0 Announcements

Coming back from spring break, we are now switching to a discussion on model checking on temporal logic.

1 Temporal Logic

1.1 Background

The simplest is linear time temporal logic (LTL), which in the last few years has been extended to both software and hardware. There are roughly 4 – 7 different kinds of temporal logic

- When working in temporal logic, our model $M$ contains several states where $M$ is a transition system.
- Our property $\varphi$ is a WFF that can be true in some states and false in others.

1.2 Example

```
- initial state (our example can only start at A or B)  
- final state (our example can only end at A)  
- A legal path will go from an initial state to a final state
```

Unlike propositional or first/second order logic, truth in temporal logic is dynamically defined. Many different properties can be expressed with temporal logic (i.e. fairness, deadlock, etc) where our $\varphi$ is only true in some states.

There are several ways we can define time with regards to temporal logic:

- linear
- branching
- discrete
- continuous
2 Syntax of LTL

Our syntax is a mixture of past terms from propositional logic (ie \( p, \neg \varphi, \bot \) etc) and new terms (see lecture Handout 18 for the complete syntax).

New terms include:

- \( \mathbf{X} \varphi \) (the "next" state)
- \( \mathbf{F} \varphi \) (a "future")
- \( \mathbf{G} \varphi \) (all global "future" states)
- \( \varphi \mathbf{U} \psi \) (until)
- \( \varphi \mathbf{W} \psi \) (weak until)
- \( \varphi \mathbf{R} \psi \) (release)

Like logics discussed before, LTL syntax has a binding hierarchy. Unary is the tightest, \( \mathbf{U}, \mathbf{W}, \mathbf{R} \) is tighter than \{\&, \lor, \rightarrow\} and \{\&, \lor\} continues to bind more tightly than \{\rightarrow\}

3 Semantics of LTL

The most recent successes in the field have been with the formal semantics of temporal logic. Since this is still a young field, there are relatively few books on the subject. In the last 2-3 years, there has been work with "unbounded" systems (ie infinite systems).

We will reuse our example from above and define \( A, B, \) and \( C \) in terms of the atoms \( p, q, r \).

We can define the model in the following manner \((S, \rightarrow, L, \text{Init}, \text{Fin})\). (Our model need not have all 5 elements, but at a very minimum it will have a graph).

3.1 Defining paths

An infinite path \( \pi \) in \( M \) is an infinite sequence of states. A possible path from the graph above is the following: \( A \ B \ A \ B \ C \ C \ C \ C \ A \). (The book will write it with \( \rightarrow \) in between like so: \( A \rightarrow B \rightarrow A \ldots \) Both are valid). An invalid path would include something like \( C \rightarrow B \) since there is no edge from \( C \) to \( B \).

3.2 Semantic rules

1. \( \pi \models \top \)
2. \( \pi \not\models \bot \)
3. \( \pi \models p \) iff \( p \in L(s_1) \) (check if atom \( p \) is found within the start state of the path)
4. $\pi \models \neg \varphi$
5. $\pi \models \varphi \land \psi$
6. $\pi \models \varphi \lor \psi$
7. $\pi \models \varphi \rightarrow \psi$
8. $\pi \models X\varphi$ iff $\pi^2 \models \varphi$
9. $\pi \models G\varphi$ iff for every $i \geq 1, \pi^i \models \varphi$
10. $\pi \models F\varphi$ iff there is $i \geq 1, \pi^i \models \varphi$
11. $\pi_i \models \varphi \quad U \quad \psi$ iff there is $i \geq 1$ s.t. $\pi^i \models \psi$ and $\pi^1 \models \varphi, \pi^2 \models \varphi, \ldots, \pi^{i-1} \models \varphi$
12. $\pi_i \models \varphi \quad W \quad \psi$ iff $EITHER$ there is $i \geq 1$ s.t. $\pi^i \models \psi$ and $\pi^1 \models \varphi, \pi^2 \models \varphi, \ldots, \pi^{i-1} \models \varphi$ $OR$ for every $k \geq 1 \pi^k \models \psi$
13. $\pi_i \models \varphi \quad R \quad \psi$ iff $EITHER$ there is $i \geq 1$ s.t. $\pi^i \models \varphi$ and $\pi^1 \models \psi, \pi^2 \models \psi, \ldots, \pi^i \models \psi$ $OR$ for every $k \geq 1 \pi^k \models \psi$

**Rules 8, 9, and 10 are unary temporal connectives while rules 11, 12, and 13 are binary connectives.

### 3.3 Examples of semantics

Using semantic rule 3 from our example graph and path $A\ B\ A\ B\ C\ C\ C\ C\ A$:

- Does $\pi \models p$? **NO** (because our initial state $A$ contains atoms $q, r$ and not $p$)
- Does $\pi \models q$? **YES**
- Does $\pi \models \neg p$? **YES**

Binary temporal connectives are more complicated.

**Picture of $\varphi \quad U \quad \psi$:**

<table>
<thead>
<tr>
<th>$\neg \psi$</th>
<th>$\neg \psi$</th>
<th>$\neg \psi$</th>
<th>$\psi$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
</tr>
</tbody>
</table>
| $\varphi$   | $\varphi$   | $\varphi$   | $\varphi \quad must$ be true until $\psi$ is true. ($\varphi$ could continue to be true but there is no obligation for it to be true once $\psi$ is true).

For $\varphi \quad W \quad \psi$, either $U$ or $\varphi$ is always true.

**Picture of $\varphi \quad R \quad \psi$:**

<table>
<thead>
<tr>
<th>$\varphi$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
</tr>
</tbody>
</table>
| $\psi$    | $\psi$    | $\psi$    | $\psi \quad must$ be true up to and including when $\varphi$ is true or $\psi$ is always true.

**LTL has been so successful because of improvements in efficiency. This is similar to how improvements have been made in propositional logic to be able to efficiently determine satisfiability in some cases.**
4 Extending properties

We can extend the satisfaction of a WFF $\varphi$ to a state $s \in S$ rather than simply a path $\pi$. We will write $M, s \models \varphi$ or $s \models \varphi$ is $M$ is clear from the context iff for every path $\pi$ that starts at state $s$ we have $\pi \models \varphi$.

See Handout 18 starting at page 22 for examples of practical patterns of specifications with LTL.

4.1 Duality

The duality of LTL (i.e. $\neg G \varphi = F \neg \varphi$ etc) should remind you of the duality of first order logic with $\exists$ and $\forall$. (see page 45 in handout 18 for more examples of duality).

4.2 Distributivity

- $X$ is distributive over $\{\land, \lor, U\}$
- $F$ is distributive over $\lor$ and not $\land$
- $G$ is distributive over $\land$ and not $\lor$

5 Conclusion

Class concluded early due to graded midterm exams being handed out.