ACL2 2009: Eighth International Workshop on the ACL2 Theorem Prover and Its Applications

Sandip Ray

May 20, 2009

The ACL2 workshops provide the key technical forum for researchers to present and discuss improvements to the theorem prover, comparisons of ACL2 with other systems, and applications of ACL2 in formal verification. ACL2, co-authored by Matt Kaufmann and J Moore, is a state-of-the-art automated reasoning system that has been used in academia, government, and industry. ACL2 2009 was held in Boston, MA, USA, on May 11-12, 2009.

The presentations in ACL2 2009 involved (1) implementations and utilities to extend the reach of ACL2, (2) application of ACL2 to different domains, and (3) pedagogical applications and user interfaces. In addition to regular papers, ACL2 2009 included an invited keynote, a panel discussion, and "rump sessions" discussing on-going research.

Sumners presented a user-controllable term simplifier, and discussed the role of user control and extensibility in its design; Moore presented a hint mechanism for automatic functional instantiation through an adaptation of Huet-Lang's pattern matching algorithm; Kaufmann presented a new facility for printing large terms in the theorem prover and provided glimpses of what goes on in the design of a new feature; Hunt discussed a new symbolic simulation technique and its application; Liu discussed a specific approach, based on a syntactic term-manipulation capability, to automatically discharge a certain type of linear inequality proofs; Greve discussed two utilities, (1) for automating proofs of formulas involving first-order quantification, and (2) for introducing arbitrary recursive definitional axioms in ACL2 with an added hypothesis that the recursion terminates where the added hypothesis permits the introduction of a (conditional) definitional axiom and associated induction scheme while not requiring a possibly difficult proof of termination.

Schmaltz and his students presented progress on verification of communication models for network-on-chips; Ralston discussed a proof of AVL tree implementation; Gamboa and Cowles gave two talks, *e.g.*, (1) a formalization of inverse functions in ACL2(R) (the extension of ACL2 supporting real numbers) , and (2) a formal proof of a number-theoretic result that determines which triangular numbers are perfect squares; Kaufmann, Kornerup, and Reitblatt discussed the use of ACL2 in National Instruments to verify LabVIEW programs; Hardin discussed verification of security-critical data structures; Pierre

and her students discussed the use of ACL2 in the verification of fault-tolerance properties of systems; Rager presented a formal proof of security protocol JFKr.

Page discussed his experience introducing computational logic in the undergraduate curriculum; Eastlund discussed *doublecheck*, a framework for testing ACL2 conjectures; Eastlund and Felleisen presented an approach to verify graphical user interfaces; Lozano and his colleagues presented a tool based on XML to render ACL2 output in more accessible format.

The keynote lecture by Barrett outlined recent progresses in SMT solving and discussed how theorem proving and SMT might benefit from each other.

The panel topic was "What is the Future of Theorem Proving?". Panelists argued that while interactive theorem proving is here to stay, for the technology to be pervasive it is critical to integrate it into the design flow as a debugging aid rather than as an activity performed post-facto.