TEMPORAL LOGIC(S)

Languages that can specify the behavior of a reactive program.

Two views:

1. the program generates a set of sequences of states
   - the models of temporal logic are infinite sequences of states
   - LTL (linear time temporal logic)
     [Manna, Pnueli] approach

2. the program generates a tree, where the branching points represent nondeterminism in the program
   - the models of temporal logic are infinite trees
   - CTL (computation tree logic)
     [Clarke, Emerson] at CMU
     Also CTL*

Temporal logic: underlying assertion language

Assertion language $\mathcal{L}$:
- first-order language over interpreted typed symbols
  (functions and relations over concrete domains)

Example: $x > 0 \rightarrow x + 1 > y$

$x, y \in \mathbb{Z}^+$

formulas in $\mathcal{L}$ called:
- state formulas or assertions
Temporal logic: underlying assertion language (Con’t)

A state formula is evaluated over a single state to yield a truth value.

For state $s$ and state formula $p$

$$s \models p \quad \text{if} \quad s[p] = T$$

We say:

- $p$ holds at $s$
- $s$ satisfies $p$
- $s$ is a $p$-state

**Example:**

For state $s \{ x : 4, y : 1 \}$

$$s \not\models x = 0 \lor y = 1$$
$$s \not\models x = 0 \land y = 1$$
$$s \not\models \exists z. x = z^2$$

Temporal logic: underlying assertion language (Con’t)

$p$ is state-satisfiable if

$$s \notmodels p \quad \text{for some state } s$$

$p$ is state-valid if

$$s \models p \quad \text{for all states } s$$

$p$ and $q$ are state-equivalent if

$$s \notmodels p \quad \text{iff} \quad s \notmodels q \quad \text{for all states } s$$

**Example:** $(x, y : \text{integer})$

state-valid:

$$x \geq y \leftrightarrow x + 1 > y$$

state-equivalent:

$$x = 0 \rightarrow y = 1$$

and

$$x \neq 0 \lor y = 1$$

TEMPORAL LOGIC (TL)

A formalism for specifying sequences of states

$TL = \text{assertions} + \text{temporal operators}$

- **assertions** (state formulas):
  - First-order formulas describing the properties of a single state

- **temporal operators**
  - **Future Temporal Operators**
    - $\square p$ – Henceforth $p$
    - $\diamond p$ – Eventually $p$
    - $p U q$ – $p$ Until $q$
    - $p W q$ – $p$ Waiting-for (Unless) $q$
    - $\circ p$ – Next $p$

- **Past Temporal Operators**
  - $\square p$ – So-far $p$
  - $\diamond p$ – Once $p$
  - $p S q$ – $p$ Since $q$
  - $p B q$ – $p$ Back-to $q$
  - $\circ p$ – Previously $p$
  - $\circ p$ – Before $p$

Fig. 0.15. The temporal operators
Temporal Logic: Syntax

- Every assertion is a temporal formula
- If \( p \) and \( q \) are temporal formulas (and \( u \) is a variable), so are:
  - \( \neg p \)
  - \( p \lor q \)
  - \( p \land q \)
  - \( p \rightarrow q \)
  - \( p \leftarrow q \)
  - \( \exists u.p \)
  - \( \forall u.p \)
  - \( \Box p \)
  - \( \Diamond p \)
  - \( pUq \)
  - \( pWq \)
  - \( pS q \)
  - \( pB q \)
  - \( \bigcirc p \)
  - \( \bigotimes p \)

Example:

\[ \Box(x > 0 \rightarrow \Diamond y = x) \]
\[ pUq \rightarrow \Diamond q \]

Temporal Logic: Semantics

Temporal formulas are evaluated over a model (an infinite sequence of states)

\[ \sigma : s_0, s_1, s_2, \ldots \]

- The semantics of temporal logic formula \( p \) at a position \( j \geq 0 \) in a model \( \sigma \),
  
  \[ (\sigma, j) \vDash p \]

"formula \( p \) holds at position \( j \) of model \( \sigma \)",

is defined by induction on \( p \):

\[ \sigma : s_0, s_1, \ldots, s_j, \ldots \]
\[ (\sigma, j) \]
Temporal Logic: Semantics (Con’t)

For state formula (assertion) \( p \) (i.e., no temporal operators)

- \( (\sigma, j) \notmodels p \iff s_j \notmodels p \)

For a temporal formula \( p \):

- \( (\sigma, j) \notmodels \neg p \iff (\sigma, j) \notmodels \neg p \)
- \( (\sigma, j) \models p \lor q \iff (\sigma, j) \models p \) or \( (\sigma, j) \models q \)

Temporal Logic: Semantics (Con’t)

- \( (\sigma, j) \models \square p \iff \) for all \( k \geq j \), \( (\sigma, k) \notmodels p \)

\[
\begin{array}{cccccc}
p & p & p & \cdots & p & q \\
0 & j & \cdots & k & \\
\end{array}
\]

- \( (\sigma, j) \models \Diamond p \iff \) for some \( k \geq j \), \( (\sigma, k) \models p \)

\[
\begin{array}{cccc}
p & p & p & \cdots & p \\
0 & j & \cdots & k & \\
\end{array}
\]

- \( (\sigma, j) \models \parr p \iff (\sigma, j) \models p \lor q \) or \( (\sigma, j) \models \square p \)

- \( (\sigma, j) \models \Diamond p \iff \) for some \( k \leq j \), \( (\sigma, k) \models p \)

\[
\begin{array}{cccc}
p & p & p & \cdots & p & p \\
0 & j & \cdots & k & \end{array}
\]
Temporal Logic: Semantics (Con’t)

• \((\sigma, j) \models p S q \iff\)
  for some \(k, 0 \leq k \leq j\), \((\sigma, k) \models q\)
  and for all \(i, k < i \leq j\), \((\sigma, i) \models p\)

\(q\quad p\quad \cdots\quad p\quad p\)
\(0\quad k\quad \cdots\quad j\)

• \((\sigma, j) \models p B q \iff\)
  \((\sigma, j) \models p S q\) or \((\sigma, j) \not\models p\)

Simple Examples

Given temporal formula \(\phi\), describe model \(\sigma\), such that
\((\sigma, 0) \models \phi\)

\(p \rightarrow \Diamond q\)
if initially \(p\) then eventually \(q\)

\(\Box (p \rightarrow \Diamond q)\)
every \(p\) is eventually followed by a \(q\)

\(\Box \Diamond q\)
every position is eventually followed by a \(q\),
i.e.,
infinitely many \(q\)'s

Simple Examples (Con’t)

\(\Diamond \Box q\)
eventually permanently \(q\),
i.e.,
finitely many \(\neg q\)'s

\(\Box \Diamond p \rightarrow \Box \Diamond q\)
if there are infinitely many \(p\)'s
then there are infinitely many \(q\)'s

\((\neg p) W q\)
\(q\) precedes \(p\) (if \(p\) occurs)

\(\Box (p \rightarrow \Diamond p)\)
once \(p\), always \(p\)

\(\Box (q \rightarrow \Diamond p)\)
every \(q\) is preceded by a \(p\)
Nested Waiting-for Formulas

\[ q_1 \mathcal{W} q_2 \mathcal{W} q_3 \mathcal{W} q_4 \]

stands for

\[ q_1 \mathcal{W} (q_2 \mathcal{W} (q_3 \mathcal{W} q_4)) \]

intervals of continuous \( q_i \)

\[ \begin{array}{cccccc}
q_1 \cdots q_1 & q_2 \cdots q_2 & q_3 \cdots q_3 & q_4 \\
0 & \uparrow \\
\end{array} \]

- possibly empty interval

\[ \begin{array}{cccccc}
q_1 \cdots q_1 & q_2 \cdots q_2 & q_3 \cdots q_3 & q_4 \\
0 & \uparrow \\
\end{array} \]

- possibly infinite interval

\[ \begin{array}{cccccc}
q_1 \cdots q_1 & q_2 \cdots q_2 & q_3 q_3 q_3 \cdots q_3 \cdots \cdots \\
0 & \uparrow & \rightarrow \\
\end{array} \]

Definitions

- For temporal formula \( p \), sequence \( \sigma \) and position \( j \geq 0 \):

  \[ (\sigma, j) \vDash p: p \text{ holds at position } j \text{ of } \sigma \]

  \[ \sigma \text{ satisfies } p \text{ at } j \]

  \[ j \text{ is a } p\text{-position in } \sigma. \]

- For temporal formula \( p \) and sequence \( \sigma \),

  \[ \sigma \vDash p \iff (\sigma, 0) \vDash p \]

Satisfiable/Valid

For temporal formula \( p \),

- \( p \) is satisfiable if \( \sigma \vDash p \) for some sequence (model) \( \sigma \)

- \( p \) is valid if \( \sigma \vDash p \) for all sequences (models) \( \sigma \)

\( p \) is valid iff \( \neg p \) is unsatisfiable

Example:

\[ (x : \text{integer}) \]

\[ \Diamond (x = 0) \text{ is satisfiable} \]

\[ \Diamond (x = 0) \lor \Box (x \neq 0) \text{ is valid} \]

\[ \Diamond (x = 0) \land \Box (x \neq 0) \text{ is unsatisfiable} \]
Equivalence

For temporal formulas $p$ and $q$:

$p$ is equivalent to $q$, written $p \sim q$
if $p \leftrightarrow q$ is valid
(i.e., $p$ and $q$ have the same truth-value at the first position of every model)

For the same reason,

\[
(\sigma, j) \not\models \psi \quad \text{true for } j = 0
\]
false for $j > 0$

\[
(\sigma, j) \not\models \varphi \quad \text{true for } j = 0
\]
false for $j > 0$

Then

\[
T \sim \Box T \sim \text{first}
\]

\[
T, \Box T, \text{first} \text{ are valid}
\]

Assume $V=\{\text{integer } x\}$

\[
\text{first} : -\bigcirc (x = 0 \lor x \neq 0)
\]

\[
T : (x = 0 \lor x \neq 0)
\]
\[
\Box T : (x = 0 \lor x \neq 0)
\]

For arbitrary $\sigma$:

\[
(\sigma, 0) \models \text{first} \quad (\sigma, 0) \models T \quad (\sigma, 0) \models \Box T
\]

\[
(\sigma, j) \not\models \text{first} \quad (\sigma, j) \models T \quad (\sigma, j) \models \Box T \quad \text{for } j > 0
\]

Congruences

"conjunction character" — match well with $\land$
"disjunction character" — match well with $\lor$

$\Box$ and $\bigcirc$ have conjunction character

$\bigcirc$ and $\Diamond$ have disjunction character

$U, W, S, B$ first argument has conjunction character
second argument has disjunction character

$\Box (p \land q) \approx \Box p \land \Box q$

$\bigcirc (p \lor q) \approx \bigcirc p \lor \bigcirc q$

$pU(q \lor r) \approx (pUq) \lor (pUr)$

$(p \land q)Ur \approx (pUr) \land (qUr)$

$pW(q \lor r) \approx (pWq) \lor (pWr)$

$(p \land q)Wr \approx (pWr) \land (qWr)$
Expansions

\[ \Box p \approx (p \land \Box p) \]
\[ \Diamond p \approx (p \lor \Diamond p) \]
\[ pUq \approx [q \lor (p \land (pUq))] \]

\[ \Box p \approx (p \land \Diamond p) \]
\[ \Diamond p \approx (p \lor \Diamond p) \]
\[ pSq \approx [q \lor (p \land (pSq))] \]

Strict Operators

(present not included)

\[ s_0 \quad s_{j-1} \uparrow \quad s_{j+1} \]

\[ \Box p \approx \Box \Box p \quad \Diamond p \approx \Diamond \Diamond p \]
\[ pUq \approx \Diamond (pUq) \quad pSq \approx \Diamond (pSq) \]
\[ pWq \approx \Diamond (pWq) \quad pBq \approx \Diamond (pBq) \]

Next and Previous Values of Exps

When evaluating \( x \) at position \( j \geq 0 \)

\[ x \] refers to \( s_j[x] \)
\[ x^+ \] refers to \( s_{j+1}[x] \)
\[ x^- \] refers to \[ \begin{cases} s_{j-1}[x] & \text{if } j > 0 \\ s_0[x] & \text{if } j = 0 \end{cases} \]

Example:

\[ \sigma: \langle x:0 \rangle, \langle x:1 \rangle, \langle x:2 \rangle, \ldots \]
satisfies

\[ x = 0 \land \Box (x^+ = x + 1) \land \Diamond \Box (x = x^- + 1) \]

Temporal Logic: Substitutivity

The ability to substitute equals for equals in a formula and obtain a formula with identical meaning.

\[ \bullet \text{ For state formula } \phi(u) \]
\[ \text{if } p \sim q \text{ then } \phi(p) \sim \phi(q) \]

Example:

Consider state formula \( \phi(u): r \land u \)

Since \[ \Diamond p \sim \Diamond \Diamond p \]
then \[ r \land \Diamond p \sim r \land \Diamond \Diamond p. \]
Temporal Logic: Substitutivity (Con’t)

This does not hold if \( \phi(u) \) is a temporal formula.

**Example:**
Consider temporal formula \( \phi(u) : \Box u \)

\[
\begin{align*}
&\Diamond p \sim \Diamond \Diamond p \\
&\text{but } \Box \Diamond p \not\sim \Box \Diamond \Diamond p
\end{align*}
\]

- For temporal formula \( \phi(u) \)
  
  if \( p \approx q \) then \( \phi(p) \approx \phi(q) \)

**Example:**
Consider the temporal formula \( \phi(u) : q U u \)

Since \( \Box p \approx \neg \Diamond \neg p \)

therefore \( q U (\Box p) \approx q U (\neg \Diamond \neg p) \)