Beyond $*$: Visualizing Quantifier Elimination for Real Arithmetic

Uday Shankar

12/18/2020

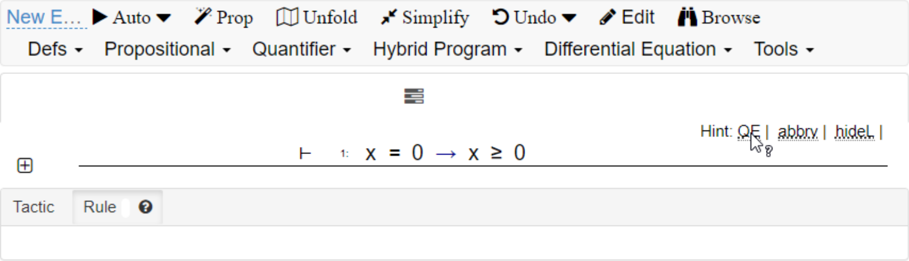
$$\frac{\textbf{?}}{\exists x\,\forall y\,\varphi}\,\mathbb{R}$$

Table of Contents

$$\frac{?}{\exists x\, \forall y\, \varphi}\mathbb{R}$$

Real Quantifier Elimination

Decision procedure is very convenient



$$\frac{?}{\exists x\, \forall y\, \varphi}\,\mathbb{R}$$

How Does it Work?

- Lab 1: decide sentences in $\mathbb{Z}/10\mathbb{Z}$.

$$\forall x\, \exists y\, (x + y = 0)$$

- `val domain = [0, 1, 2, 3, 4, 5, 6, 7, 8, 9]`
- Just loop!

$$\frac{?}{\exists x\, \forall y\, \varphi}\mathbb{R}$$

How Does it Work?

- Decide sentences in $\mathbb{R}$.

$$\forall x \, \exists y \, (x + y = 0)$$

- `val domain = [0, 1,` $3/2$`,` $\sqrt{2}$`,` π`, ...]`
- Just... loop?

$$\frac{?}{\exists x \, \forall y \, \varphi}\mathbb{R}$$

Real QE Algorithms

- Tarski: complex and slow
- CAD: (very) complex and fast
- Virtual substitution: not complete
- Cohen-Hörmander: (not too) complex and (not too) slow

$$\frac{?}{\exists x\, \forall y\, \varphi}\mathbb{R}$$

Project Goals

- Learn about Real QE (via Cohen-Hörmander)
- Make it easier for others to learn
  - Detailed writeup with motivation
  - Embedded animations
  - In-browser implementation

$$\frac{?}{\exists x\, \forall y\, \varphi}\mathbb{R}$$

Table of Contents

$$\frac{\mathbf{?}}{\exists x\, \forall y\, \varphi}\mathbb{R}$$

A Specific Case

Focus on univariate case: $\forall x\, \varphi$ or $\exists x\, \varphi$, $\mathsf{FV}(\varphi) = \{x\}$

$$\frac{?}{\exists x\, \forall y\, \varphi}\mathbb{R}$$

Expressiveness

- Terms in real arithmetic are polynomials (in x)
- Atomic formulae assert something about the sign of a polynomial

$$p_1(x) > p_2(x) \iff (p_1 - p_2)(x) > 0$$

$$\frac{?}{\exists x\, \forall y\, \varphi}\mathbb{R}$$

The Key Idea

To decide a formula, just need to know the **signs** of the polynomials involved at each $x \in \mathbb{R}$.

$$\frac{?}{\exists x \, \forall y \, \varphi} \mathbb{R}$$

The Sign Matrix

- Animation: `signmat_meaning`

$$\forall x\, [(p_1(x) \geq 0 \wedge p_2(x) \geq 0) \vee p_3(x) > 0]$$

$$p_1(x) = 4x^2 - 4$$
$$p_2(x) = (x+1)^3$$
$$p_3(x) = -5x - 5$$

- No numerical information!

$$\frac{?}{\exists x\, \forall y\, \varphi}\mathbb{R}$$

How the Sign Matrix is Useful

Animation: `signmat_usage`

$$\frac{?}{\exists x\, \forall y\, \varphi}\mathbb{R}$$

How the Sign Matrix is Constructed

- Want to construct sign matrix for $p_1, \ldots, p_n$.
- Recursively construct for $p_1', p_2, \ldots, p_n, r_1, \ldots, r_n$, where

$$
\begin{aligned}
r_1 &= p_1 \pmod{p_1'} \\
r_i &= p_1 \pmod{p_i}
\end{aligned}
$$

???

Given the recursively constructed matrix,

- Determine sign of p_1 at the existing roots and intervals (remainders)
- Add any roots of p_1 not already included and determine signs (derivative)

$\frac{?}{\exists x \, \forall y \, \varphi}\mathbb{R}$

Remainders

- Tells us the sign of p_1 at each existing root (of the $p_2, \ldots, p_n$)
- Animation: `remainder_reason`
- Animation: `signmat_roots`

$$
\begin{aligned}
r_1 &= p_1 \pmod{p_1'} \\
r_i &= p_1 \pmod{p_i}
\end{aligned}
$$

$\frac{?}{\exists x \, \forall y \, \varphi}\mathbb{R}$

Derivative p_1'

- Only 0 or 1 “new” root possible in each interval
- Animation: `deriv_root`

$\frac{?}{\exists x \, \forall y \, \varphi}\mathbb{R}$

New Roots and Signs on Intervals

- Already know signs of p_1 at every relevant root
- Use intermediate value theorem to find new roots
- Animation: `interval_opp`

$\dfrac{?}{\exists x\, \forall y\, \varphi}\mathbb{R}$

Putting it All Together

- Sign Matrix Implementation
- Univariate Decision Procedure

$$\frac{\mathbf{?}}{\exists x\,\forall y\,\varphi}\,\mathbb{R}$$

Table of Contents

$$\frac{?}{\exists x\, \forall y\, \varphi}\mathbb{R}$$

Resources

- Webpage
  - Term paper
  - Full writeup
  - Animations embedded
  - Implementation embedded
- GitHub repo, with some bonuses
  - Animation code, HQ renders
  - Implementation code

$$\frac{?}{\exists x \, \forall y \, \varphi}\mathbb{R}$$

Acknowledgements

- Prof. Platzer: telling me about Cohen-Hörmander
- 3blue1brown: animation framework
- infusion: Polynomial and Rational number JS libraries

$$\frac{?}{\exists x\,\forall y\,\varphi}\mathbb{R}$$