Temporal Specification

Michael Fisher

Department of Computer Science, University of Liverpool, UK

[MFisher@liverpool.ac.uk]
Exercises

We will now look at three simple scenarios showing concurrent, communicating elements.

Three scenarios are:

1. A **simple auction** system where three ‘bidder’ elements send ‘bids’ to an ‘auctioneer’ element, which chooses the highest bid.

2. A **variation** on the bidding system above where one of the bidders can lend money to another to allow a successful bid.

3. A **ring network** where activity is passed around the ring.
Simple Auction

- one ‘auctioneer’ element
  - key behaviour is to collect bids using the ‘bidded’ predicate. e.g. \(\text{bidded}(b_1, 5)\) means that auctioneer has received a bid of 5 from bidder \(b_1\).
  - Auctioneer decides between bids, e.g.
    
    \[
    \begin{array}{c}
    \{ \text{bidded}(b_1, X) \land \text{bidded}(b_2, Y) \land \\
    \text{bidded}(b_3, Z) \land (X \leq Y) \land (Y \leq Z) \} \Rightarrow \Box \text{awarded}(b_3) \\
    \end{array}
    \]

- three ‘bidder’ elements, each of which bids a fixed number at every moment in time:
  - \(b_1\) always bids 7
  - \(b_2\) always bids 5
  - \(b_3\) always bids 3
Specify (1) and (2) below.

1. Write out temporal specifications for each of the ‘bidder’ elements. Within each element, just use the predicate ‘bid’, where

\[ \text{bid}(C, V) \]

means that element \( C \) bids value \( V \).
2. Write out a few of the elements of a temporal specification for the auctioneer element, based on the predicates ‘\textit{bidded}’ and ‘\textit{awarded}’, where

\[
bidded(C, V)\]

means that the auctioneer received a bid of value \(V\) from element \(C\), and

\[
awarded(C)\]

means that the auction is won by element \(C\).
Then:

3. Write out temporal specifications for the ‘comms’ formulae between each element, i.e.
   \[\text{Comms}(\text{auctioneer}, b_1), \text{Comms}(\text{auctioneer}, b_2), \text{and} \]
   \[\text{Comms}(\text{auctioneer}, b_3).\]

**Note** that we can verify

\[\Box (\text{awarded}(b_1) \land \neg \text{awarded}(b_2) \land \neg \text{awarded}(b_3))\]
4. Modify the specification so that $b_3$ and $b_2$ communicate.

In particular, $\text{borrow}\ ?$ in $b_2$ is linked to $\text{lend}\ ?$ in $b_3$, and $\text{borrowed}(V)$ in $b_2$ is linked to $\text{lent}(V)$ in $b_3$ (where $V$ is a value).

5. $b_2$ normally bids 5 as before but at some point in the future asks to borrow money from $b_3$.

If $b_3$ later agrees to this, $b_2$ makes a bid that is the sum of the ‘borrowed’ amount and ‘5’.

$b_3$, when it receives $b_2$’s request will, at some point in the future, agree to this and lend 3 to $b_2$

Write out the modified specificaitions for the above.
Ring Network

Three elements: *larry*, *curly* and *mo*.

Each element has communications, but only in the direction specified by

\[ larry \rightarrow curly \rightarrow mo \rightarrow larry \]

Each element is guarding *something*. It guards for an arbitrary length of time, then communicates to the next element to take over guarding.

Key property of communication is that messages take one time step to arrive at their destination.

The property we wish to verify of the whole system is that, throughout the whole of execution, either *larry* is guarding, *curly* is guarding or *mo* is guarding.
Sample Answers
1. Bidder Components

\[
\begin{align*}
\text{Spec}_{b1} & : \quad \start \Rightarrow bid(b1, 7) \\
& \quad \land \quad \text{true} \Rightarrow \Diamond bid(b1, 7)
\end{align*}
\]

\[
\begin{align*}
\text{Spec}_{b2} & : \quad \start \Rightarrow bid(b2, 5) \\
& \quad \land \quad \text{true} \Rightarrow \Diamond bid(b2, 5)
\end{align*}
\]

\[
\begin{align*}
\text{Spec}_{b3} & : \quad \start \Rightarrow bid(b3, 3) \\
& \quad \land \quad \text{true} \Rightarrow \Diamond bid(b3, 3)
\end{align*}
\]
2. Auctioneer Component

Sample $Spec_{auc}$ formulae:

\[
\begin{align*}
\text{bidded}(b1, X) \land \text{bidded}(b2, Y) \land \text{bidded}(b3, Z) \land (X \leq Y) \land (Y \leq Z) \\
\Rightarrow \quad \text{awarded}(b3) \\
\text{bidded}(b1, X) \land \text{bidded}(b2, Y) \land \text{bidded}(b3, Z) \land (X \leq Y) \land (Y > Z) \\
\Rightarrow \quad \text{awarded}(b2) \land \neg \text{awarded}(b3) \\
\text{bidded}(b1, X) \land \text{bidded}(b2, Y) \land \text{bidded}(b3, Z) \land (X > Y) \land (X > Z) \\
\Rightarrow \quad \text{awarded}(b1) \land \neg \text{awarded}(b2) \land \neg \text{awarded}(b3)
\end{align*}
\]

And so on.
3. Auction Communications

Typically, \( \text{Comms}(\text{auc, } b_1) = \]

\[
\square \left[ \begin{array}{c}
\text{bid}(b_1, V) \Rightarrow \bigcirc \text{bidded}(b_1, V)
\end{array} \right]
\]
4. Coalition Communications

\[
Comms(b_2, b_3) =
\]

\[
\square \left[ \begin{array}{c}
\text{borrow?} \Rightarrow \bigcirc \text{lend?} \\
\land \quad \text{lent}(V) \Rightarrow \bigcirc \text{borrowed}(V)
\end{array} \right]
\]
5. Coalition Specifications

$Spec_{b2}$:

\[
\begin{bmatrix}
\text{start} & \Rightarrow & \text{bid}(b2, 5) \\
\land & \neg \text{borrowed}(V) & \Rightarrow & \lozenge \text{bid}(b2, 5) \\
\land & \text{borrowed}(V) & \Rightarrow & \lozenge \text{bid}(b2, V + 5) \\
\land & \text{true} & \Rightarrow & \lozenge \text{borrow}\
\end{bmatrix}
\]

$Spec_{b3}$:

\[
\begin{bmatrix}
\text{start} & \Rightarrow & \text{bid}(b3, 3) \\
\land & \neg \text{lent}(V) & \Rightarrow & \lozenge \text{bid}(b3, 3) \\
\land & \text{lent}(V) & \Rightarrow & \lozenge \text{bid}(b3, 3 - V) \\
\land & \text{lend}? & \Rightarrow & \lozenge \text{lent}(3)\
\end{bmatrix}
\]
Typical component specification (for \textit{larry}): 

\begin{align*}
\text{start} & \implies \text{larry\_guards} \\
\text{larry\_guards} & \implies \Diamond \neg \text{larry} \\
(\neg \text{not\_larry} \land \text{larry\_guards}) & \implies \lozenge \text{larry\_guards} \\
(\neg \text{not\_larry} \land \text{larry\_guards}) & \implies \lozenge \neg \text{larry\_guards} \\
(\neg \text{is\_larry} \land \neg \text{larry\_guards}) & \implies \lozenge \neg \text{larry\_guards} \\
(\text{is\_larry} \land \neg \text{larry\_guards}) & \implies \lozenge \text{larry\_guards}
\end{align*}
6. Ring Network (2)

\[ \text{Comms}(\text{larry, curly}) = \text{not}_\text{larry} \Rightarrow \Box \text{is}_\text{curly} \]
\[ \text{Comms}(\text{curly, mo}) = \text{not}_\text{curly} \Rightarrow \Box \text{is}_\text{mo} \]
\[ \text{Comms}(\text{mo, larry}) = \text{not}_\text{mo} \Rightarrow \Box \text{is}_\text{larry} \]

Verification of

\[ \Box (\text{larry\_guards} \lor \text{curly\_guards} \lor \text{mo\_guards}) \]