Integrating Nonlinear Arithmetic into ACL2

Warren A. Hunt, Jr., Robert Bellarmine Krug, and J Moore

hunt@cs.utexas.edu, rkrug@cs.utexas.edu, moore@cs.utexas.edu

Department of Computer Sciences

University of Texas at Austin

Austin, TX 78712-1188, USA

Outline

- Introduction
- The Arithmetic Packages
- ACL2

Guiding Ideas

- What is obvious to the user, should be obvious to ACL2
- To this end, use computer cycles rather than human effort
- As computers get ever faster, algorithms and ideas which were previously considered too inefficient, under appropriate limiting heuristics, become ever more important.

The Arithmetic Packages

Arithmetic Package

- Linear Arithmetic
- Linear Lemmas
- Nonlinear Arithmetic

Linear Arithmetic Example

$$3 \cdot x + 7 \cdot a < 4 \quad \wedge \quad 2 \cdot x > 3 \quad \Longrightarrow \quad a < 0$$

Linear Arithmetic Example

$$3 \cdot x + 7 \cdot a < 4 \quad \wedge \quad 2 \cdot x > 3 \quad \Longrightarrow \quad a < 0$$

Proof by contradiction,
assume hypotheses and negation of conclusion:

$$0 < -3 \cdot x + -7 \cdot a + 4$$
$$0 < 2 \cdot x + -3$$
$$0 \leq a$$

Linear Arithmetic Example

$$3 \cdot x + 7 \cdot a < 4 \quad \wedge \quad 2 \cdot x > 3 \quad \Longrightarrow \quad a < 0$$

Proof by contradiction,
assume hypotheses and negation of conclusion:

$$0 < -3 \cdot x + -7 \cdot a + 4$$
$$0 < 2 \cdot x + -3$$
$$0 \leq a$$

Linear Arithmetic Example

$$3 \cdot x + 7 \cdot a < 4 \quad \wedge \quad 2 \cdot x > 3 \quad \Longrightarrow \quad a < 0$$

Proof by contradiction,
assume hypotheses and negation of conclusion:

$$0 < -3 \cdot x + -7 \cdot a + 4$$
$$0 < 2 \cdot x + -3$$
$$0 \leq a$$

$$0 < -14 \cdot a + -1$$

Linear Arithmetic Example

$$3 \cdot x + 7 \cdot a < 4 \quad \wedge \quad 2 \cdot x > 3 \quad \Longrightarrow \quad a < 0$$

Proof by contradiction,
assume hypotheses and negation of conclusion:

$$0 < -3 \cdot x + -7 \cdot a + 4$$
$$0 < 2 \cdot x + -3$$
$$0 \leq a$$

$$0 < -14 \cdot a + -1$$

Linear Arithmetic Example

$$3 \cdot x + 7 \cdot a < 4 \quad \wedge \quad 2 \cdot x > 3 \quad \Longrightarrow \quad a < 0$$

Proof by contradiction,
assume hypotheses and negation of conclusion:

$$0 < -3 \cdot x + -7 \cdot a + 4$$
$$0 < 2 \cdot x + -3$$
$$0 \leq a$$

$$0 < -14 \cdot a + -1$$

$$0 < -1$$

Observations

Three key properties of linear algorithm:

- Incremental
- Non-destructive
- Quick Start-up

Optimizations

- Better Filtering of Polys
- Depth-first Vs. Breadth-first

Better Filtering of Polys

- Observation: It makes no sense to add a poly to the database a second time
- Previous: Check whether an equal poly had already been added to database.
- Now: Check for stronger or equal poly.
- $0 < y + 2 \cdot x + 5$ is stronger than $0 < y + 2 \cdot x + 7$
- Neither is related to $0 < y + 3 \cdot x + 1$

Depth-first Vs. Breadth-first

Claim: By switching from a depth-first to a breadth-first search, we can filter polys more effectively.

Linear Lemmas

- Many problems are “close” to linear
- By “partially” interpreting functions other than +, -, etc., more problems can be solved.
  - $\text{len}(x) >= 0$
  - $x > 1 \quad \wedge \quad n > 1 \quad \Longrightarrow \quad x^n > x$
- Type reasoning and linear lemmas carry out this partial interpretation.

Nonlinear Arithmetic Example

$$
\begin{aligned}
3 \cdot x \cdot y + 7 \cdot a < 4 \\
\wedge \quad 2 \cdot x > 3 \\
\wedge \quad y > 1 \\
\Longrightarrow \quad a < 0
\end{aligned}
$$

Nonlinear Arithmetic Example

$$
\begin{aligned}
& 3 \cdot x \cdot y + 7 \cdot a < 4 \\
& \quad \wedge \quad 2 \cdot x > 3 \\
& \quad \wedge \quad y > 1 \\
& \quad \Longrightarrow \quad a < 0
\end{aligned}
$$

$$
\begin{aligned}
& 0 < -3 \cdot x \cdot y + -7 \cdot a + 4 \\
& 0 < 2 \cdot x + -3 \\
& 0 < y + -1 \\
& 0 \leq a
\end{aligned}
$$

Nonlinear Arithmetic Example

$$
\begin{aligned}
3 \cdot x \cdot y + 7 \cdot a < 4 & \\
\wedge \quad 2 \cdot x > 3 & \\
\wedge \quad y > 1 & \\
\Longrightarrow \quad a < 0 &
\end{aligned}
$$

$$
\begin{aligned}
0 &< -3 \cdot x \cdot y + -7 \cdot a + 4 \\
0 &< 2 \cdot x + -3 \\
0 &< y + -1 \\
0 &\leq a
\end{aligned}
$$

Nonlinear Arithmetic Example

$$0 < -3 \cdot x \cdot y + -7 \cdot a + 4$$
$$0 < 2 \cdot x + -3$$
$$0 < y + -1$$
$$0 \leq a$$

Nonlinear Arithmetic Example

$$0 < -3 \cdot x \cdot y + -7 \cdot a + 4$$
$$0 < 2 \cdot x + -3$$
$$0 < y + -1$$
$$0 \leq a$$

Nonlinear Arithmetic Example

$$0 < -3 \cdot x \cdot y + -7 \cdot a + 4$$
$$0 < 2 \cdot x + -3$$
$$0 < y + -1$$
$$0 \leq a$$

$$0 < 2 \cdot x \cdot y + -3 \cdot y + -2 \cdot x + 3$$

Nonlinear Arithmetic Example

$$0 < -3 \cdot x \cdot y + -7 \cdot a + 4$$
$$0 < 2 \cdot x + -3$$
$$0 < y + -1$$
$$0 \leq a$$

$$0 < 2 \cdot x \cdot y + -3 \cdot y + -2 \cdot x + 3$$

Nonlinear Arithmetic Example

$$0 < -3 \cdot x \cdot y + -7 \cdot a + 4$$
$$0 < 2 \cdot x + -3$$
$$0 < y + -1$$
$$0 \leq a$$

$$0 < 2 \cdot x \cdot y + -3 \cdot y + -2 \cdot x + 3$$

$$0 < -9 \cdot y + -6 \cdot x + -14 \cdot a + 9$$

Nonlinear Arithmetic Example

$$0 < -3 \cdot x \cdot y + -7 \cdot a + 4$$
$$0 < 2 \cdot x + -3$$
$$0 < y + -1$$
$$0 \leq a$$

$$0 < 2 \cdot x \cdot y + -3 \cdot y + -2 \cdot x + 3$$

$$0 < -9 \cdot y + -6 \cdot x + -14 \cdot a + 9$$

Nonlinear Arithmetic Example

$$0 < -3 \cdot x \cdot y + -7 \cdot a + 4$$
$$0 < 2 \cdot x + -3$$
$$0 < y + -1$$
$$0 \leq a$$

$$0 < 2 \cdot x \cdot y + -3 \cdot y + -2 \cdot x + 3$$

$$0 < -9 \cdot y + -6 \cdot x + -14 \cdot a + 9$$

$$0 < -6 \cdot x - 14 \cdot a$$

Nonlinear Arithmetic Example

$$0 < -3 \cdot x \cdot y + -7 \cdot a + 4$$
$$0 < 2 \cdot x + -3$$
$$0 < y + -1$$
$$0 \leq a$$

$$0 < 2 \cdot x \cdot y + -3 \cdot y + -2 \cdot x + 3$$

$$0 < -9 \cdot y + -6 \cdot x + -14 \cdot a + 9$$

$$0 < -6 \cdot x - 14 \cdot a$$

Nonlinear Arithmetic Example

$$0 < -3 \cdot x \cdot y + -7 \cdot a + 4$$
$$0 < 2 \cdot x + -3$$
$$0 < y + -1$$
$$0 \leq a$$

$$0 < 2 \cdot x \cdot y + -3 \cdot y + -2 \cdot x + 3$$

$$0 < -9 \cdot y + -6 \cdot x + -14 \cdot a + 9$$

$$0 < -6 \cdot x - 14 \cdot a$$

$$0 < -14 \cdot a + -9$$

Nonlinear Arithmetic Example

$$0 < -3 \cdot x \cdot y + -7 \cdot a + 4$$
$$0 < 2 \cdot x + -3$$
$$0 < y + -1$$
$$0 \leq a$$

$$0 < 2 \cdot x \cdot y + -3 \cdot y + -2 \cdot x + 3$$

$$0 < -9 \cdot y + -6 \cdot x + -14 \cdot a + 9$$

$$0 < -6 \cdot x - 14 \cdot a$$

$$0 < -14 \cdot a + -9$$

Nonlinear Arithmetic Example

$$0 < -3 \cdot x \cdot y + -7 \cdot a + 4$$
$$0 < 2 \cdot x + -3$$
$$0 < y + -1$$
$$0 \leq a$$

$$0 < 2 \cdot x \cdot y + -3 \cdot y + -2 \cdot x + 3$$

$$0 < -9 \cdot y + -6 \cdot x + -14 \cdot a + 9$$

$$0 < -6 \cdot x - 14 \cdot a$$

$$0 < -14 \cdot a + -9$$

$$0 < -9$$

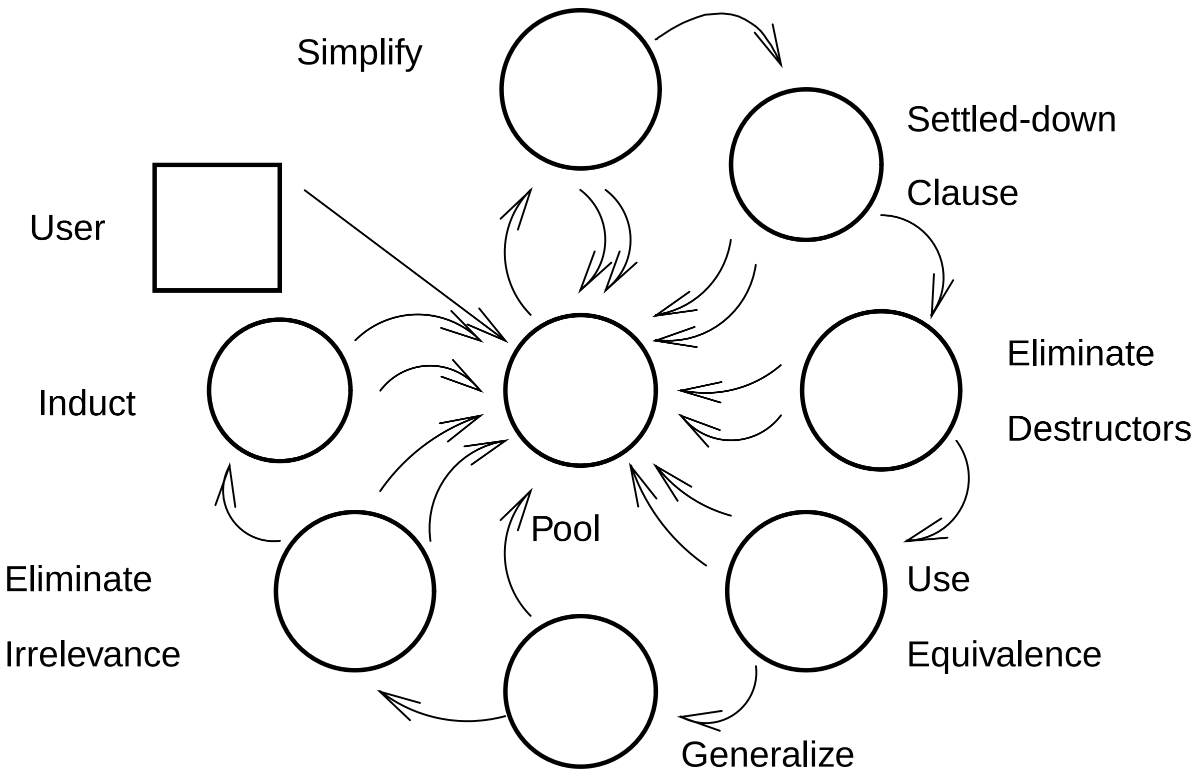
Observations

- Extremely high computational complexity
- Expensive in practice, but by limiting the search can often be practical

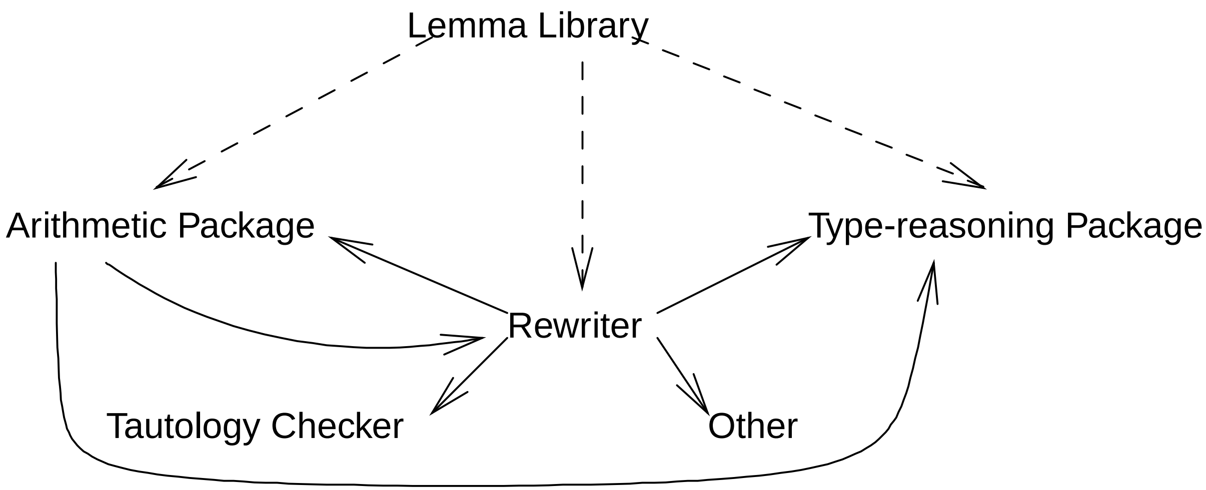
Incompleteness

- Necessarily incomplete for nonlinear arithmetic over the rationals (Julia Robinson, 1949)
- $x^2 = 3$
  No real numbers in ACL2
  $\forall x \,.\, x^2 \neq 2$
- $$\begin{array}{ll} & 0 < a \cdot b \\ \wedge & 0 < c \cdot d \\ \wedge & 0 < a \cdot c \\ \Longrightarrow & 0 < b \cdot d \end{array}$$
  No factors to multiply

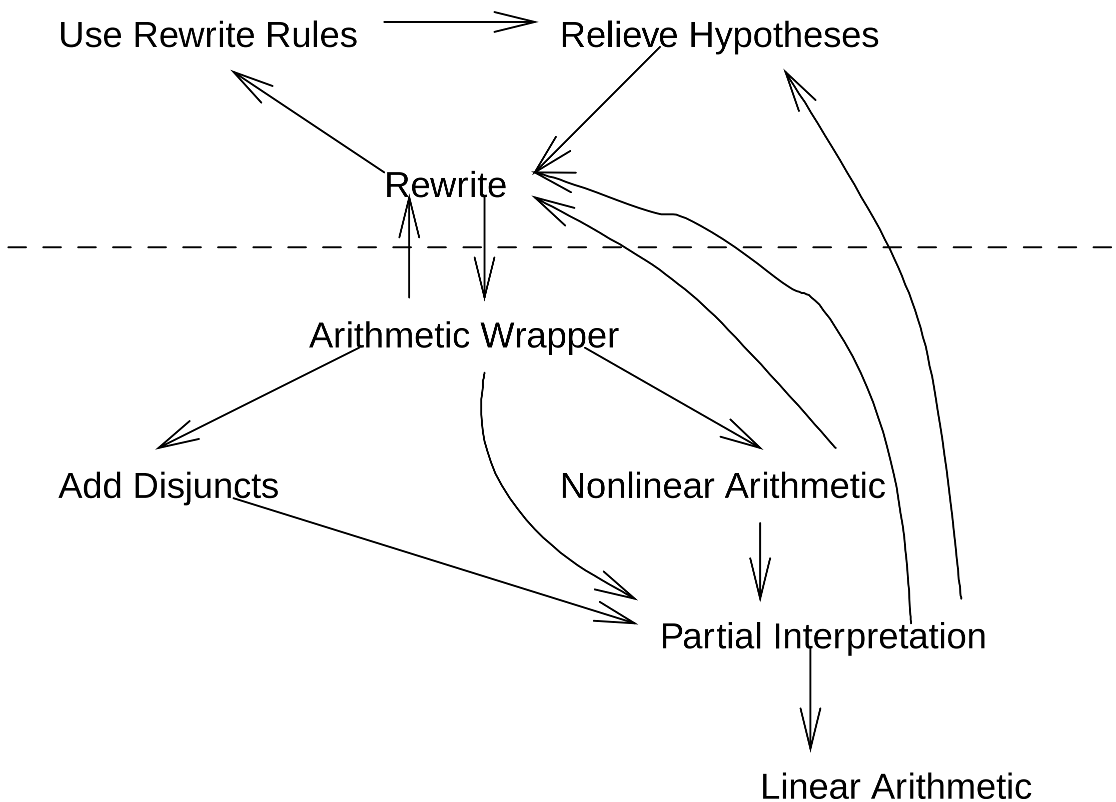
ACL2 — a High Level View



The Simplifier



Arithmetic and the Rewriter



Conclusion

More theorems can now be proved more easily