Proof by Verified Symbolic Execution in ACL2

Sol Swords
sswords@cs.utexas.edu

May 9, 2009
Recall Boyer and Hunt’s G system:

- Symbolic functions in raw Lisp
- Symbolic data objects are in raw Lisp, unrepresentable in ACL2
- Usable for proof with unverified clause processor

G in the Logic, or “GL”:

- Symbolic functions are in the ACL2 logic
- Symbolic objects are a subset of ACL2 objects
- Automatically-proven theorems about the system allow proof without trusting anything but ACL2 itself
The GL System

Code transform produces symbolic simulator $P_{sym}$ given program $P$

Symbolic object semantics defined by evaluator $ev_s$

Correspondence proof automatically generated for $P_{sym}$

$env = \{A_2 = 1, A_1 = 0, A_0 = 1\}$