ACL2 Support for Interactive Proof

Matt Kaufmann
The University of Texas at Austin
Dept. of Computer Science

Chalmers, August 10, 2015
OUTLINE

Introduction

Background

Demos (I)

Rewriting in ACL2

Demos (II)

Very Brief Survey of ACL2 Features

Conclusion
Quoting the **ACL2 home page**:

> ACL2 is a logic and programming language in which you can model computer systems, together with a tool to help you prove properties of those models. “ACL2” denotes ”A Computational Logic for Applicative Common Lisp”.

**Goal for this talk:** Give a sense of the ACL2 system, especially how it supports **user interaction**.

**Confession:** there is considerable overlap with KeY invited talk given last month.

But I may skip some material. I hope to leave lots of time for discussion. **Please ask questions** during the talk!
OUTLINE

Introduction

Background

Demos (I)

Rewriting in ACL2

Demos (II)

Very Brief Survey of ACL2 Features

Conclusion
BACKGROUND: OVERVIEW

- ACL2 is freely available, including libraries of certifiable books, from the ACL2 home page.
- ACL2 is written mostly in itself (!).
  - About 10 MB of source code (Version 7.1).
- Bleeding edge for libraries (community books) and the ACL2 system are available from Github.
  - Well over 400,000 events (theorems, definitions, other) are evaluated in the community books.
BACKGROUND: OVERVIEW (CONTINUED)

Development history:


- Boyer-Moore Theorem Provers go back to the start of their collaboration in 1971.

Industrial usage: As far as I know, ACL2 is the only interactive theorem prover (ITP) used with some regularity at several companies:

- AMD, Centaur, IBM, Intel, Oracle, Rockwell Collins

There are also users in the U.S. Government and universities, including —

- UT Austin: x86 interpreter defined in ACL2, validation by co-simulation, proofs about x86 machine code
**BACKGROUND: Logic**

The ACL2 logic is a first-order logic with induction up to $\varepsilon_0$.

But all ACL2 theories extend a given ground-zero theory, which axiomizes data types for:

- numbers (complex rationals), characters, strings, symbols;
- trees and lists, using a pairing operation (\texttt{cons}).

ACL2 extensions are conservative (a demo will discuss this).

BACKGROUND: STRENGTHS

- Proof automation
- Support for user interaction
- Fast execution
- Documentation (about 100,000 lines for just the system)
- Interfaces include Emacs (Is that really an interface? A strength?) and the Eclipse-based ACL2 Sedan.

A potential weakness: first-order logic with only basic quantifier support (but recursion helps).
BACKGROUND: MORE INFORMATION

NOTE: A longer variant of this talk, but targeted to CS grad students and with more focus on using ACL2, is here:


That talk mentions this link to several demos and their logs:

BACKGROUND: HIGHER-ORDER LOGIC?

Bob Boyer and I did some work in the mid-1980s on adapting the Boyer-Moore prover to the programming language, SASL, which is a weakly typed ancestor of Haskell.

Our work is described at some length in a Burroughs Technical Report, and is summarized briefly here:


Not included above is a larger example (a SASL unification program).
OUTLINE

Introduction

Background

Demos (I)

Rewriting in ACL2

Demos (II)

Very Brief Survey of ACL2 Features

Conclusion
DEMOS (I)

- All demos today, with logs, are available from this link to a gzipped tarfile demos.tgz.

- ACL2 programming and evaluation
  [DEMO]: file demo-1.lsp
  (log demo-1-log.txt)

- ACL2 as an automatic theorem prover
  [DEMO]: file demo-2.lsp
  (log demo-2-log.txt)
  - ACL2 provides automation for induction, linear arithmetic, Boolean reasoning, rule application, …
  - … but lemmas are usually needed (sometimes from libraries).
Demos (I) (continued)

ACL2 supports formally verified extensions.

In particular, GL is a verified clause processor defined and verified by an ACL2 user, Sol Swords. GL does proofs about finite domains by bit-blasting.

The next demo illustrates GL. It also shows the use of LOCAL, for “private” events (using conservativity).

[DEMO]: book demo-gl.lisp
(log demo-gl-log.txt)
OUTLINE

Introduction

Background

Demos (I)

Rewriting in ACL2

Demos (II)

Very Brief Survey of ACL2 Features

Conclusion
Outline

Introduction

Background

Demos (I)

Rewriting in ACL2

Demos (II)

Very Brief Survey of ACL2 Features

Conclusion
**Rewriting in ACL2**

ACL2 is typically controlled with conditional rewrite rules, although there are other rule-classes too.

The basic idea: the ACL2 rewriter automatically applies the rule

\[ H \rightarrow L = R \]

by replacing an instance \( L/s \) of \( L \) by \( R/s \), when the rewriter can verify \( H/s \).

The documentation topic for rewrite shows many ways to control the rewriter (needed only occasionally). I’ll mention only a few:
REWITING IN ACL2 (2)

- **backchain-limit**: limit effort to relieve hypotheses
- **force**: defer proving $H$ if necessary
- **hide**: hide a term from the rewriter
- **syntaxp**: attach a heuristic filter on a rule

Example of **syntaxp**: consider $3 + (4 + x)$.
It’s already in normal form: right-associated.
Our wish: $3 + (4 + x) = (3 + 4) + x = 7 + x$.

ACL2 !>:pe associativity-of-+
-997  (DEFAXIOM ASSOCIATIVITY-OF-+
  (EQUAL (+ (+ X Y) Z) (+ X (+ Y Z))))

ACL2 !>:pe fold-consts-in-+
-158  (DEFTHM FOLD-CONSTS-IN-+
  (IMPLIES (AND (SYNTAXP (QUOTEP X))
               (SYNTAXP (QUOTEP Y)))
           (EQUAL (+ X (+ Y Z)) (+ (+ X Y) Z))))
Rewriting in ACL2 (3)

\[ H \rightarrow L = R \quad \text{(ordinary rewrite rule)} \]

\[ H \rightarrow L \sim R \quad \text{(congruence-based rewrite rule)} \]

where \( \sim \) is an equivalence relation.

Users prove equivalence, congruence, and refinement rules, to tell ACL2 when such rewrites are valid.


OUTLINE

Introduction

Background

Demos (I)

Rewriting in ACL2

Demos (II)

Very Brief Survey of ACL2 Features

Conclusion
OUTLINE

Introduction

Background

Demos (I)

Rewriting in ACL2

Demos (II)

Very Brief Survey of ACL2 Features

Conclusion
Demos (II)

Our final demo shows how ACL2 proof development often follows “the method”:

- ACL2 heuristically chooses and applies a destructor-style induction scheme.
- ACL2 simplifies the base and induction steps.
- The user looks at key checkpoints, which are unproved goals printed by ACL2.
- The user formulates conditional rewrite rules to simplify those checkpoints.
- Repeat.
Quoting the documentation for induction:

... the interested reader should see Chapter XIV of A Computational Logic (Boyer and Moore, Academic Press, 1979) which represents a fairly complete description of the induction heuristics of ACL2.

This demo should give a sense of how ACL2 chooses (and applies) induction schemes, but the focus will be on user interaction.

— DEMO (excerpted from my TPHOLs 2008 talk) —
OUTLINE

Introduction

Background

Demos (I)

Rewriting in ACL2

Demos (II)

Very Brief Survey of ACL2 Features

Conclusion
Very Brief Survey of ACL2 Features

Let’s see a bit more about how ACL2 supports proof development . . .

▶ . . . by exploring briefly the ACL2 documentation.

NOTE:
I would be very happy to elaborate on any of these topics!
In particular, we might explore a few debugging features, as time and interest permit.

- accumulated-persistence
- break-rewrite
- cgen
- cw-gstack
- disassemble$
- dmr
- failed-forcing
- failure
- find-lemmas
- forward-chaining-reports
- guard-debug
- measure-debug
- nil-goal
- print-gv
- profile-acl2
- profile-all
- proof-checker
- proof-tree
- pstack
- quick-and-dirty-subsumption-replacement-step
- redo-flat
- remove-hyps
- set-debugger-enable
- set-guard-msg
- sneaky
- spacewalk
- splitter
- time-tracker
- trace
- walkabout
- watch
OUTLINE

Introduction

Background

Demos (I)

Rewriting in ACL2

Demos (II)

Very Brief Survey of ACL2 Features

Conclusion
OUTLINE

Introduction

Background

Demos (I)

Rewriting in ACL2

Demos (II)

Very Brief Survey of ACL2 Features

Conclusion
CONCLUSION

- ACL2 has a 25 (or 44) year history and is used in industry.
  
  "Microprocessor design goes daily through numerous optimizations that affect thousands of lines of code. These optimizations must be proved correct."

  — Anna Slobodova, verification manager at Centaur Technology

- ACL2 provides automation but scales to large problems . . . .
  . . . with libraries and by supporting user interaction.

- For more information, see the ACL2 home page.

THANK YOU!