ACL2: Implementation of a Computational Logic

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

June 10, 2015
HELLO!
HELLO!

I’m so happy to be visiting here! I plan to be in Gothenburg until August 15.
HELLO!

I’m so happy to be visiting here! I plan to be in Gothenburg until August 15. *Thanks, Ali!*
HELLO!

I’m so happy to be visiting here! I plan to be in Gothenburg until August 15. *Thanks, Ali!*

Today I’ll discuss a logic and software tool, ACL2, which has been my focus off and on since the early 1990s.
HELLO!

I’m so happy to be visiting here! I plan to be in Gothenburg until August 15. *Thanks, Ali!*

Today I’ll discuss a logic and software tool, ACL2, which has been my focus off and on since the early 1990s.

(But my intention in Gothenburg is to return to my roots in model theory, especially models of set theory and arithmetic.)
OUTLINE

Overview

ACL2 Introduction

Logical Foundations

Conclusion
<table>
<thead>
<tr>
<th>Outline</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overview</td>
</tr>
<tr>
<td>ACL2 Introduction</td>
</tr>
<tr>
<td>Logical Foundations</td>
</tr>
<tr>
<td>Conclusion</td>
</tr>
</tbody>
</table>
OVERVIEW

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:
▶ The focus will be on mechanizing logic for a practical proof assistant.
▶ Boring or not, logical challenges must be addressed! (Note: ACL2 does not generate formal proofs.)
OVERVIEW

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".*
OVERVIEW

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:**
Say something about ACL2 of interest to logicians.
OVERVIEW

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:
Say something about ACL2 of interest to logicians.

- The focus will be on mechanizing logic for a practical proof assistant.
OVERVIEW

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:
Say something about ACL2 of interest to logicians.

- The focus will be on mechanizing logic for a practical proof assistant.
- Boring or not, logical challenges must be addressed!
Overview

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:
Say something about ACL2 of interest to logicians.

- The focus will be on mechanizing logic for a practical proof assistant.
- Boring or not, logical challenges must be addressed! (Note: ACL2 does not generate formal proofs.)
Overview: The plan for today
OVERVIEW: THE PLAN FOR TODAY

I’ll start by following these slides . . .
OVERVIEW: THE PLAN FOR TODAY

I’ll start by following these slides . . .

. . . but I’d be happy to take us in whatever direction you’d prefer (if I can!).

OVERVIEW: THE PLAN FOR TODAY

I’ll start by following these slides . . .
. . . but I’d be happy to take us in whatever direction you’d prefer (if I can!).

I’ve prepared about an hour’s worth of material, so there should be plenty of time to explore . . .
OVERVIEW: THE PLAN FOR TODAY

I’ll start by following these slides . . .
. . . but I’d be happy to take us in whatever direction you’d prefer (if I can!).

I’ve prepared about an hour’s worth of material, so there should be plenty of time to explore . . .
. . . and of course, I can skip slides.
OVERVIEW: THE PLAN FOR TODAY

I’ll start by following these slides . . .
. . . but I’d be happy to take us in whatever direction you’d prefer (if I can!).

I’ve prepared about an hour’s worth of material, so there should be plenty of time to explore . . .
. . . and of course, I can skip slides.

Please feel free to ask questions!
OVERVIEW: THE PLAN FOR TODAY

I’ll start by following these slides . . .
. . . but I’d be happy to take us in whatever direction you’d prefer (if I can!).

I’ve prepared about an hour’s worth of material, so there should be plenty of time to explore . . .
. . . and of course, I can skip slides.

Please feel free to ask questions!

Let’s start with some context.
Overview: Formal Verification

Many organizations now use tools to formally verify hardware and software systems, augmenting traditional testing by using tools based on some notion of proof. Such tools are typically equivalence checkers, model checkers, or static checkers. But occasionally, interactive theorem provers (ITPs) are used, e.g. Coq, Isabelle, HOL4, PVS, Agda — or ACL2. As far as I know, ACL2 is the only 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:

- UT Austin: x86 interpreter defined in ACL2, validation by co-simulation, proofs about x86 machine code
OVERVIEW: FORMAL VERIFICATION

Many organizations now use tools to *formally verify* hardware and software systems, augmenting traditional *testing* by using tools based on some notion of *proof*. 
**Overview: Formal Verification**

Many organizations now use tools to *formally verify* hardware and software systems, augmenting traditional *testing* by using tools based on some notion of *proof*.

Such tools are typically *equivalence checkers, model checkers, or static checkers*. 
Overview: Formal Verification

Many organizations now use tools to formally verify hardware and software systems, augmenting traditional testing by using tools based on some notion of proof.

Such tools are typically equivalence checkers, model checkers, or static checkers.

But occasionally, interactive theorem provers (ITPs) are used, e.g. Coq, Isabelle, HOL4, PVS, Agda — or ACL2.
OVERVIEW: FORMAL VERIFICATION

Many organizations now use tools to formally verify hardware and software systems, augmenting traditional testing by using tools based on some notion of proof.

Such tools are typically equivalence checkers, model checkers, or static checkers.

But occasionally, interactive theorem provers (ITPs) are used, e.g. Coq, Isabelle, HOL4, PVS, Agda — or ACL2.

As far as I know, ACL2 is the only ITP used with some regularity at several companies:
OVERVIEW: FORMAL VERIFICATION

Many organizations now use tools to *formally verify* hardware and software systems, augmenting traditional *testing* by using tools based on some notion of *proof*.

Such tools are typically *equivalence checkers, model checkers, or static checkers*.

But occasionally, *interactive theorem provers* (ITPs) are used, e.g. Coq, Isabelle, HOL4, PVS, Agda — or *ACL2*.

As far as I know, ACL2 is the only ITP used with some regularity at several companies:

- AMD, Centaur, IBM, Intel, Oracle, Rockwell Collins
OVERVIEW: FORMAL VERIFICATION

Many organizations now use tools to formally verify hardware and software systems, augmenting traditional testing by using tools based on some notion of proof.

Such tools are typically equivalence checkers, model checkers, or static checkers.

But occasionally, interactive theorem provers (ITPs) are used, e.g. Coq, Isabelle, HOL4, PVS, Agda — or ACL2.

As far as I know, ACL2 is the only 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.
Overview: Formal Verification

Many organizations now use tools to formally verify hardware and software systems, augmenting traditional testing by using tools based on some notion of proof.

Such tools are typically equivalence checkers, model checkers, or static checkers.

But occasionally, interactive theorem provers (ITPs) are used, e.g. Coq, Isabelle, HOL4, PVS, Agda — or ACL2.

As far as I know, ACL2 is the only 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.

▶ UT Austin: x86 interpreter defined in ACL2, validation by co-simulation, proofs about x86 machine code
OVERVIEW: INTERACTIVE THEOREM PROVING
**Overview: Interactive Theorem Proving**

- Yearly ITP conference
Overview: Interactive Theorem Proving

- Yearly ITP conference
- Many ITP systems (e.g., ACL2) can send sub-problems to automatic proof tools, e.g., SAT solvers for Boolean problems.
Overview: Interactive Theorem Proving

- Yearly ITP conference
- Many ITP systems (e.g., ACL2) can send sub-problems to automatic proof tools, e.g., SAT solvers for Boolean problems.
- ITP is typically more scalable than automatic theorem proving, but requires some human assistance.
Overview: Interactive Theorem Proving

- Yearly ITP conference
- Many ITP systems (e.g., ACL2) can send sub-problems to automatic proof tools, e.g., SAT solvers for Boolean problems.
- ITP is typically more scalable than automatic theorem proving, but requires some human assistance. For ACL2: prove lemmas used to simplify terms in later proofs.
Overview: Interactive Theorem Proving

- Yearly ITP conference
- Many ITP systems (e.g., ACL2) can send sub-problems to automatic proof tools, e.g., SAT solvers for Boolean problems.
- ITP is typically more scalable than automatic theorem proving, but requires some human assistance. For ACL2: prove lemmas used to simplify terms in later proofs.

Some particular strengths of ACL2 among ITPs:
Overview: Interactive Theorem Proving

- Yearly ITP conference
- Many ITP systems (e.g., ACL2) can send sub-problems to automatic proof tools, e.g., SAT solvers for Boolean problems.
- ITP is typically more scalable than automatic theorem proving, but requires some human assistance. For ACL2: prove lemmas used to simplify terms in later proofs.

Some particular strengths of ACL2 among ITPs:

- Proof automation
OVERVIEW: INTERACTIVE THEOREM PROVING

- Yearly ITP conference
- Many ITP systems (e.g., ACL2) can send sub-problems to automatic proof tools, e.g., SAT solvers for Boolean problems.
- ITP is typically more scalable than automatic theorem proving, but requires some human assistance. For ACL2: prove lemmas used to simplify terms in later proofs.

Some particular strengths of ACL2 among ITPs:
- Proof automation
- Proof debugging utilities
OVERVIEW: INTERACTIVE THEOREM PROVING

- Yearly ITP conference
- Many ITP systems (e.g., ACL2) can send sub-problems to automatic proof tools, e.g., SAT solvers for Boolean problems.
- ITP is typically more scalable than automatic theorem proving, but requires some human assistance. For ACL2: prove lemmas used to simplify terms in later proofs.

Some particular strengths of ACL2 among ITPs:

- Proof automation
- Proof debugging utilities
- Fast execution
OVERVIEW: INTERACTIVE THEOREM PROVING

- Yearly ITP conference
- Many ITP systems (e.g., ACL2) can send sub-problems to automatic proof tools, e.g., SAT solvers for Boolean problems.
- ITP is typically more scalable than automatic theorem proving, but requires some human assistance. For ACL2: prove lemmas used to simplify terms in later proofs.

Some particular strengths of ACL2 among ITPs:

- Proof automation
- Proof debugging utilities
- Fast execution
- Documentation (about 100,000 lines for just the system)
OVERVIEW: ON USING ACL2

This talk will focus on logical aspects of ACL2, so will say rather little about using ACL2.
**Overview: On Using ACL2**

This talk will focus on logical aspects of ACL2, so will say rather little about using ACL2.

**NOTE:** A longer variant of this talk, but oriented towards CS grad students and with more focus on using ACL2, is here:
OVERRIDE: ON USING ACL2

This talk will focus on logical aspects of ACL2, so will say rather little about using ACL2.

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

**OVERVIEW: ON USING ACL2**

This talk will focus on logical aspects of ACL2, so will say rather little about *using* ACL2.

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


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

Overview

ACL2 Introduction

Logical Foundations

Conclusion
OUTLINE

Overview

ACL2 Introduction

Logical Foundations

Conclusion
ACL2 INTRODUCTION

- Freely available, including libraries of *certifiable books*
ACL2 Introduction

- Freely available, including libraries of certifiable books
- Let’s explore the ACL2 home page.
ACL2 INTRODUCTION

- Freely available, including libraries of certifiable books
- Let’s explore the ACL2 home page.
- ACL2 is written mostly in itself (!).
ACL2 Introduction

- Freely available, including libraries of *certifiable books*
- Let’s explore the ACL2 home page.
- ACL2 is written mostly in itself (!).
  - About 10 MB of source code (Version 7.1).
ACL2 Introduction

- Freely available, including libraries of certifiable books
- Let’s explore 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.
ACL2 Introduction

▶ Freely available, including libraries of certifiable books
▶ Let’s explore 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.
ACL2 INTRODUCTION

- Freely available, including libraries of certifiable books
- Let’s explore 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.
ACL2 Introduction

- Freely available, including libraries of certifiable books
- Let’s explore 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.
- History
ACL2 Introduction

- Freely available, including libraries of certifiable books
- Let’s explore 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.

History

ACL2 Introduction

- Freely available, including libraries of certifiable books
- Let’s explore 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.
- History
  - Boyer-Moore Theorem Provers go back to the start of their collaboration in 1971.
ACL2 Demos

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

- 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 DEMOS

- 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, ...
ACL2 Demos

- 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, ...

- The demos above, with logs, are in the gzipped tar file demos-1-and-2.tgz in this directory.
ACL2 Demos

- 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, ...

- The demos above, with logs, are in the gzipped tar file demos-1-and-2.tgz in this directory.

- Interfaces include Emacs, ACL2 Sedan (Eclipse-based), none.
ACL2 Introduction Wrap-Up

ACL2 is a mature system with features *not* discussed today, including:
ACL2 Intro Wrap-Up

ACL2 is a mature system with features *not* discussed today, including:

- Prover algorithms
ACL2 Intro Wrap-Up

ACL2 is a mature system with features *not* discussed today, including:

- Prover algorithms
- Using the prover effectively
ACL2 Intro Wrap-Up

ACL2 is a mature system with features *not* discussed today, including:

- Prover algorithms
- Using the prover effectively
- Programming support
ACL2 Intro Wrap-Up

ACL2 is a mature system with features not discussed today, including:

- Prover algorithms
- Using the prover effectively
- Programming support
- System-level support
ACL2 INTRO WRAP-UP

ACL2 is a mature system with features *not* discussed today, including:

- Prover algorithms
- Using the prover effectively
- Programming support
- System-level support

(We can expand on these topics if there is time and interest.)
PARTIAL TIMELINE

1970
- Boyer and Moore meet
- insertion sort
- binary adder
- prime factorization
- BDX930 abandoned
- RSA
- unsolvability of halting problem

1975
- FM8502
- Gödel
- FM9001
- micro Gypsy compiler
- Byzantine Generals

1980
- Piton
- Gauss
- Unity
- FM8501
- Paris-Harrington Ramsey
- Motorola CAP
- Dijkstra shortest path

1985
- X86 ISA
- FM8502
- Y86 with STOBJ
- Galois/Rockwell SHADE

1990
- real-time model
- clock sync
- biphase mark
- FM9001
- Nqthm compiler
- Kalman filters
- Mostra CAP
- fast consensus analysis

1995
- IBM floating point algorithms
- x86 ring model/proof
- initial ACL2 workshop
- AMD floating-point rtl, ongoing
- Logic formalization (Spain), ongoing

2000
- AMD K5 floating-point division
- µcode
- Logic formalization (Spain)

2005
- Y86
- sixth ACL2 workshop
- Buyer/seller
- Rockwell Greenhills OS

2010
- ACM Software System Award
- UCLID integration prototype

2015
- X86 ISA
OUTLINE

Overview

ACL2 Introduction

Logical Foundations

Conclusion
The ACL2 logic is a first-order logic with induction up to $\varepsilon_0$. 
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 is essentially Peano Arithmetic with $\varepsilon_0$-induction, extended with data types for:
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 is essentially Peano Arithmetic with $\varepsilon_0$-induction, extended with data types for:

- characters,
- strings,
- symbols,
- complex numbers with rational coefficients, and
- closure under a pairing operation (\texttt{cons}).
Logical Foundations (2)

Evolving theories: conservative extensions
Evolving theories: **conservative extensions**

- Suppose theory $T_1$ extends theory $T_0$. Then $T_1$ is a *conservative extension* of theory $T_0$ if every theorem of $T_1$ in the language of $T_0$ is a theorem of $T_0$.  

ACL2 extensions are conservative... even with recursive definitions, since "termination" must be provable.


Importance: One may want to introduce new concepts to carry out some proofs, but this must be done conservatively in order to believe the results.
Evolving theories: **conservative extensions**

- Suppose theory $T_1$ extends theory $T_0$. Then $T_1$ is a *conservative extension* of theory $T_0$ if every theorem of $T_1$ in the language of $T_0$ is a theorem of $T_0$.
- **ACL2 extensions are conservative** …
Evolving theories: \textit{conservative extensions}

- Suppose theory $T_1$ extends theory $T_0$. Then $T_1$ is a \textit{conservative extension} of theory $T_0$ if every theorem of $T_1$ in the language of $T_0$ is a theorem of $T_0$.
- \textbf{ACL2 extensions are conservative} \ldots
  - \ldots even with recursive definitions, since "termination" must be provable.


Importance: One may want to introduce new concepts to carry out some proofs, but this must be done conservatively in order to believe the results.
Evolving theories: **conservative extensions**

- Suppose theory $T_1$ extends theory $T_0$. Then $T_1$ is a *conservative extension* of theory $T_0$ if every theorem of $T_1$ in the language of $T_0$ is a theorem of $T_0$.
- **ACL2 extensions are conservative** . . .
  - . . . even with recursive definitions, since “termination” must be provable.
Logical Foundations (2)

Evolving theories: conservative extensions

- Suppose theory $T_1$ extends theory $T_0$. Then $T_1$ is a conservative extension of theory $T_0$ if every theorem of $T_1$ in the language of $T_0$ is a theorem of $T_0$.
- ACL2 extensions are conservative . . .
  - . . . even with recursive definitions, since “termination” must be provable.
- Importance: One may want to introduce new concepts to carry out some proofs, but this must be done conservatively in order to believe the results.
**LOGICAL FOUNDATIONS (3)**

Fun example in **ACL2(r)**, a variant of ACL2 that supports the real numbers due to Ruben Gamboa:
Logical Foundations (3)

Fun example in ACL2(r), a variant of ACL2 that supports the real numbers due to Ruben Gamboa:
The Overspill Principle of non-standard analysis.
Fun example in ACL2(r), a variant of ACL2 that supports the real numbers due to Ruben Gamboa:
The Overspill Principle of non-standard analysis.

Informally:
If internal predicate $P(n, x)$ holds for all standard natural numbers $n$, then $P(n, x)$ holds for some non-standard natural number $n$. 
LOGICAL FOUNDATIONS (3)

Fun example in ACL2(r), a variant of ACL2 that supports the real numbers due to Ruben Gamboa:
The Overspill Principle of non-standard analysis.

Informally:
If internal predicate $P(n, x)$ holds for all standard natural numbers $n$, then $P(n, x)$ holds for some non-standard natural number $n$.

▶ overspill.lisp: Nice formalization
Fun example in ACL2(r), a variant of ACL2 that supports the real numbers due to Ruben Gamboa:

The Overspill Principle of non-standard analysis. **Informally:**

If internal predicate $P(n, x)$ holds for all standard natural numbers $n$, then $P(n, x)$ holds for some non-standard natural number $n$.

- **overspill.lisp**: Nice formalization
- **overspill-proof.lisp**: Ugly proof, but **LOCAL** to the main proof, by conservativity
Logical Foundations (3)

Fun example in ACL2(r), a variant of ACL2 that supports the real numbers due to Ruben Gamboa:

The Overspill Principle of non-standard analysis.

Informally:
If internal predicate $P(n, x)$ holds for all standard natural numbers $n$, then $P(n, x)$ holds for some non-standard natural number $n$.

- overspill.lisp: Nice formalization
- overspill-proof.lisp: Ugly proof, but LOCAL to the main proof, by conservativity

NOTE: If there is time and interest, I’ll show how to apply the Overspill Principle in ACL2.
Fun example in ACL2(r), a variant of ACL2 that supports the real numbers due to Ruben Gamboa:
The Overspill Principle of non-standard analysis.

Informally:
If internal predicate $P(n, x)$ holds for all standard natural numbers $n$, then $P(n, x)$ holds for some non-standard natural number $n$.

► overspill.lisp: Nice formalization
► overspill-proof.lisp: Ugly proof, but LOCAL to the main proof, by conservativity

NOTE: If there is time and interest, I’ll show how to apply the Overspill Principle in ACL2.

But for now, let’s just show how LOCAL and conservativity apply: 25 lines in overspill-proof.lisp correspond to 256 lines in overspill-proof.lisp.
Key parts of the book `overspill.lisp`:

```lisp
(local (include-book "overspill-proof"))
(set-enforce-redundancy t)
(defstub overspill-p (n x) t)

(defun overspill-p* (n x)  
  (if (zp n)  
      (overspill-p 0 x)  
      (and (overspill-p n x)  
           (overspill-p* (1- n) x))))

(defchoose overspill-p-witness (n) (x)  
  (or (and (natp n) (standardp n)  
          (not (overspill-p n x)))  
      (and (natp n) (i-large n)  
           (overspill-p* n x))))

(defthm overspill-p-overspill  
  (let ((n (overspill-p-witness x)))  
    (or (and (natp n) (standardp n)  
              (not (overspill-p n x)))  
        (and (natp n) (i-large n)  
              (implies (and (natp m)  
                            (<= m n))  
                        (overspill-p m x))))))

:rule-classes nil)
```
Many “simple” logical issues require care in the implementation. While \texttt{LOCAL} is a great example, there are others.
Many “simple” logical issues require care in the implementation. While \texttt{LOCAL} is a great example, there are others.

We’ll look at just a few on the next slides.
Defattach allows non-conservative extensions. Example:
Defattach allows non-conservative extensions. **Example:**

- **Constraint for “specification” function** \( \text{spec} \): \[
x \in \mathbb{Z} \implies \text{spec}(x) \in \mathbb{Z}
\]
**Defattach (1)**

Defattach allows non-conservative extensions. **Example:**

- **Constraint for “specification” function** `spec`:
  \[ x \in \mathbb{Z} \implies \text{spec}(x) \in \mathbb{Z} \]

- **Define function** `f`:
  \[ f(x, y) = \text{spec}(x + y) \]
Defattach allows non-conservative extensions. Example:

- Constraint for “specification” function $\text{spec}$:
  
  $$ x \in \mathbb{Z} \implies \text{spec}(x) \in \mathbb{Z} $$

- Define function $f$: $f(x, y) = \text{spec}(x + y)$

- Define “implementation function” $\text{impl}$: $\text{impl}(x) = 10 \times x$
Defattach (1)

Defattach allows non-conservative extensions. Example:

- Constraint for “specification” function \( \text{spec} \):
  \[ x \in \mathbb{Z} \implies \text{spec}(x) \in \mathbb{Z} \]

- Define function \( f \): \( f(x, y) = \text{spec}(x + y) \)

- Define “implementation function” \( \text{impl} \): \( \text{impl}(x) = 10 \times x \)

- Attach \( \text{impl} \) to \( \text{spec} \):
  \[ (\text{defattach spec impl}) \]
**Defattach** (1)

*Defattach* allows non-conservative extensions. **Example:**

- **Constraint for** "specification" function \( \text{spec} \):
  \[ x \in \mathbb{Z} \implies \text{spec}(x) \in \mathbb{Z} \]

- **Define** function \( f \): \( f(x, y) = \text{spec}(x + y) \)

- **Define** "implementation function" \( \text{impl} \): \( \text{impl}(x) = 10 \ast x \)

- **Attach** \( \text{impl} \) to \( \text{spec} \):
  
  ```
  (defattach spec impl)
  ```

**Result not provable from axioms for** \( f \) **and** \( \text{spec} \):

ACL2 !> (f 3 4)
**Defattach (1)**

Defattach allows non-conservative extensions. **Example:**

- **Constraint for “specification” function** \( \text{spec} \):
  \[ x \in \mathbb{Z} \implies \text{spec}(x) \in \mathbb{Z} \]
- **Define function** \( f \): \( f(x, y) = \text{spec}(x + y) \)
- **Define “implementation function”** \( \text{impl} \): \( \text{impl}(x) = 10 \times x \)
- **Attach impl to spec:**
  
  ```lisp
  (defattach spec impl)
  ```

**Result not provable from axioms for** \( f \) **and** \( \text{spec} \):

ACL2 !>(f 3 4)
70
ACL2 !>
**DEFATTACH (2)**

Issues to consider:

- Is `local (defattach ...)` supported? **YES**, `local` is supported.
- Then how do we deal with conservativity? Two theories: The current theory for reasoning and a stronger evaluation theory, extended using `defattach`:
  
  ```lisp
  spec (x) = impl (x)
  ```
  
- Ah, but what about this? `(thm (equal (f 3 4) 70))` The proof fails! (Whew!)
- **Why is the evaluation theory consistent?** A key requirement is that the attachment relation is suitably acyclic. For details, including issues pertaining to evaluation, see the Essay on Defattach comment in the ACL2 sources.
DEFATTACH (2)

Issues to consider:

- Is (local (defattach ...)) supported?
DEFATTACH (2)

Issues to consider:

► Is (local (defattach ...)) supported?
  YES, local is supported.
DEFATTACH (2)

Issues to consider:

▶ **Is** (local (defattach ...)) **supported?**
  
  **YES**, **local is supported**.

▶ Then how do we deal with conservativity?
DEFATTACH (2)

Issues to consider:

▶ Is `(local (defattach ...))` supported?
  YES, local is supported.
▶ Then how do we deal with conservativity?
  Two theories: The current theory for reasoning and a stronger evaluation theory, extended using `defattach`:
  \[ \text{spec}(x) = \text{impl}(x) \]
**DEFATTACH (2)**

Issues to consider:

- **Is** (**local** (**defattach** ...)) **supported?**
  - **YES**, **local** is **supported**.
- **Then how do we deal with conservativity?**
  - **Two theories**: The **current theory** for reasoning and a **stronger evaluation theory**, extended using **defattach**:
    
    \[
    \text{spec}(x) = \text{impl}(x)
    \]

- **Ah, but what about this?**
  
  ```lisp
  (thm (equal (f 3 4) 70))
  ```
**Defattach (2)**

Issues to consider:

- Is `(local (defattach ...))` supported?
  YES, local is supported.

- Then how do we deal with conservativity?
  **Two theories:** The current theory for reasoning and a stronger evaluation theory, extended using `defattach`:
  \[ \text{spec}(x) = \text{impl}(x) \]

- Ah, but what about this?
  `(thm (equal (f 3 4) 70))`
  **The proof fails!** (Whew!)
**Defattach (2)**

Issues to consider:

- **Is** `(local (defattach ...))` **supported?**
  - **YES**, *local* is supported.

- Then how do we deal with conservativity?
  - **Two theories**: The *current theory* for reasoning and a *stronger evaluation theory*, extended using `defattach`:

    ```lisp
    spec(x) = impl(x)
    ```

- **Ah, but what about this?**

  ```lisp
  (thm (equal (f 3 4) 70))
  ```

  **The proof fails!** (Whew!)

- Why is the evaluation theory consistent?
**Defattach (2)**

Issues to consider:

▶ Is `(local (defattach ...))` supported?  
**YES**, `local` is supported.

▶ Then how do we deal with conservativity?  
**Two theories**: The *current theory* for reasoning and a stronger *evaluation theory*, extended using `defattach`:

\[ \text{spec}(x) = \text{impl}(x) \]

▶ Ah, but what about this?

```
(thm (equal (f 3 4) 70))
```

**The proof fails!** (Whew!)

▶ Why is the evaluation theory consistent?  
A key requirement is that the *attachment relation* is suitably **acyclic**.
**Defattach (2)**

Issues to consider:

- **Is** `(local (defattach ...))` **supported?**  
  *YES, local is supported.*

- Then how do we deal with conservativity?  
  **Two theories:** The *current theory* for reasoning and a *stronger evaluation theory*, extended using `defattach`:

  
  \[ \text{spec}(x) = \text{impl}(x) \]

- Ah, but what about this?

  ```lisp
  (thm (equal (f 3 4) 70))
  ```

  **The proof fails!** *(Whew!)*

- Why is the evaluation theory consistent?  
  A key requirement is that the attachment relation is **suitably acyclic**.

For details, including issues pertaining to evaluation, see the *Essay on Defattach* comment in the ACL2 sources.
Quantification is implemented using what amounts to a choice operator. **Example:**
Quantification, Choice, & Induction (1)

Quantification is implemented using what amounts to a choice operator. Example:

When asked to define
\[ r(y, z) = (\exists x)(p(x, y, z) \land q(x, y, z)) \]
ACL2 generates the following.
Quantification, Choice, & Induction (1)

Quantification is implemented using what amounts to a choice operator. **Example:**

When asked to define
\[ r(y, z) = (\exists x)(p(x, y, z) \land q(x, y, z)) \]
ACL2 generates the following.

**Conservatively introduce** \( w(y, z) \) and \( r(y, z) \) using local witness \( w(y, z) = (\varepsilon x)(p(x, y, z) \land q(x, y, z)) \)
to prove these axioms:

\[
\begin{align*}
&\quad r(y, z) = (p(w(y, z), y, z) \land q(w(y, z), y, z)) \\
&\quad (p(x, y, z) \land q(x, y, z)) \implies r(y, z)
\end{align*}
\]
This sort of thing is clearly conservative (assuming the Axiom of Choice or at least well-orderable models) . . .
This sort of thing is clearly conservative (assuming the Axiom of Choice or at least well-orderable models) . . .

. . . IF we ignore induction!
Quantification, Choice, & Induction (2)

This sort of thing is clearly conservative (assuming the Axiom of Choice or at least well-orderable models) . . .

. . . IF we ignore induction!

Conservativity with induction follows from a model-theoretic forcing argument.
Meta-theoretic Reasoning (1)

In ACL2, you can:
Meta-theoretic Reasoning (1)

In ACL2, you can:

- code a simplifier,
Meta-theoretic Reasoning (1)

In ACL2, you can:

- code a simplifier,
- prove that it is sound, and
Meta-theoretic Reasoning (1)

In ACL2, you can:

- code a simplifier,
- prove that it is sound, and
- direct its use during later proofs.
META-THEORETIC REASONING (1)

In ACL2, you can:

- code a simplifier,
- prove that it is sound, and
- direct its use during later proofs.

We can return to this on an extra slide, if there is time and interest.
OTHER LOGICAL CHALLENGES

Here are some other challenges in the foundations of ACL2.
Other Logical Challenges

Here are some other challenges in the foundations of ACL2.

- **Functional instantiation** allows the replacement of functions $f_1, \ldots, f_k$ by other functions $g_1, \ldots, g_k$ such that the $g_i$ satisfy the axioms introducing the $f_i$. 

- **Packages** provide namespaces — e.g., `PKG1::F` and `PKG2::F` are distinct. But packages introduce axioms such as `symbol-package-name(PKG1::F) = "PKG1"`. So package introduction is not conservative and hence must be recorded.

- One can specify a measure in order to admit a recursive definition. But what if the measure is defined in terms of a function whose definition is LOCAL?
**Other Logical Challenges**

Here are some other challenges in the foundations of ACL2.

- *Functional instantiation* allows the replacement of functions $f_1, \ldots, f_k$ by other functions $g_1, \ldots, g_k$ such that the $g_i$ satisfy the axioms introducing the $f_i$.

- *Packages* provide namespaces — e.g., $\text{PKG1}::F$ and $\text{PKG2}::F$ are distinct. But packages introduce axioms such as $\text{symbol-package-name(\text{PKG1}::F)} = \text{"PKG1"}$. So package introduction is not conservative and hence must be recorded.
Other Logical Challenges

Here are some other challenges in the foundations of ACL2.

- **Functional instantiation** allows the replacement of functions $f_1, \ldots, f_k$ by other functions $g_1, \ldots, g_k$ such that the $g_i$ satisfy the axioms introducing the $f_i$.

- **Packages** provide namespaces — e.g., `PKG1::F` and `PKG2::F` are distinct. But packages introduce axioms such as `symbol-package-name(PKG1::F) = "PKG1"`. So package introduction is not conservative and hence **must be recorded**.

- One can specify a **measure** in order to admit a recursive definition. But what if the measure is defined in terms of a function whose definition is **LOCAL**?
OUTLINE

Overview

ACL2 Introduction

Logical Foundations

Conclusion
**CONCLUSION**

- ACL2 has a 25 (or 44) year history and is used in industry.
CONCLUSION

- ACL2 has a 25 (or 44) year history and is used in industry.
  - People are actually *paid* to prove theorems with ACL2.
CONCLUSION

- ACL2 has a 25 (or 44) year history and is used in industry.
  - People are actually *paid* to prove theorems with ACL2.
    “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
Conclusion

- ACL2 has a 25 (or 44) year history and is used in industry.
  - People are actually paid to prove theorems with ACL2.
    
    "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

- As an ITP system, it relies on user guidance for large problems but enjoys scalability.
CONCLUSION

- ACL2 has a 25 (or 44) year history and is used in industry.
  - People are actually paid to prove theorems with ACL2.
    
    “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

- As an ITP system, it relies on user guidance for large problems but enjoys scalability.
- Mechanizing a logic, for efficient and flexible evaluation and proof, can present challenges.
CONCLUSION

- ACL2 has a 25 (or 44) year history and is used in industry.
  - People are actually *paid* to prove theorems with ACL2.
    
    “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

- As an ITP system, it relies on user guidance for large problems but enjoys scalability.

- Mechanizing a logic, for efficient and flexible evaluation and proof, can present challenges.

- For more information, see the ACL2 home page, in particular links to The Tours and Publications, which links to introductory material.
CONCLUSION

► ACL2 has a 25 (or 44) year history and is used in industry.
  ► People are actually paid to prove theorems with ACL2.
    “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

► As an ITP system, it relies on user guidance for large problems but enjoys scalability.

► Mechanizing a logic, for efficient and flexible evaluation and proof, can present challenges.

► For more information, see the ACL2 home page, in particular links to The Tours and Publications, which links to introductory material.

THANK YOU!
EXTRA SLIDES

We can go on, time permitting....
Some ACL2 features *not* discussed further today:

- **Prover algorithms**
  - **Waterfall, linear arithmetic, Boolean reasoning, ...**
  - **Rewriting:** Conditional, congruence-based, rewrite cache, syntaxp, bind-free, ...

- **Using the prover effectively**
  - **The-method and introduction-to-the-theorem-prover**
  - **Theories, hints, rule-classes, ...**
  - **Accumulated-persistence, brr, proof-checker, dmr, ...**

- **Programming support, including (just a few):**
  - **Guards**
  - **Hash-cons and function memoization**
  - **Packages**
    - **Mutable State, stobjs, arrays, applicative hash tables, ...**

- **System-level:** **Emacs support, books and certification, abbreviated printing, parallelism (ACL2(p)), ...**
META-THEORETIC REASONING (2)

ACL2 supports a notion of “eval”, together with this sort of meta theorem, directing the use of fn to transform terms that are calls of nth or of foo.
META-THEORETIC REASONING (2)

ACL2 supports a notion of “eval”, together with this sort of *meta* theorem, directing the use of \texttt{fn} to transform terms that are calls of \texttt{nth} or of \texttt{foo}.

\begin{verbatim}
(defthm fn-correct-1
  (equal (evl x a)
      (evl (fn x) a))
  :rule-classes ((:meta :trigger-fns (nth foo))))
\end{verbatim}
META-THEORETIC REASONING (2)

ACL2 supports a notion of “eval”, together with this sort of meta theorem, directing the use of \( fn \) to transform terms that are calls of \( nth \) or of \( foo \).

```
(defun fn-correct-1
  (fn x)
  \n  :rule-classes ((\:meta \:trigger-fns (nth foo))))
```

More complex forms are supported, including:
META-THEORETIC REASONING (2)

ACL2 supports a notion of “eval”, together with this sort of *meta* theorem, directing the use of `fn` to transform terms that are calls of `nth` or of `foo`.

```
(defun fn-correct-1
  (equal (evl x a)
         (evl (fn x) a))
  :rule-classes ((:meta :trigger-fns (nth foo))))
```

More complex forms are supported, including:

- **extended-metatheorems** that take `STATE` and contextual inputs;
META-THEORETIC REASONING (2)

ACL2 supports a notion of “eval”, together with this sort of *meta* theorem, directing the use of `fn` to transform terms that are calls of `nth` or of `foo`.

```
(defun fn-correct-1
  (equal (evl x a)
         (evl (fn x) a)))
```

More complex forms are supported, including:

- **extended-metafunctions** that take `STATE` and contextual inputs;
- **transformations at the goal level**; and
**Meta-theoretic Reasoning (2)**

ACL2 supports a notion of “eval”, together with this sort of *meta* theorem, directing the use of \( \text{fn} \) to transform terms that are calls of \( \text{nth} \) or of \( \text{foo} \).

```lisp
(defthm fn-correct-1
  (equal (evl x a)
         (evl (fn x) a))
  :rule-classes ((:meta :trigger-fns (nth foo))))
```

More complex forms are supported, including:

- *extended-metafunctions* that take \( \text{STATE} \) and contextual inputs;
- *transformations at the goal level*; and
- *hypotheses that extract known information* from the logical world.
META-THEORETIC REASONING (2)

ACL2 supports a notion of "eval", together with this sort of *meta* theorem, directing the use of `fn` to transform terms that are calls of `nth` or of `foo`.

```lisp
(defthm fn-correct-1
  (equal (evl x a)
         (evl (fn x) a))
  :rule-classes ((:meta :trigger-fns (nth foo))))
```

More complex forms are supported, including:

- **extended-metafunctions** that take `STATE` and contextual inputs;
- **transformations at the goal level**; and
- **hypotheses that extract known information** from the logical world.

For details, including issues pertaining to evaluation, see the *Essay on Correctness of Meta Reasoning* comment in the ACL2 sources.
**Meta-theoretic Reasoning (2)**

ACL2 supports a notion of “eval”, together with this sort of *meta* theorem, directing the use of `fn` to transform terms that are calls of `nth` or of `foo`.

(defthm fn-correct-1
  (equal (evl x a)
         (evl (fn x) a))
  :rule-classes ((:meta :trigger-fns (nth foo))))

More complex forms are supported, including:

- extended-metafunctions that take `STATE` and contextual inputs;
- transformations at the goal level; and
- hypotheses that extract known information from the logical world.

For details, including issues pertaining to evaluation, see the *Essay on Correctness of Meta Reasoning* comment in the ACL2 sources. *Attachments* provide a challenge.