \( s_i \) is a set of propositions.

But: We will generally use the \( \text{Model} = \langle \mathbb{N}, \pi \rangle \) variety.

**Formal Semantics**

The semantics of a temporal formula is provided by an interpretation relation

\[
\models : (\text{Model} \times \mathbb{N}) \rightarrow \mathbb{B}
\]

For a model, \( M \), temporal index, \( i \), and formula, \( \varphi \), then

\[
\langle M, i \rangle \models \varphi
\]

is true if \( \varphi \) is satisfied at moment \( i \) within model \( M \).

The way the interpretation relation is defined provides the semantics for the logic.

**Semantic Structures (3)**

We will use the

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

semantic basis, which can be viewed as

\[
\begin{array}{c}
\bullet \quad \bullet \quad \bullet \\
\pi(i) \quad \pi(i+1) \quad \\
P, q, s, w \quad p, q, s, \ldots
\end{array}
\]

\[
\begin{array}{c}
\bullet \quad \bullet \quad \bullet \\
\pi(i) \quad \pi(i+1) \quad \\
P, q, s, w \quad p, q, s, \ldots
\end{array}
\]

**Semantics of Propositions**

We begin with the semantics of basic propositions:

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

i.e. look up the proposition in the model provided to see whether it is satisfied or not.

**Recall:**

\[
\begin{array}{c}
\bullet \quad \bullet \quad \bullet \\
\pi(i) \quad \pi(i+1) \quad \\
P, q, s, w \quad p, q, s, \ldots
\end{array}
\]
Semantics of Classical Operators

Next we consider the standard classical operators.

\[ \langle M, i \rangle \models \neg \varphi \iff \text{it is not the case that } \langle M, i \rangle \models \varphi \]

\[ \langle M, i \rangle \models \varphi \land \psi \iff \langle M, i \rangle \models \varphi \text{ and } \langle M, i \rangle \models \psi \]

\[ \langle M, i \rangle \models \varphi \lor \psi \iff \langle M, i \rangle \models \varphi \text{ or } \langle M, i \rangle \models \psi \]

And so on....

Temporal Operators: Start

\[ \langle M, i \rangle \models \text{start} \iff (i = 0) \]

Only ever satisfied at the “beginning of time”.

Temporal Operators: Next

Provides a constraint on the next moment in time.

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

Examples

\[ \langle \text{sad} \land \neg \text{rich} \rangle \models \Box \text{sad} \]
\[ \text{hop} \land \Box \text{skip} \land \Box \Box \text{jump} \]
\[ \langle x \_equals \_1 \land \text{added} \_3 \rangle \models \Box (x \_equals \_4) \]

Temporal Operators: Sometime

Provides a constraint on the future — we can not be sure when \( \varphi \) will be true, only that it will eventually occur.

\[ \langle M, i \rangle \models \Diamond \varphi \iff \text{there exists } j \geq i \text{ such that } \langle M, j \rangle \models \varphi \]
Temporal Operators: Sometime

There is a choice in the semantics of ‘sometime’ about whether to take $j \geq i$ or $j > i$; an alternative operator can be defined as follows:

\[ (M, i) \models \diamondsuit \varphi \iff \text{there exists } j > i \text{ such that } (M, j) \models \varphi \]

Clearly:

\[ \diamondsuit \varphi \leftrightarrow (\varphi \lor \diamondsuit \varphi) \]

Examples:

\[ \neg \text{resigned} \land \text{sad} \Rightarrow \diamondsuit \text{famous} \]
\[ \diamondsuit \text{accident} \Rightarrow (\Box \text{buy_insurance}) \]
\[ \text{sad} \Rightarrow \Box \text{happy} \]
\[ \text{is_monday} \Rightarrow \diamondsuit \text{is_friday} \]

Temporal Operators: Always

Provides invariant properties (c.f. safety properties).

\[ (M, i) \models \Box \varphi \iff \text{for all } j. \text{ if } (j \geq i) \text{ then } (M, j) \models \varphi \]

Example

Why do we term $\Box \diamondsuit p$, “infinitely often $P$”?

Let us take the semantics of $\Box \diamondsuit p$ at a particular moment $i$ in model $M$:

\[ (M, i) \models \Box \diamondsuit \varphi \iff \text{for all } j. \text{ if } (j \geq i) \text{ then } (M, j) \models \Box \varphi \]

Now, choose a $j$, and a $k \geq j$ where $(M, k) \models \varphi$
As we quantify over all $j$’s, then we can now choose another $j$, such that $j > k$, which requires us to satisfy $\varphi$ again in the future, and so on....

Aside: No Future

Rather than using $\mathbb{N}$ as our underlying model of time, what if we use a linear, discrete sequence, but with a finite length:

Semantics of the temporal operators must be modified.
For example, the ‘$\Box$’ operator typically defaults to true if there is no ‘next’ moment. So, ‘$\Box \text{false}$’ is actually only satisfied at the last state in a finite sequence!

See also: bounded approximations and related techniques.

"Spatial Logics": A State-of-the-Art Survey

"Temporal Logics": An Introduction to Practical Formal Methods Using Temporal Logic
Temporal Operators: Until

A property persists until a point occurs (which is guaranteed to occur) where another property becomes true.

\[ \langle M, i \rangle \models \varphi U \psi \iff \text{there exists } j. (j \geq i) \text{ and } \langle M, j \rangle \models \psi \text{ and for all } k. \text{if } (j > k \geq i) \text{ then } \langle M, k \rangle \models \varphi \]

Examples:
- \( \_ \_ \text{start\_lecture} \Rightarrow \text{talk\_U\_end\_lecture} \)
- \( \_ \_ \text{born} \Rightarrow \text{living\_U\_dead} \)

Temporal Operators: Unless (1)

Unless: as until, except that the ‘\( \psi \)’ point is not guaranteed to occur and so the persistent property can potentially persist forever.

\[ \langle M, i \rangle \models \varphi W \psi \iff \langle M, i \rangle \models \varphi U \psi \text{ or } \langle M, i \rangle \models \square \varphi \]

Examples:
- \( \_ \_ \text{stay\_in\_roomW\_fire\_alarm} \)
- \( \_ \_ \text{commence} \Rightarrow \text{(executing\_W\_stop\_msg)} \)

Useful Interactions

By their semantic definitions:

- \( aUb \leftrightarrow ((aWb) \land \Diamond b) \)
- \( cWd \leftrightarrow ((cUd) \lor \Box c) \)

Of course:

- \( \neg \Box r \leftrightarrow \Diamond \neg r \)

Less obviously:

- \( \neg (eUf) \leftrightarrow (\neg f)W(\neg f \land \neg e) \)
- \( \neg (pWq) \leftrightarrow (\neg q)U(\neg p \land \neg q) \)

But, happily, at least in infinite and linear models,

- \( \neg \Diamond w \leftrightarrow \Diamond \neg w \)