3. Temporal Logic and Model Checking

Kenneth L. McMillan

1. Reactive Systems and Temporal Properties

1.1 Example: The alternating bit protocol

This is an example of a “reactive” system [1] (Pnueli):
- Reacts to stimulus from environment.
- Does not terminate.

Note each component (sender, receiver, channels) is also a reactive system.

1.2 Temporal properties

To reason about reactive systems and the interaction of their components, we need to be able to state temporal properties.

Example: For the alternating bit protocol:
- Every message sent is eventually received.
- A message is not received unless one is sent
- If x is sent before y, then x is received before y.

Some properties of the components:
- Sender continues to resend msg until ack.
- If channel continues to receive input, it eventually transmits (does not drop) a msg.
- Recvr does not produce ack before msg is output.
- etc.

Note: these are properties about relationships in time (i.e., temporal properties).
1.3 Formalizing temporal properties

... to specify and reason about reactive systems.

- Consider using first order logic to write temporal properties, representing time by a natural number t.
  For example: “every time an x msg is input, one is eventually output”

\[ \forall t \geq 0 : \text{input}(x, t) \Rightarrow \exists t' \geq t : \text{output}(x, t') \]

This is adequate, but a bit hard to read!

- Temporal Logic

Pnueli suggested using temporal logic to express properties of reactive systems. In temporal logic, the time parameter t is implicit:

- \( G p \) true at time t if p is true at all \( t' \geq t \).

- \( F p \) true at time t if p is true at some \( t' \geq t \).

Note, \( G \) and \( F \) are dual:

\[ G p \equiv \neg F \neg p \]
\[ F p \equiv \neg G \neg p \]

Here are, for example, some other equivalences:

\[ Gp \land Gq \equiv G(p \lor q) \]
\[ Fp \lor Fp \equiv F(p \land q) \]

But note,

\[ Gp \lor Gq \not\equiv G(p \land q) \]
\[ Fp \land Fp \not\equiv F(p \lor q) \]

Our previous example in temporal logic:

\[ G(\text{input}(x) \Rightarrow F \text{ output}(x)) \]

This can be read “always, if input(x) then eventually output(x)” It is an example of a liveness property, since it states some “good” condition that must eventually occur.

- “Infinitely often” properties

- Note \( G F p \) means that p occurs infinitely often (“always eventually p”).
  This is equivalent by De Morgan’s laws to \( \neg F G \neg p \) or “a point is never reached where p is forever false”.