Abstract State Machines

Verification and Final Thoughts

Verification of ASM

Three methods:

1. Reviews
2. Testing
3. Formal Proofs

Review of ASMs

- Similar to code reviews
- Natural to the system
- Knowledge base

Testing ASMs

- ASMs can be executed
  - AsmL
  - XASM
- Testing is performed earlier

Formal Proofs of ASMs

- ASMs are a Formal Description
- Verification of ASMs

Example

Prove the definition of Kruskal's algorithm for finding a minimum spanning tree terminates.

```
if CurrentMode = initial then
    do-forall p: Node
        Label(p) := p
    enddo
    CurrentMode := run
elseif CurrentMode = run then
    choose e: Edge: Eligible(e) and ((∀f: Edge) Eligible(f) ⇒ Weight(f) ≥ Weight(e))
        Tree(e) := true
        choose p, q: Node: {p, q} = Endpoints(e)
            do-forall r: Node: Label(r) = Label(p)
                Label(r) := Label(q)
            enddo
        endchoose
    ifnone CurrentMode := done
    endchoose
endif
```

From "An Abstract State Machine Primer" by J, K. Higgins and C. Wallace

Example: Kruskal's

- Prove the algorithm finds a spanning tree
  - Graph of *n* nodes
  - Algorithm creates edges between nodes
- Termination:
  - All nodes with the same label
  - *n - 1* edges

Example: Kruskal's

- At each state:
  - Label $\rightarrow p$
  - Set of nodes labelled $p \rightarrow L_p$
  - Number of nodes in $L_p \rightarrow n_p$
  - Edges connected to nodes in $L_p \rightarrow t_p$
- Each set of nodes in a non-empty L_p
  - $t_p = n_p - 1$
- Loop until only one non-empty L_p

Example: Kruskal's

- Now prove the claim by induction
- At the first step each node is separately labelled
  - $n_p = 1$
  - $t_p = 0$
  - Claim holds true so far.

Example: Kruskal's

- Edge *e* chosen between two labels
  - (*p* and *q*)
- All nodes labelled *p* are re-labelled *q*
- L'_q is the new set of nodes labelled *q*
  - $t'_q = n_q + n_p - 1$
- The proof holds true
  - L'_p is now empty
  - All other labels remain the same
- Number of non-empty labels decreases by 1

Final Thoughts

- ASMs not limited to software
- Multi-agent ASMs
  - Distributed Systems
  - Real-time Systems