The Potential of MetiTarski for Interactive Theorem Proving

Lawrence C Paulson

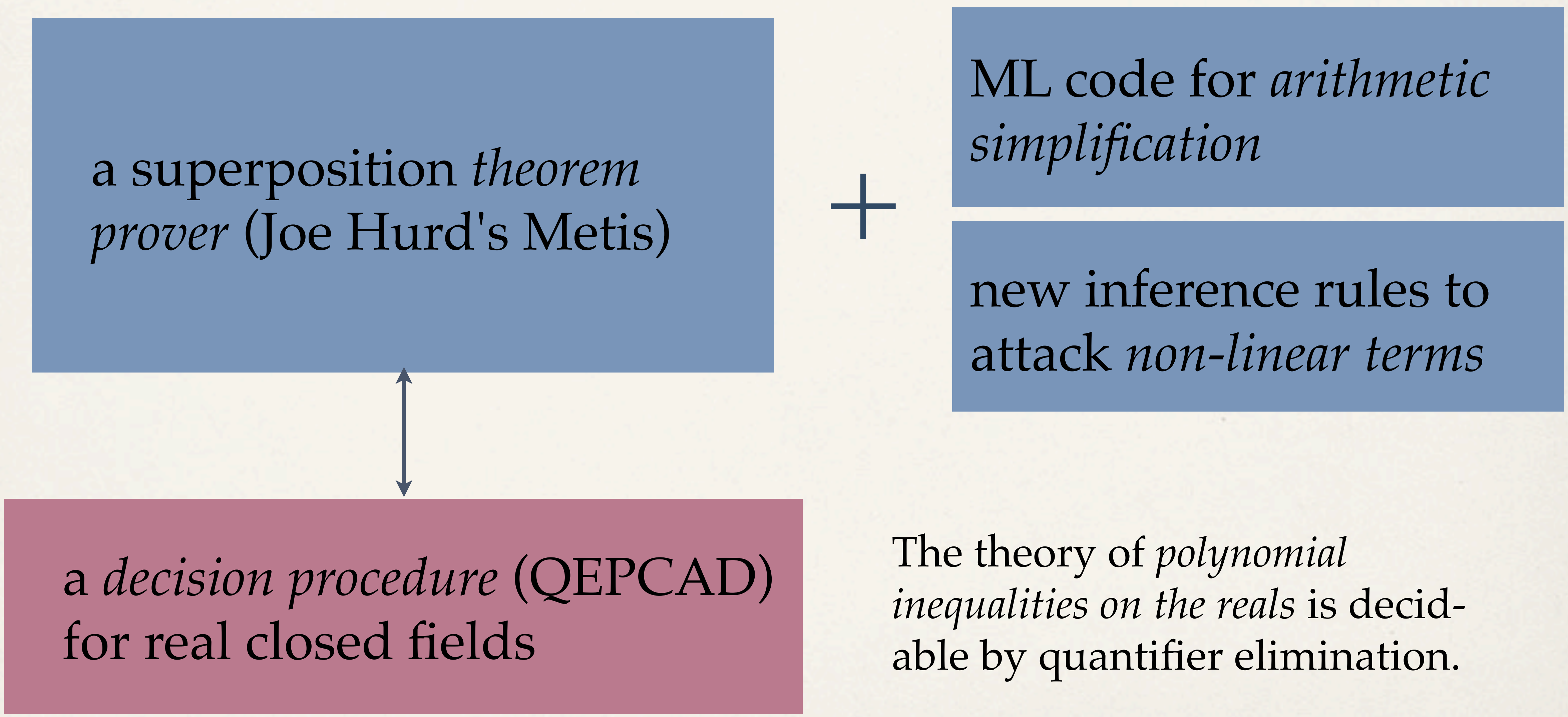
August 2010

MetiTarski, An Automatic Prover

$$\forall x.\ |x| < 1 \implies |\ln(1+x)| \le -\ln(1-|x|)$$

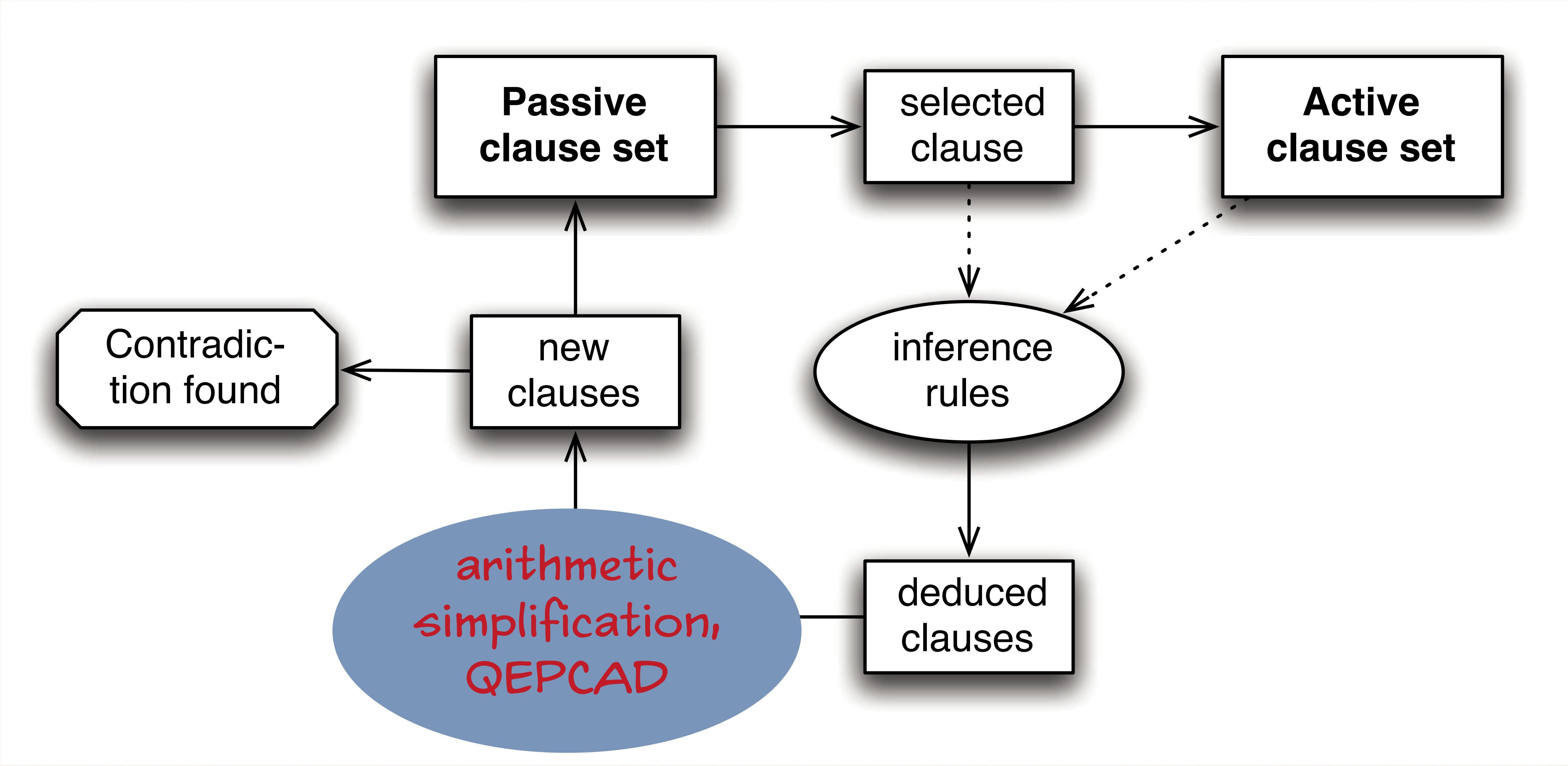
... for real-valued special functions

Architecture



The theory of *polynomial inequalities on the reals* is decidable by quantifier elimination.

Modified Resolution Main Loop



Examples (Mostly proved in seconds!)

$$x > 0 \implies \tan^{-1} x > 8\sqrt{3}\,x/(3\sqrt{3} + \sqrt{75 + 80x^2})$$

$$x > 0 \implies (x + 1/x)\tan^{-1} x > 1$$

$$x > 0 \implies \tan^{-1} x > 3x/(1 + 2\sqrt{1 + x^2})$$

$$0 < x \le \pi \implies \cos(x) \le \sin(x)/x$$

$$0 < x < \pi/2 \implies \cos x < \sin^2 x/x^2$$

$$\pi/3 \le x \le 2\pi/3 \implies \sin x/3 + \sin(3x)/6 > 0$$

$$0 \le x \le 289 \implies 3.51 > .023e^{-.019x} + 2.35e^{.00024x}\cos(.019x) + .42e^{.00024x}\sin(.019x)$$

$$0 \le x \wedge 0 \le y \implies y\tanh(x) \le \sinh(yx)$$

Got this by solving a DIFFERENTIAL EQUATION

Potential Applications

Analogue circuit verification (Concordia University)

Control and hybrid systems

Error analysis

Anything that can be modelled by linear differential equations

+?

Trust Issues

- *Arithmetic simplification*: reducing polynomials to canonical form; extending the scope of quotients
- *Specialised axioms* giving upper or lower bounds of special functions
- RCF decision procedure

But, we get machine-readable proofs!
(Resolution + extensions)

A Machine-Readable Proof

```
SZS output start CNFRefu
cnf(lgen_le_neg, axiom,

cnf(leq_left_divide_mul_

cnf(leq_right_divide_mul

cnf(leq_right_divide_mul

cnf(exp_positive, axiom,

cnf(exp_lower_taylor_1,
    (~ -1 <= X | ~ lgen(

cnf(exp_lower_taylor_5_c
    (~ lgen(R, Y,
            (1 + X / 3 +
             1 / 24 * (X
     lgen(R, Y, exp(X)))
```

nearly 200 steps!

```
.
.
.
cnf(refute_0_191, plain, ($false),
    inference(resolve,
              [$cnf(skoX *
                    (21743271936 +
                     skoX *
                     (10871635968 +
                      skoX *
                      (3623878656 +
                       skoX *
                       (891813888 +
                        skoX *
                        (169869312 +
                         skoX *
                         (25657344 +
                          skoX *
                          (3096576 +
                           skoX *
                           (297216 +
                            skoX *
                            (22272 +
                             skoX * (1248 + skoX * (48 + skoX)))))))))) <=
                    -21743271936)], [refute_0_189, refute_0_190])).
SZS output end CNFRefutation for abs-problem-14.tptp
```

Arithmetic Simplification

Translation to canonical form

Obvious cancellation laws

$$\left(\frac{x}{y}\right)\frac{1}{\left(x+\frac{1}{x}\right)} = \frac{x^2}{y(x^2+1)}$$

Transformation of quotients

Reconstruction in an ITP
should be straightforward...

Verifying the Axioms

- *Taylor series expansions* are already verified for the elementary functions (sin, cos, $\tan^{-1}$, exp, ln).
- Continued fraction/Padé approximations are better (more accurate over wider ranges), but seem to rely on advanced theory.
- We could *take them on trust*: they are well understood. Specific expansions could be checked using computer algebra systems.

Verifying the Decision Procedure

- The best-known procedure (cylindrical algebraic composition) is complicated and requires an efficient computer algebra system.
- Real quantifier elimination is *doubly exponential* in the number of variables (Davenport and Heintz, 1988)
- Few implementations of any sort exist; fewer justify their answers with any sort of **evidence**.
- *Hörmander's decision procedure* (in HOL-Light) is useless if the polynomial's degree exceeds 6. *Sum-of-squares methods* also yield evidence.

How Much Must We Trust The Decision Procedure?

- During its search, MetiTarski may call the decision procedure hundreds of times, also to discard redundant clauses.
- We only need to trust calls appearing in the proof, but there could still be dozens!
- These are specific conjunctions of polynomial inequalities, which could be validated by other means (not necessarily deductive).

Summary: a Lot to Trust…

- At least, the proofs give us a specific list of simpler properties to trust:
  - Polynomial inequalities (could be checked numerically)
  - Continued fraction approximations (and finitely many cover a huge number of problems)
- The situation may be much improved after 10 years.

MetiTarski Acknowledgements

- Postdoc: Behzad Akbarpour
- Assistance from C. W. Brown, A. Cuyt, I. Grant, J. Harrison, J. Hurd, D. Lester, C. Muñoz, U. Waldmann, etc.
- The research was supported by the Engineering and Physical Sciences Research Council [grant number EP/C013409/1].