MetiTarski's Menagerie of Cooperating Systems

Lawrence C. Paulson

Computer Laboratory

University of Cambridge

1. On Combining Systems

Combining Systems is Hard!

- Example 1: “Integrating decision procedures into heuristic theorem provers: A case study of linear arithmetic” (Boyer and Moore, 1988)
- Example 2: “Reachability programming in HOL98 using BDDs” (MJC Gordon, 2000)
- Example 3: Isabelle’s Sledgehammer (2007)
- Example 4: Resolution + RCF = MetiTarski (2008)

Adding Linear Arithmetic to the Boyer/Moore Prover

- Simply adding their (custom-made!) decision procedure to the Boyer/Moore prover had little effect.
- Deep integration with the rewriter was necessary: their decision procedure was no black box.
- Final version “like the software for the space shuttle”

Adding BDDs to HOL98

- What's the point of BDDs here? Proof assistants don't *need* to check huge tautologies. But…
- Mike Gordon added the BDD data structure to HOL.
  - assertions relating formulas to their BDDs
  - BDD-level *operations* directly available
- This package was general enough to implement *model checking* in HOL!

Adding ATPs to Isabelle

- Similar integrations were attempted before, but how to make it usable for novices — and useful to experts?
- Sledgehammer provides *automatic*…
  - problem translation (into FOL or whatever)
  - lemma selection (out of the *entire* lemma library)
  - process management (remote invocations, etc.)
- ATPs are invoked as black boxes—and are not trusted!

Combining Clause Methods with Decision Procedures

- SMT: propositional over-approximation
- DPLL($\Gamma+\mathcal{T}$): a *calculus* for DPLL + superposition
- MetiTarski: a modified *resolution prover*
  - using decision procedures to simplify clauses…
  - and to delete redundant ones

2. MetiTarski

MetiTarski: the Key Ideas

- proving statements about exp, ln, sin, cos, $\tan^{-1}$ — *via*
  - axioms bounding the functions by rational functions
  - heuristics to isolate and remove function occurrences
  - decision procedures for real arithmetic (RCF)

(Real polynomial arithmetic is decidable!
— though doubly exponential…)

Some Upper/Lower Bounds

$$\exp(x) \geqslant 1 + x + \cdots + x^n/n! \qquad (n \text{ odd})$$

$$\exp(x) \leqslant 1 + x + \cdots + x^n/n! \qquad (n \text{ even}, x \leqslant 0)$$

$$\exp(x) \leqslant 1/(1 - x + x^2/2! - x^3/3!) \qquad (x < 1.596)$$

Taylor series, …

continued fractions, …

$$\frac{x-1}{x} \leqslant \ln x \leqslant x - 1$$

$$\frac{(1+5x)(x-1)}{2x(2+x)} \leqslant \ln x \leqslant \frac{(x+5)(x-1)}{2(2x+1)}$$

Division Laws, abs, etc…

$$\neg(x \leqslant y \cdot z) \vee x/z \leqslant y \vee z \leqslant 0$$

$$\neg(x \leqslant y/z) \vee x \cdot z \leqslant y \vee z \leqslant 0$$

$$\neg(x \cdot z \leqslant y) \vee x \leqslant y/z \vee z \leqslant 0$$

$$\neg(x/z \leqslant y) \vee x \leqslant y \cdot z \vee z \leqslant 0$$

$$x \geqslant 0 \Rightarrow |x| = x$$

$$x < 0 \Rightarrow |x| = -x$$

Analysing A Simple Problem

split on signs of expressions

split on sign of x

$$|\exp x - (1 + x/2)^2| \leqslant |\exp(|x|) - (1 + |x|/2)^2|$$

- isolate occurrences of functions
- … replace them by their bounds
- replace division by multiplication
- call decision procedure

How do we bring about these transformations?

Architectural Alternatives

Roll your own tableau prover?

Analytica (1993)
Weierstrass (2001)

we have full control — must micromanage the proof search

Hack an existing resolution prover?

no calculus — it's ad-hoc
(what is "the algorithm"?)

resolution can surprise us

3. Details of the Integration

Resolution Refresher Course

- Resolution operates on *clauses*: disjunctions of literals.
- Resolving two clauses yields a new one.
- The aim is to contradict the negation of the goal — by deriving the empty clause.

$$P(X) \vee R(X, 1) \quad \neg R(0, Y) \vee Q(Y)$$

$$\Downarrow$$

$$P(0) \vee Q(1)$$

Algebraic Literal Deletion

- Retain a list of the *ground polynomial clauses* (no variables).
- Delete any literal that is inconsistent with them…
- by calling an RCF decision procedure.
- Deleting literals helps to derive the empty clause.
- This process yields a fine-grained integration between resolution and a decision procedure.

Literal Deletion Examples

- *Unsatisfiable* literals such as $p^2 < 0$ are deleted.
- If $x(y+1) > 1$ is known, then $x=0$ will be deleted.
- The context includes the *negations of adjacent literals* in the clause: $z^2 > 3 \cancel{\vee z > 5}$

… the decision procedure reduces $\exists z\, [z^2 \leq 3 \wedge z > 5]$ to false.

A Tiny Proof: $\forall x\, |e^x - 1| \leqslant e^{|x|} - 1$

negating the claim

$$e^{|c|} < 1 + |e^c - 1|$$

absolute value (neg)

$$0 \leqslant c \vee e^{-c} < 1 + |e^c - 1|$$

absolute value (neg)

$$1 \leqslant e^c \vee 0 \leqslant c \vee e^{-c} < 2 - e^c$$

lower bound: $1 - c \leq e^{-c}$

$$1 \leqslant e^c \vee 0 \leqslant c \vee e^c < 1 + c$$

lower bound: $1 + c \leq e^c$

$$1 \leqslant e^c \vee 0 \leqslant c$$

$0 \leq c \Rightarrow 1 \leq e^c$

$$1 \leqslant e^c$$

absolute value (pos)

$$e^{|c|} < e^c \cancel{\vee e^c < 1}$$

absolute value, etc.

$$c < 0$$

$$\square$$

To Summarise...

Replace functions by *rational function upper or lower bounds*,

and then get rid of division.

We obtain conjunctions of *polynomial inequalities*,

... which are **decidable**.

Resolution theorem proving applies these steps “in its own way”.

A Few Easy Examples...

$$
\begin{aligned}
0 < t \land 0 < v_f \implies & ((1.565 + .313 v_f)\cos(1.16t) \\
& + (.01340 + .00268 v_f)\sin(1.16t))e^{-1.34t} \\
& - (6.55 + 1.31 v_f)e^{-.318t} + v_f + 10 \geqslant 0
\end{aligned}
$$

$$
\begin{aligned}
& 0 \leqslant x \land x \leqslant 289 \land s^2 + c^2 = 1 \implies \\
& \qquad 1.51 - .023e^{-.019x} - (2.35c + .42s)e^{.00024x} > -2
\end{aligned}
$$

$$
0 \leqslant x \land 0 \leqslant y \implies y \tanh(x) \leqslant \sinh(yx)
$$

Our Decision Procedures

QEPCAD (Hoon Hong, C. W. Brown et al.)
venerable — very fast for univariate problems

Mathematica (Wolfram research)
much faster than QEPCAD for 3–4 variables

Z3 (de Moura et al., Microsoft Research)
an SMT solver with non-linear reasoning

Integration Issues

- QEPCAD was purposely designed for human use — not as a back-end.
- With Z3 we go beyond black box integration, feeding back models to speed later execution.
- Machine learning can help identify the best decision procedure for a given problem.
- Many integration issues are trivial (e.g. buffer blocking) but **vexing**.

4. Applications

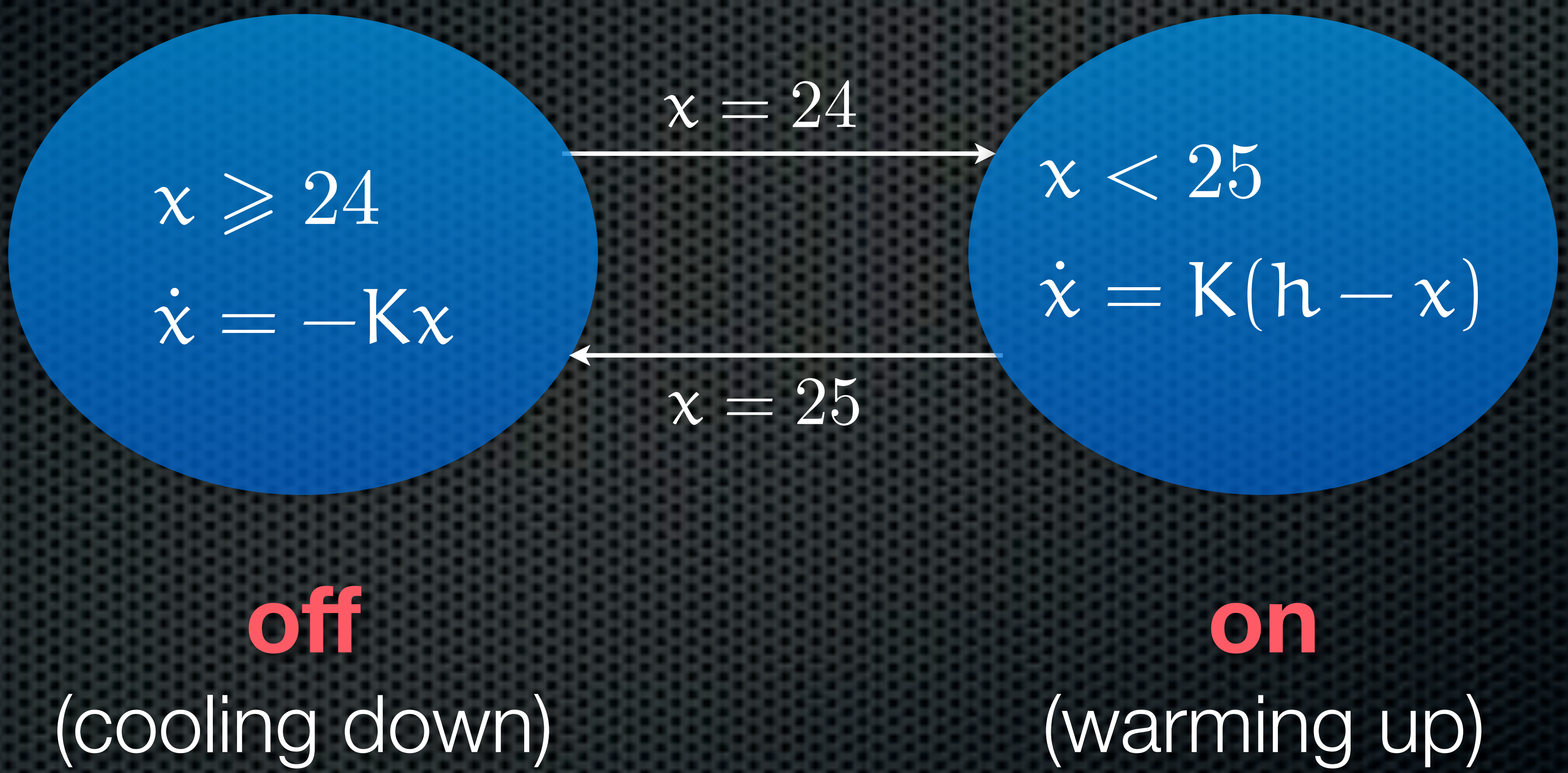
MetiTarski's Applications

- Analogue circuit verification (Denman et al., 2009)
- Linear hybrid systems (Akbarpour & LCP, 2009)
- Abstracting non-polynomial dynamical systems (Denman, 2012)
- KeYmaera linkup: non-linear hybrid systems (Sogokon et al.)
- PVS linkup: NASA collision-avoidance projects (Muñoz & Denman)

(What are Hybrid Systems?)

- dynamical systems where the state space has
  - discrete *modes* (with transitions to other modes)
  - *continuous dynamics* in each mode
- simple examples: bouncing ball, water tank
  - any computer-controlled physical process
  - autopilots, driverless trains, automated factories, …

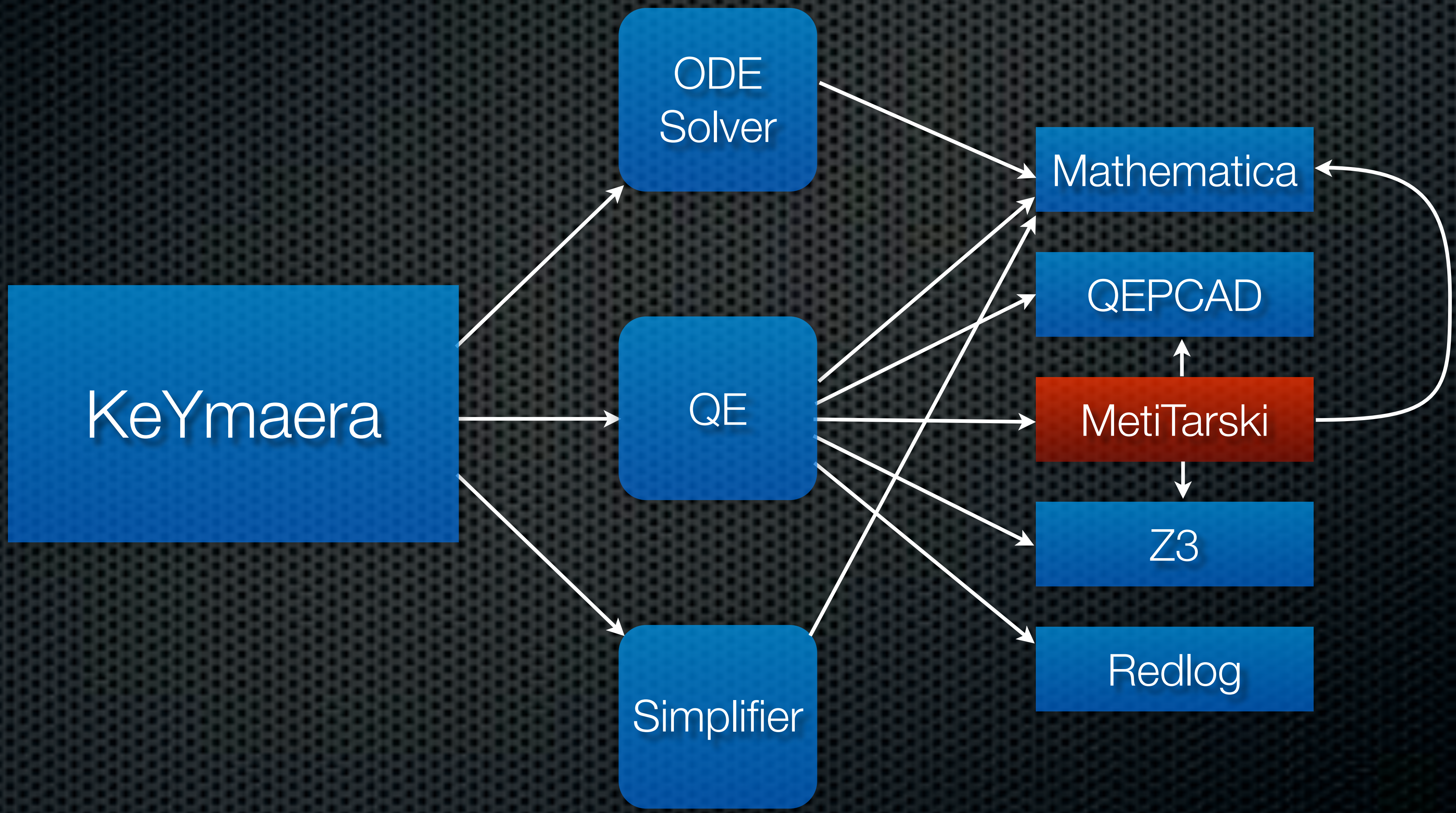
The Theromstat (sorry)



KeYmaera

- a verification tool for hybrid systems (Platzer)
- extends the KeY interactive prover with a dynamic logic
  - a free-variable tableau calculus
  - “differential induction”
  - integration with RCF decision procedures
- MetiTarski extends its language from polynomials to allow transcendental functions.

KeYmaera + MetiTarski



Some KeYmaera Examples

- Damped pendulum, described by the second-order differential equation $\ddot{x} + 2d\omega\dot{x} + \omega^2 x = 0$
- Ultimately, MetiTarski has to prove (This takes 1/4 sec)

$$t \geqslant 0 \wedge 0 \leqslant x \wedge x \leqslant 1 \Longrightarrow x e^{-\frac{6t}{5}} \left(4\cos\left(\frac{8t}{5}\right) + 3\sin\left(\frac{8t}{5}\right)\right) \leqslant 4$$

- Stability proofs using Lyapunov functions

MetiTarski + PVS

- Trusted interface, complementing PVS support of interval methods for polynomial estimation
- It's being tried within NASA's ACCoRD project.
- MetiTarski has been effective in early experiments
- … but there's much more to do.

Future Possibilities

- Refinements to the RCF decision process
- Integration with Isabelle?
  - Formal proofs of all upper/lower bounds
  - Can decision procedures return certificates?
- Machine learning within the decision procedures

The Cambridge Team

James Bridge

William Denman

Zongyan Huang

(*to 2008*: Behzad Akbarpour)

Acknowledgements

- *Edinburgh*: Paul Jackson, G Passmore, A Sogokon; *Manchester*: Eva Navarro
- Assistance from C. W. Brown, A. Cuyt, J. H. Davenport, J. Harrison, J. Hurd, D. Lester, C. Muñoz, U. Waldmann, etc.
- The research was supported by the Engineering and Physical Sciences Research Council [grant numbers EP/C013409/1,EP/I011005/1,EP/I010335/1].