Prototype Verification System

Remy Viehoff
Overview

- John Rushby, Sam Owre & Natarajan Shankar from SRI international (US)
- Inspired by LCF, HOL and Nqthm
- Implemented in common lisp
- First version in 1993, current version 5.0 (2011)
Interactive theorem prover with powerful commands and user-definable strategies (collection of commands)

Based on classical higher order logic

Rich type system with e.g. predicate subtypes:
\{ f : [real \to real] \mid \text{injective?}(f) \}\n
A lot of automation

Emacs front-end
Primary application domain

- Not one specific domain, works for all kinds of applications e.g:
- Verification of AAMP5 microprocessor: M. Srivas & S. Miller
- Mifare card security broken: B. Jacobs
- Various NASA applications e.g. collision avoidance, fault-tolerance, clock synchronization
• Has its own PVS library: ± 115 MB of (mostly) mathematics
• Includes things like floating point arithmetic, real analysis, probability etc.
• Freely available
Tools

- Why (software verification platform) has PVS as a back-end prover
- LOOP-tool for java verification by B. Jacobs & E. Poll
- InVeSt for the verification of invariants by S. Bensalem, Y. Lakhnech & S. Owre
- TLPVS, a PVS based LTL verification system by A. Pnueli & T. Arons
Demo
References

- http://pvs.csl.sri.com/
- http://en.wikipedia.org/wiki/Prototype_Verification_System