Grand Challenge Applications Panel

Paul Loewenstein

22 February 2005

Outline

- Who am I?
- What do I do?
- How do I do it?
- Summary.

Who am I?

- Paul Loewenstein, Senior Staff Engineer at Sun Microsystems.
- Started being interested in formal methods around 1987 (when at Fairchild Semiconductor).
- Stuck at it through one takeover, one layoff and one resignation to join Sun Microsystems.

What Do I Do?

- Try to ensure correctness of computer hardware at the system architecture level, in particular:
  - Cache Coherence and Sparc memory model ordering.
  - Forward Progress (deadlock and starvation avoidance).
  - Specifying and ensuring correct ordering of I/O and DMA.

How Do I Do it?

- At first used Murphi invariant checker for Cache Coherence.
- Later used HOL, then PVS for verification (key properties of) coherence protocols.
- Conformance to memory model checked by hand by finding existential witness of memory order.
- First forward progress work done with HOL (found deadlock in machine that had been running for six months).
- Later forward progress work done by hand.
- I/O and DMA just getting started.

How Do I Do It?

- Schedule.
- Schedule.
- Deliver on time. Compromise on what is delivered to meet schedule:
  - Develop “Golden” verification model from formally verified model, for simulation of protocol agents.
  - Develop deep understanding so that errors can be found by inspection.
  - Document and communicate forward progress requirements.

Summary

- Use formal proof only when time permits and problem is sufficiently difficult.
- Leads to compromise—we can't yet formally prove everything.
- Insist on at least lines of proof for many properties of design:
  - Memory model, including I/O and DMA.
  - Forward progress—no deadlock or starvation.
  - Sparc execution model.
  - And more.