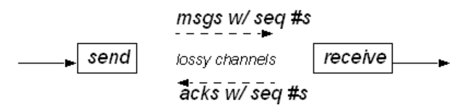
Reactive Systems and Temporal Properties

Sérgio Campos

Reactive Systems

Example: the alternating bit protocol



- Channels may drop (or duplicate) messages.
- Sender retransmits until matching ack received.
- Sequence numbers prevent duplication of msgs.
- Sequ. numbers are modulo 2 ("alternating bit").

This is an example of a *reactive* system (Pnueli):

- "Reacts" to stimulus from environment.
- Does not terminate.

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

Temporal properties

To reason about reactive systems we need to be able to state temporal properties.

E.g., 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 ack before msg is output.

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

Formalizing Temporal Properties

Consider using 1st order logic to write temporal properties, representing time by a natural number t.
"Every time an x msg is input, one is eventually output"

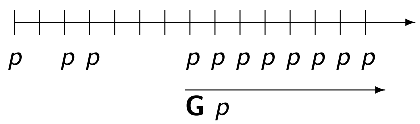
$$\forall t > 0 : \mathrm{input}(x, t) \rightarrow \exists t' \geq t : \mathrm{output}(x, t')$$

- This is adequate, but a bit hard to read!

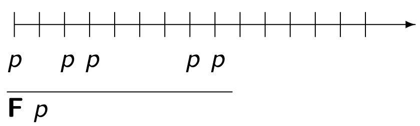
Temporal Logic

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 $t' \geq t$.



Temporal Logic

Note, **G** and **F** are dual:

$$\mathbf{G}\,p \equiv \neg\,\mathbf{F}\,\neg p$$
$$\mathbf{F}\,p \equiv \neg\,\mathbf{G}\,\neg p$$

Here are, for example, some other equivalences:

$$\mathbf{G}\,p \wedge \mathbf{G}\,q \equiv \mathbf{G}(p \wedge q)$$
$$\mathbf{F}\,p \vee \mathbf{F}\,q \equiv \mathbf{F}(p \vee q)$$

But note,

$$\mathbf{G}\,p \vee \mathbf{G}\,q \not\equiv \mathbf{G}(p \vee q)$$
$$\mathbf{F}\,p \wedge \mathbf{F}\,q \not\equiv \mathbf{F}(p \wedge q)$$

Temporal Logic

Our previous example in temporal logic:

$$\mathbf{G}(\mathrm{input}(x) \rightarrow \mathbf{F}\,\mathrm{output}(x))$$

"It is always that, if input(x) then eventually output(x)"

This is an example of a liveness property, since it states some "good" condition that must eventually occur.

Temporal Logic

"Infinitely often" properties:

- $\mathbf{G}\,\mathbf{F}\,p$ means that p occurs infinitely often ("always eventually p").

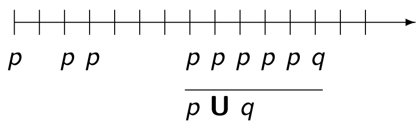
  Equivalent by De Morgans laws to $\neg\,\mathbf{F}\,\mathbf{G}\,\neg p$ or "a point is never reached where p is forever false".

Example: $\mathbf{G}\,\mathbf{F}\,\mathrm{send}(x) \rightarrow \mathbf{G}\,\mathbf{F}\,\mathrm{recv}(x)$ "If x is sent infinitely often, it is received infinitely often". This is an example of a *fairness* property.

Temporal Logic

The *until* operator: $p\,\mathbf{U}\,q$ is true at time t if

- q is true at some $t' \geq t$, and
- p is true in the range $[t, t')$



This can be read as "q is eventually true, and until that time p remains true."

Temporal Logic

The *weak until*: $p\,\mathbf{W}\,q \equiv p\,\mathbf{U}\,q \vee \mathbf{G}\,p$

- It allows the possibility that q never happens and p remains true forever.
- This is useful for expressing properties like:

$$\neg\mathrm{output}(x)\,\mathbf{W}\,\mathrm{input}(x)$$

"An output does not occur before an input occurs."

Example of a safety property. It states some "bad" condition that should never occur.

Temporal Logic

The formal distinction between safety and liveness is the following:

- A safety property, if false, can always be proved false by exhibiting a finite run.
- A liveness property can only be proved false by exhibiting an infinite run – any finite run can be extended so that it satisfies the eventuality condition.

Temporal Logic

Some other temporal operators:

- The *next time* operator: $\mathbf{X}\,p$ is true at time t if p is true at time $t+1$.
- Past time operators: **H**, **P** and **S** are past time versions of **G**, **F** and **U** respectively.